INDIA'S NATIONAL CYBER SECURITY POLICY (NCSP) AND ORGANISATION – A CRITICAL ASSESSMENT

Captain Sanjay Chhabra

"One hundred victories in one hundred battles is not the most skilful. Seizing the enemy without fighting is the most skilful."

- Sun Tzu Sixth Century BC [1]

Introduction

The nature of war does not alter but its character does.[2] Several seminal events and technological innovations were responsible for these alterations. War has expanded from the land and sea domain to air and space with the advent of the modern air force and space orbiters. In the last two decades, warfare discovered yet another powerful medium offered by ubiquitous digital networks, thus establishing the fifth dimension: 'Cyberspace.'

Background - Realm of Cyber Vulnerabilities

Cyberspace vulnerabilities are evident from the annual global statistics of cyber attacks suffered by a majority of nations. The 2012 Cyber Crime report of 24 leading countries by Norton indicated 556 million victims with an estimated loss of $ 110 million[3] as shown in Figure 1. Therefore, it cannot be denied that a cyber attack is not an end in itself, but a powerful means to a wide variety of ends, from propaganda to espionage and Denial of Service (DoS) to destruction of critical infrastructure.

---

[1] *Sun Tzu, 'The Art of War'. Translated by Samuel B. Griffith (Oxford University Press, 1963).*
[2] *Clausewitz, 'On War', book 1, Ch 1.*
[3] *Norton, Annual report by Symantec, '2012 Norton Cyber Crime Report' (Aug 12), available at URL: http://in.norton.com/cybercrimereport, (accessed on 15 Feb 14).*

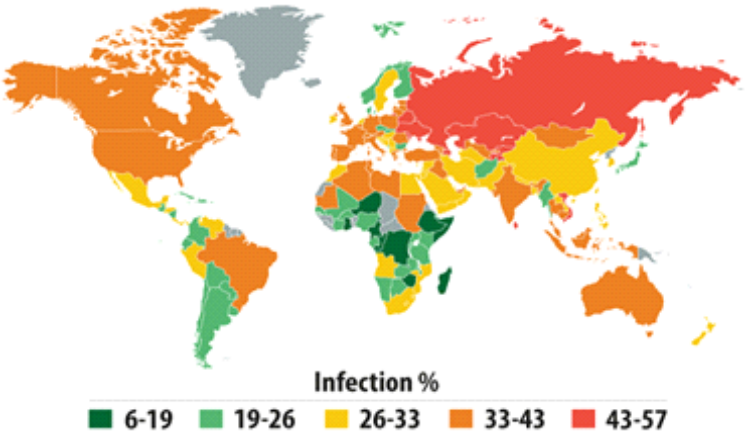

Fig 1: The statistics of cyber attacks committed on countries globally. (Source: Annual Report-2013 by Kaspersky Labs)

Global Flavour of Cyber Warfare. The scope and dimensions of the lethality of cyber attacks were evident when the Syrian air defence was reportedly disabled in October 2007 by the Israeli Air Force.[4] In another instance, Russia accrued significant benefits as it tightly integrated cyber operations with kinetic, diplomatic and strategic communication operations during the 2008 Georgia[5] conflict. In 2009, the reach and range of cyber espionage were also demonstrated by the 'GhostNet' program devised by China to snoop on 103 countries.[6] The fundamental methodology practiced by individuals with malicious intent was to inject malicious software universally known as malware. Malware such as TitanRain[7] in 2004, Stuxnet[8] in 2010, Duqu[9] in 2011, Flamer[10] and Disttrack

[4]*Ward Carroll, (26 Jan 2007), 'Israel's Cyber Shot at Syria', available at URL: http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria (accessed on 14 Feb 14).*

[5]*David M. Hollis, 'Cyberwar Case Study: Georgia 2008',(Small Wars Journal, 06 Jan 11), available at URL:http ://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008, (accessed on 10 Jan 14)*

[6]*Information Warfare Monitor, (March 2009), 'Tracking GhostNet: Investigating a Cyber Espionage Network, available at URL: http://www.dhra.mil/perserec/osg/counterintelligence/ cyber-espionage.htm, (accessed on 14 Feb 14).*

[7]*Nathan Thornburgh, 'Inside the Chinese Hack Attack', (Time US, 25 Aug.05), available at URL: http://content. time. com / time / nation /article/0,8599,1098371,00.html, (accessed on 24 Jan 14)*

[8]*Rowan Scarborough, 'In classified cyberwar against Iran, trail of Stuxnet leak leads to White House', (The Washington Times 18 Aug 13), available at URL: http://www.Washingtontimes.com/ news/2013/aug/18/trail-of-stuxnet-cyberwar-leak-to-author-leads-to-/#ixzz2rU3s4D18, (accessed on 11 Dec 13)*

[9]*HosseinJaseb, (13 Nov 2011), 'Iran-detected Duqu computer virus', available at: http:// www.reuters.com/article/2011/11/13/us-iran-computer-duqu-idUSTRE7AC0YP20111113, (accessed on 11 Feb 14).*

[10]*David Goldman, (30 May 2012), 'Super-virus Flame raises the stakes', available at:http://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security,(accessed 10 Feb 14).*

(Shamoon)[11] in 2012 and Red October[12] in 2013 demonstrated ever increasing levels of sophistication and lethality. The escalating trend in the number of malware recorded up to mid-2013 is shown in Figure 2.[13]

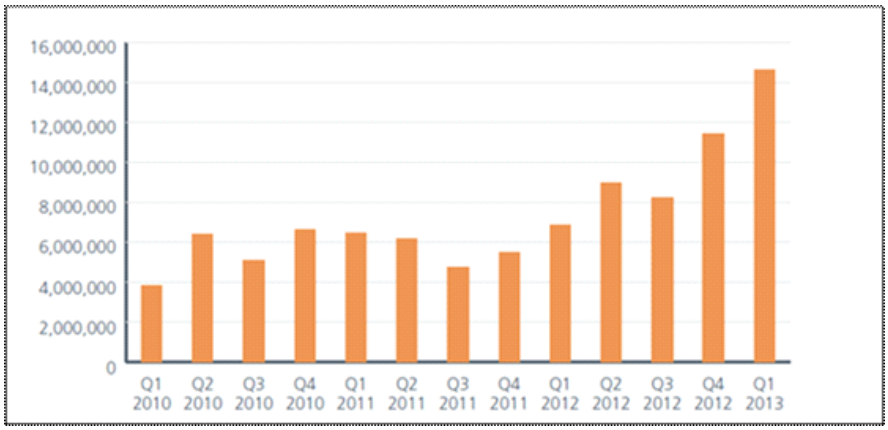

Fig 2: The graph indicates escalatory trend of Malware in the last three years. (Source : McAfee Labs, http://www.mcafee.com/in/resources/reports/rp-quarterly-threat-q1-2013.pdf, (accessed on 15 Feb 14))

Indian Cyberspace Perspective

Realm of Indian Cyberspace. The annual cyber crime statistics released by Norton reported that India suffered losses worth $ 8 billion in 2011.[14] The annual average number of cyber crimes was estimated to be 42 million on a pan-India basis.[15] Similarly, in another report, Indian Computer Emergency and Response Team (CERT-In) registered a total of 22060 attacks in the year 2012.[16] The trends as shown in Table 1, indicate a staggering 9,58,130% increase since 2004.

---

[11] *Mike Mount, CNN, (16 Oct 12), 'U.S. Officials believe Iran behind recent cyber attacks Shamoon Malware' available at URL: http: //edition.cnn.com/2012/10/15/world/iran-cyber/ (accessed on 8 Feb 14).*

[12] *Kaspersky Lab Report, 'The Red October Campaign', (14 Jan 13), available at URL: http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies, (accessed on 15 Feb 14)*

[13] *Jonathan Fildes, (BBC News 23 Sep 2010), 'Stuxnet worm 'targeted high-value Iranian assets',available at URL: http://www.bbc.co.uk/news/technology-11388018, (accessed on 8 Feb 14).*

[14] *Norton, Annual report by Symantec, '2012 Norton Cyber Crime Report' (Aug 12), available at URL: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton _ Cybercrime _ Report_Master_FINAL_050912.pdf, (accessed on 15 Feb 14)*

[15] *George Joseph, 'India has 42 mn cyber crime victims every year', (Business Standard 24 Jun 13), available at URL: http://www.business-standard.com/article/current-affairs/india-has-42-mn-cyber-crime-victims-every-year-113062400097_1.html, (accessed on 8 Feb 14).*

[16] *GOI, Ministry of Communications and Information Technology, (01 Mar 2013), 'Annual Report (2012) by CERT-In', available at URL: http://cert-in.org.in/Internet/Downloads/ANUAL-2013-0041.pdf, (accessed on 17 Feb 14).*

Table 1: Year-wise Summary of Cyber Security Incidents handled by CERT-In (Source: CERT-In Annual Report)

Security Incidents	2004	2005	2006	2007	2008	2009	2010	2011	2012
Phishing	3	101	339	392	604	374	508	674	887
Network Scanning / Probing	11	40	177	223	265	303	277	1748	2866
Virus / Malicious Code	5	95	19	358	408	596	2817	2765	3149
Spam	-	-	-	-	305	285	181	2480	8150
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344	4394	4591
Others	4	18	17	264	148	160	188	1240	2417
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**	**22060**

Evidence of Cyber Attacks. The most compelling evidence of cyber attacks was the hacking of the Prime Minister's Office in 2011[17] and breach of 12,000 sensitive email accounts in 2012 including those of officials from the Ministry of External Affairs (MEA),[18] Ministry of Home Affairs (MHA), Defence Research and Development Organisation (DRDO) and the Indo-Tibetan Border Police (ITBP).[19] Such intrusions also permeated into the Indian Armed Forces domain, though with limited success. Overseas cyber attacks were also reported from the Indian Embassies at Kabul and Moscow, the Consulate General at Dubai and the High Commission at Abuja, Nigeria.[20]

Indian Countermeasure Framework. India's response to cyber threats so far has been reactive and piecemeal. Over the last two decades, India has relied either on the formation of a new agency or a coordination committee after every

[17]*Saikat Datta, 'PMO fights largest cyber attack', (DNA, 22 Aug 11), available at URL: http://www.dnaindia.com/india/report-dna-investigation-pmo-fights-largest-cyber-attack-1578348, (accessed on 25 Jan 13).*
[18]*Phil Muncaster, '10,000 Indian government and military emails hacked', (Business Standard 24 Jun 13), available at http://www.theregister.co.uk/2012/12/21/indian_government_email_ hacked/, (accessed on 20 Feb 14).*
[19]*M Kaushik and P M Fitter, 'Beware of the bugs', (Business Today, 17 Feb 13), available at URL: http://businesstoday.intoday.in/story/india-cyber-security-at-risk/1/191786.html, (accessed on 26 Feb 14).*
[20]*Monika Chansoria, 'China's Cyber WarsIndia Strategicalso hacked', (The Indian Express, April 10), available athttp://www.indiastrategic.in/indian_air_force.htm,(accessed on 24 Feb 14)*

major cyber attack or intelligence failure. Complementing these actions, India's Department of Electronics and Information Technology (DEITY),[21] under the aegis of Ministry of Communication and Information Technology (MCIT), released the country's maiden National Cyber Security Policy (NCSP) on 02 Jul 2013.The policy document was considered a step in the right direction by the Data Security Council of India (DSCI)[22] and Institute for Defence Studies and Analysis (IDSA).[23] However, it is opined by the author that the policy still overlooks several cyber issues and fails to incorporate lessons learnt by cyber mature nations. Comparatively, in the last three decades the US, UK, Europe/ North Atlantic Treaty Organisation (NATO) and China have crossed the Rubicon in cyberspace security and warfare. The essence of their policy, concept and organisation are discussed in succeeding paragraphs.

CYBER BALANCE SHEET OF CYBER MATURE NATIONS

United States

In the early stages, the US struggled with several lacunae like inadequacy of national policy, multiple regional and national bodies, wasteful funding and practically no regulation to penalise the perpetrators. Realising this, President Bill Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP) in 1997.[24] According to the FBI Annual Report 2009, the surge of cyber attacks had continued unabated all through, leading to financial loss amounting to nearly $ 560 million.

The cyber breaches infiltrated military networks as well and the Pentagon reported an unprecedented 360 million attempts in the year 2006 including hacking into the $300 billion Joint Strike Fighter project.[25] In another spectacular

[21] *Government of India Policy on Cyber Security (GOI) (2013) – GOI notification on National Cyber Security Policy-2013 (NSCP-2013) File No 2(35)/2011-CERT-In dated 2, July 2013, available at URL: http://deity.gov.in/content/national-cyber-security-policy-2013-1, (accessed on 14 Nov 13).*

[22] *Report by Data Security Council of India, (Sep 13) 'Analysis of National Cyber Security Policy (NCSP – 2013)' available at URL: https://www.dsci.in/sites/default/files/NCSP%202013_ DSCI%20 Analysis%20v 1.0. pdf (accessed on 14 Dec 13).*

[23] *Sanjiv Tomar, (26 Aug 13) 'IDSA comment on National Cyber Security Policy 2013: An Assessment', available at http://www.idsa.in/idsacomments/NationalCyberSecurityPolicy 2013_stomar_260813 (accessed on 14 Dec 13).*

[24] *William J. Clinton, The President USA (15 Jul 1996). 'Executive Order EO 13010 Critical Infrastructure Protection', available athttp://www.fas.org/irp/offdocs/eo13010.htm (accessed on 18 Feb 14).*

[25] *Randy James (Time, US, 01 Jun 09) 'A Brief History of Cybercrime' available at URL: http://content.time.com/time /nation /article/0,8599,1902073,00.html (accessed on 28 Jan 14).*

breach, the Pentagon spent nearly 14 months in 2008 cleaning the worm 'agent.btz' which originated from a Department of Defence (DoD) facility in the Middle East. Under those circumstances, the US formed the United States Cyber Command (USCYBERCOM) on 23 June 2009 under the US Strategic Command (USSTRATCOM).[26]

Integration of Organisation. The onus of cyber security was spread across the Department of Homeland Security (DHS), Department of Defence (DoD) and Department of Justice (DoJ), which despite enviable credibility could not eradicate cyber attacks against the United States. Based on the realisation that these agencies operated in their own silos rather than in collaboration due to which protection of the nation as a whole was amiss, the National Cyber Investigative Joint Task Force (NCIJTF)[27] was formed in 2008 and compelled the US to move towards unity of command. The process included cross-integration between ISPs, DHS and DoD[28] to operate cohesively. The DoD also forged an alliance with the Federal Bureau of Investigation (FBI) to further strengthen the whole-of-government approach.

Policy Framework. The integration of agencies[30] was articulated in the overarching National Security Strategy (NSS) released in May 2010.[31] Based on the NSS the DoD phrased cyber concerns in the National Defense Strategy (NDS)[32] and the Quadrennial Defense Review (QDR).[33] Further, these strategic documents were used by the Joint Staff to formulate the National Military

---

[26]US Def Sec Robert Gates memorandum (23 Jun 2003) 'Establishment of subordinate unified U.S. Cyber command under Strategic Command for Military Cyberspace Operations', availableat http://online.wsj.com/public/resources/documents/OSD05914.pdf (accessed on 10 Nov 13)

[27]N Caplan, opcit, p 106

[28]A D Givens&N E Busch, 'Integrating Federal Approaches to Post-Cyber Incident Mitigation', (Journal of Homeland Security and Emergency Management.Vol 10, Issue 1,Jan 2013)pp 1–28

[29]N Caplan, 'Cyber War: the Challenge to National Security', (Global Security Studies,Winter 2013, Vol. 4 Issue 1), p 104

[30]C Henderson, 'The 2010 United States National Security Strategy and the Obama Doctrine of Necessary Force' (Journal of Conflict and Security Law vol 15, no. 3, 2010), p 405

[31]Barack Obama, The President of USA, White House, (May 2010), 'National Security Strategy' also available at URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_ strategy.pdf (accessed on 18 Feb 14).

[32]United States Department of Defense, 'National Defence Strategy-2008', (Washington DC, Jun 08), available at URL: http://www.defense.gov/news/2008%20national%20defense %20 strategy .pdf (accessed on 28 Jan 14), p 1

[33]United States Department of Defense, 'Quadrennial Defense Review -2014', (Washington DC, Mar 14), available at URL: http://www.defense.gov/pubs/2014_Quadrennial_Defense_ Review.pdf (accessed on 20 Mar 14), p 12

Strategy (NMS).[34] In sum, the US government now has a highly evolved and time-tested policy document to address cyber security at all levels, i.e. Strategic (NSS), Operational (NDS and QDR) and tactical (NMS).

United Kingdom

The British Government followed a similar template as the US and included an exclusive section on cyber security in its National Security Strategy (NSS) document of October 2010. The UK Government elevated cyber attack to a Tier-1 threat and pitched it alongside international terrorism.[35] The UK Cyber Policy articulates international cooperation as a strategy and identifies India as one of its strategic partner.[36] The NCSS has set aside £650 million and a time frame of five years to develop security against the entire spectrum of cyber threats.

European Union / NATO

NATO has also articulated its cyber policy in the National Cyber Security Framework Manual (NCSFM)[37] and set up a cyber organisation known as NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) on 14 May 2008 at Tallinn, Estonia. The Centre received full accreditation by NATO and attained the status of an International Military Organisation on 28 October 2008.[38]

ASSESSMENT - INDIA'S CYBER SECURITY POLICY 2013

The synthesis of NSCP-13 by juxtaposing the Indian cyber ecosystem and lessons learnt by cyber mature nations reveals that the national policy sets high goals and covers a wide array of initiatives ranging from an institutional

---

[34] *United States Department of Defense, Chairman of the Joint Chiefs of Staff 'National Military Strategy - 2004', (Washington DC, Mar 05), available at URL: http://www.defense.gov/news /mar2005/d20050318 nms.pdf (accessed on 28 Jan 14), p 1*

[35] *David Cameron , Prime Minister, Nick Clegg, Deputy Prime Minister, Presented to Parliament by the Prime Minister, HM Office (October 2010), 'A Strong Britain in an age of Uncertainty: The National Security Strategy (NSS-2010)', available at URL: https://www.gov.uk/government /uploads /system/uploads /attachment_data /file/61936/national-security-strategy.pdf, (accessed on 09 Jan 14).*

[36] *HM National Audit Office, 'The UK cyber security strategy: Landscape review', HC 890 session 2012-13 (12 Feb 13), available at URL http://www.nao.org.uk/wp-content/uploads/2013 /03/Cyber-security-Full-report.pdf, (accessed on 25 Jan 14)*

[37] *NATO, 'NATO and cyber defence', available at http://www.nato.int/cps/en/natolive/topics_ 78170 .htm?, (accessed on 01 Dec 13).*

[38] *NATO, 'Cyber Defence', available at http://ccdcoe.org/2.html, (accessed on 01 Dec 13).*

framework for emergency response to indigenous capacity building.[39] However, closer examination of NCSP-13 and a detailed review of the cyber organisation indicate several shortcomings in addressing our nation's cyber vulnerabilities.

Policy Shortcomings

Absence of National Security Policy. Firstly, the National Security Council (NSC) mandated with formulation of national policies since 1999 has not published any official document outlining the National Security Policy (NSP). Since NCSP-13 was not a subset of any national security policy, it was relegated to the status of an isolated departmental document of the Ministry of Communication and Information Technology (MCIT) rather than desirable national level policy.

Legislative Lacuna. Unlike legislation, which is enacted after a debate in the Parliament, NCSP-13 was not subjected to extensive public evaluation before it was brought into force. The draft was, however, shared with the National Association of Software Service Companies (NASSCOM) prior to release. Therefore, like any other policy, the NCSP too drifts towards being neither binding nor enforceable by the multitude of cyber agencies.

New Looming Threats. In 2012-13, bulk of e-transactions were brought about through cloud computing or smart phones and the hackers, too, have shifted their focus towards this medium. Evidently, more than 1,48,427 android based malware were detected in 2013.[40] The NCSP-13 neither elucidates this looming threat nor gives direction to secure this medium.

NCSP-13 and Armed Forces Landscape. 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-13 is largely ambiguous about the role, interplay and interdependence of these two distinct aspects of national cyber security. Defence Minister, Shri AK Antony during his speech on 25 May 13 at INA Ezhimala stated that the Indian Armed Forces were in the process of

[39]*Government of India Policy on Cyber Security (GOI) (2013) – GOI notification on National Cyber Security Policy-2013 (NSCP-2013) File No 2(35)/2011-CERT-In dated 2 Jul 2013, available at URL: http://deity.gov.in/ content / national-cyber-security-policy-2013-1, (accessed on 14 Nov 13).*

[40]*C Raiu and D Emm, Report by Kaspersky Labs, (Dec 13), 'Malware Evolution -the Top Security Stories of 2013'available at URL:https://www.securelist.com/en/analysis/204792318/ Kaspersky_Security_ Bulletin _2013_Overall_statistics_for_2013, (accessed on January 28, 2014 Jan 14), p 11.*

establishing a Cyber Command.[41] Creation of Cyber Command will mean a parallel hierarchical structure, and being an important stakeholder, it would be prudent to delineate the jurisdictional limits right at the beginning of policy implementation; an area where the NSCP-13 falls short.

Organisational Shortcomings

Multiple Cyber Agencies. Over the last two decades, the responsibility of cyberspace security has been fragmented among several ministries, agencies, departments and even non-government organisations (NGO), thereby making coherent and consistent government-wide action a challenge. Table 2 is a depiction of all the all recognised agencies involved in cyber security.

Table 2: Catalogue of all Possible Ministries and Agencies involved in Management of Cyber Environment in India (Source: Created by the Author)

India – Cyber Organisation					
PM Office/ Cabinet Secy (PMO/ Cab Sec)	**Ministry of Home Affairs(MHA)**	**Ministry of External Affairs (MEA)**	**Ministry of Defence (MOD)**	**Ministry of Common Info Technology (MCIT)**	**Non Govt Organisation (NGO)**
National Security Council (NSC)	National Cyber Coordn Centre (NCCC)	Country Ministers and Ambassador	Tri Service Cyber Command - Pending Operationalisation	Department of Information Technology (DIT)	Cyber Security and Anti hacking Organisation (CSAHO)
National Technical Research Orgn (NTRO)	Directorate of Forensic Science (DFS)	Defence Attaches	Army (MI)	Department of Telecommn (DoT)	Cyber Society of India (CySI)
National Critical Info Infrastructure Protection Centre(NCIIPC)	National Disaster Mgt Authority (NDMA)	Joint Secretary (IT)	Navy (DNI)	Indian Computer Emergency Response Team CERT-IN	Centre of Excellence for Cyber Security Research & Development In India (CECSRDI)
Joint Intelligence Group (JIG)	Central Forensic Science Lab (CFSLs)		Air Force (AFI)	Education Research Network (ERNET)	Cyber Security of India(CSI)
National Crisis Management Committee (NCMC)	Intelligence Bureau (IB)		Def Info Assurance & Research Agency (DIARA)	Informatics Center (NIC)	National Cyber Security of India (NCS)
Research and Analysis Wing (RAW)			Defence Intelligence Agency (DIA)	Centre for Development of Advanced Computing C-DAC	Cyber Attacks Crisis Management Plan of India (CACMP)
Multi Agency Center (MAC)			Defence Research Dev Authority (DRDO)	Standardisation, Testing and Quality Certification (STQC)	
National Information Board (NIB)					

[41] *Shri AK Antony, Hon'ble Defence minister of India, speech at Indian Naval Academy, Ezhimala, 'Cyber command will be formed soon: Antony', (The Hindu, 25 May 13), http://www.thehindu. com /news /national/kerala/cyber-command-will-be-formed-soon-antony/article4750061.ece, (accessed on 22 Jan 14)*

Prognosis. It can be easily concluded that no single official or entity oversees implementation of cyber security policy across the nation, and no single agency has the responsibility or authority to match the scope and scale of the cyber challenge, thereby eluding unity of command in the country. This hypothesis is supported by the following arguments:-

(a) **Multiple Apex Agencies**. To start with, the apex level itself has as many as six agencies (appended below), which are involved in cyber security management.[42] Over and above, the NCSP-13 has prescribed the formation of yet another apex level agency namely, 'National Cyber Coordination Centre' (NCCC),[43] thus adding to the confusion.

(i) National Information Board (NIB)[44]
(ii) National Security Council (NSC) / National Security Council Secretariat (NSCS)[45]
(iii) National Crisis Management Committee (NCMC)[46]
(iv) National Disaster Management of Authority (NDMA)[47]
(v) National Cyber Response Center (NCRC)[48]
(vi) National Technical Research Organisation (NTRO)

(b) **Nebulous Second Tier**. The onus at the next level is spread across the Ministry of Communication and Information Technology (MCIT), Ministry of Defence (MoD), Ministry of Home Affairs (MHA) and Ministry of External Affairs (MEA), thereby diluting accountability and clear lines of reporting.

(c) **Overlapping Responsibilities**. Often, agencies have been assigned overlapping responsibilities. For instance, CERT-IN formed in

[42]*Saikat Datta, 'India's cyber protection body pushes ahead', (Hindustan Times, 20 Jan 14), available at URL: http://www.hindustantimes.com/india-news/cyber-protection-body-pushes-ahead/article1-1174753.aspx (accessed on 27 Feb 14).*
[43]*Sandeep Joshi, 'India gets ready to roll out cyber snooping agency', (The Hindu, 10 June 13), available at URL http://www.thehindu.com/news/national/india-gets-ready-to-roll-out-cyber-snoo ping-agency/article479 8049.ece ?homepage=true (accessed on 27 Feb 14).*
[44]*MP Gupta, P Kumar & J Bhattacharya, 'Government Online', (Tata McGraw-Hill, New Delhi, 2006), p 241.*
[45]*M Shrivastava, 'Re-Energising Indian Intelligence', (Vij books, New Delhi, 2013), ch II, p 22.*
[46]*S Modh, 'Introduction to Disaster Management', (Macmillan, New Delhi, 2010), p 165.*
[47]*S Modh, op citibid, p 169.*
[48]*N Desai et al, IDSA Task Force Report 'India's Cyber Security Challenge', (IDSA Publication, New Delhi, 2012)), p 26.*

2004 vide GoI IT Act of 2000 (70B) under MCIT, was mandated to ensure cyber security of Critical Infrastructure,[49] which was later limited to only non-critical structures. Four years later, the National Critical Information Infrastructure Protection Centre (NCIIPC) formed under the NTRO vide GOI under IT (Amendment) Act, 2008, 70A[50] was mandated with the protection of critical infrastructure, directly under the Prime Minister's Office (PMO). At the same time, the National Disaster Management Authority (NDMA) which is under MHA, was also assigned responsibility for protection of cyber critical infrastructure. It can now be seen that three different agencies under three different ministries are operating towards the singular objective of securing critical/non-critical infrastructure.

(d) In the past, although the lead was taken by DEITY/MCIT in formulating national policy, this ministry does not have jurisdiction over influential ministries/departments like the MoD, MHA and NSCS/NTRO.

(e) Though the National Security Council/ National Information Board (NSC/NIB) is the sole authority to formulate and promulgate national policies, NCSP-13 was released by DEITY, which operates under another ministry, i.e. MCIT.

(f) NIB has become too unwieldy with 21 secretary level[51] members drawn from the entire spectrum of Indian ministry and bureaucracy who usually double-hat as NIB members. There are two impediments here; firstly, it takes enormous effort to assemble all NIB members together, and secondly, it leads to decision paralysis and protracted delays.

(g) CERT-IN is designated as a nodal cyber incident referral agency which is under MCIT but does not have any law enforcement capability/ responsibility which is currently assigned to MHA.

(h) **MEA Entry into Cyberspace**. MEA too has nudged into

[49]*Ministry of Communication and Information Technology (GOI) 'Indian Computer response Team', (02 Mar 14) available at URL http://cert-in.org.in/ (accessed on 02 Mar 14).*
[50]*PV Singh, 'India is victim to cyber espionage', (08 Feb 13), available at URL http://www. Governance now. com/views/interview/india-victim-cyber-espionage (accessed on 27 Feb 14).*
[51]*V.Singh, (26 Aug 13) 'Point out the function of National Information Board in Cyber Security',available at URL: http://www.preservearticles.com/2012032027854/point-out-the-function-of-national-information-board -in-cyber-security.html (accessed on 14 Dec 13).*

cyberspace as another coordinating agency. It has coordinated bilateral agreements on Cyber Security between CERT-In (under another ministry, MCIT) and USA,[52] Korea[53] and UK.[54] This is another classic example of wires being crossed between two ministries.

(j) Furthermore, the MoD has mandated the Defence Information Assurance and Research Agency (DIARA) and the DRDO as the nodal cyber security agency for the armed forces. The NCSP-13 has not brought out clearly whether their role would be in tandem or isolation in the event of a national cyber crisis.

RECOMMENDATIONS

Cyber Policy

Formulation of National Security Policy. India must formulate an all encompassing National Security Policy (NSP) by the Cabinet Council on Security (CCS) and NSC duly endorsed by the PMO. The National Cyber Security Policy should be a subset of this policy. Thereafter, National Cyber Doctrine can be formulated by NSC/NIB, and Cyber Security Strategy by respective ministries. This would introduce tier-based 'policy-doctrine-strategy' formulation and ensure 'whole-of-nation' approach in cyber security. The policy document must adequately articulate the role of armed forces and the review cycle.

Cyber Organisation

Revamp Apex Organisation. In sum, there are six apex bodies, five ministries, almost 30 agencies and five coordinating agencies that make up the cyber organisation. Needless to say, it requires serious introspection to make the entire structure conducive to effective command and control. It is recommended

---

[52] *Ministry of External Affairs (GOI) 'India-US Cyber Security Forum - Fact Sheet', (02 Mar 06) available at URL http://www.mea.gov.in/bilateral-documents.htm?dtl/6014/IndiaUS+Cyber+Security+Forum++Fact+Sheet (accessed on 27 Feb 14).*

[53] *Ministry of External Affairs (GOI) 'India- Republic of Korea Joint Statement for Expansion of the Strategic Partnership', (16 Jan 14) available at URL: http://www.mea.gov.in/bilateral-documents.htm?dtl/22752/India+Republic+of+Korea+Joint+Statement+for+Expansion+of+the+Strategic+Partnership (accessed on 27 Feb 14).*

[54] *Ministry of External Affairs (GOI) 'Joint Statement on Cooperation between India and the United Kingdom on Cyber Issues', (08 Nov 12) available at URL: http://www.mea.gov.in/bilateral-documents.htm?dtl/20792/Joint+Statement+on+Cooperation+between+India+and+the+United+Kingdom+on+Cyber+Issues (accessed on 27 Feb 14).*

that GoI reconfigure apex bodies 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 National Security Council (NSC), which would be singularly responsible for policy formulation, budget allocation and nationwide implementation. The CSC team should be constituted from personnel who have served in the field of cyber security at MCIT/MoD/MHA/NSCS in the past for a minimum period of five years. The existing and proposed structure are given in Figure 3 and 4 respectively.

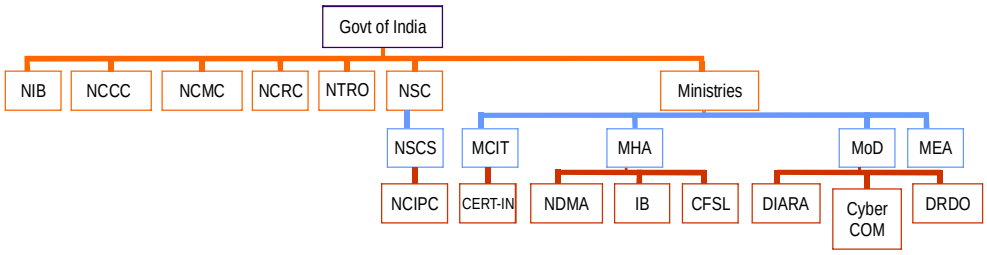

Fig 3: Present Organisational Structure (Source: Created by Author)

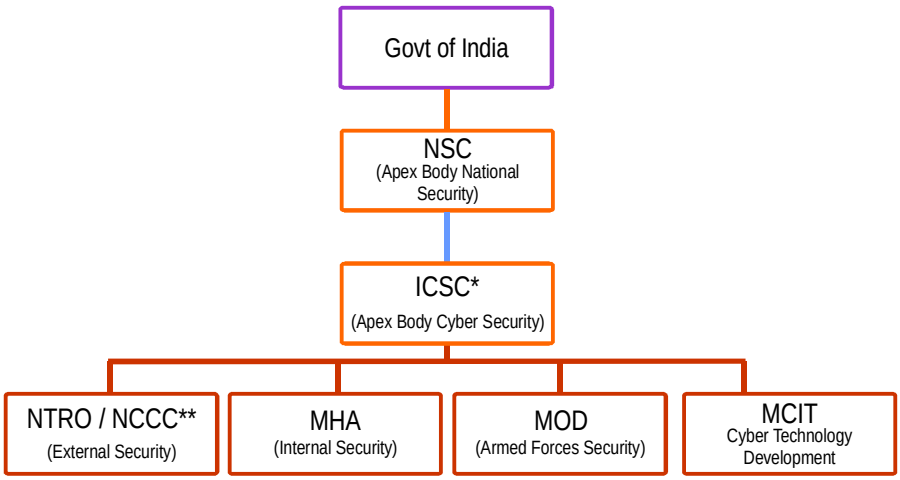

Fig 4: Proposed Function-based Hierarchical Structure.
** Proposed by author, ** Proposed in NCSP-13 (Source: Created by Author)*

A Leaner NIB. Although NIB saddled with 21 members has overarching control, it is ineffective and too unwieldy. It ought to be reduced to five to six members as the core, and the remaining members associated as subordinate members. It is recommended that at an opportune time NIB be merged with the aforesaid CSC.

Remodel Cyber Security Structure. It can be seen that due to progressive proliferation of multiple agencies, no organisation can claim primacy in the Indian cyber security landscape. The overall structure too does not follow any classical configuration, thereby having multiple reporting lines and blurred accountability. It is recommended that the cyber organisation be remodelled based on functionality and integrated collaborative structure. One such proposal is summarised in Table 3.

(a) As CERT-In does not have powers for law enforcement in the cyber domain, it is recommended that this agency be shifted under MHA from MCIT. This would not only simplify lines of reporting, but also ensure single-point responsibility and accountability of vulnerability assessment and law enforcement.

(b) The facility at DRDO, which is also foraying into the cyber security domain, must restrict itself to the Armed Forces domain. The onus of design and development of software for cyber security must remain with MCIT as the facility already exists with Centre of Development for Advance Computing (CDAC).

(c) As a short term goal, MCIT needs to develop basic software on the lines of 'WhatsApp' or 'Facebook' for India including the Armed Forces and as a long-term goal it must aim to develop our own browser and Operating System (OS).

*Table 3: Proposed Function-based Cyber Organisation. ✓ indicates direct responsibility of the function and ☑ indicates supporting role by external agencies. * Proposed apex agency with sole responsibility of national cyber security. (Source: Created by Author)*

Agencies →	CCS/ NSC	Indian CSC*	NTRO/ NCCC	MCIT	MHA	MOD	Pvt Play-ers	NGO/ Acade -mic
Function ↓	Apex	Internat'l Coopn	Ext Security	S/W and H/W/ Network	Int Secy	Cyber W/F		
National Secy Policy	✓	--	--	--	--	--	--	--
National Cyber Security Policy (NCSP)	--	✓	--	--	--	--	☑	--
National Cyber Doctrine	--	✓	--	--	--	--	--	--
Cyber Security Strategy	--	--	✓	✓	✓	✓	☑	--
Cyber W/F / Offense	--	--	--	--	--	✓	--	--
Cyber Secy	--	--	--	--	✓	--	☑	--
Cyber Crime / Terrorism	--	--	--	--	✓	--	☑	☑
Critical Infrastructure	--	--	--	--	✓	✓	☑	--
Development of S/W / Net Technologies	--	--	--	✓	--	✓	☑	--
Interagency Coordination	--	--	✓	--	--	--	--	--
Interface with Pvt Players to Develop H/W	--	--	--	✓	--	✓	☑	--
International Treaties & bilateral MoU	--	✓	--	--	--	--	--	--
HR Development	--	--	--	✓	--	--	--	☑
Overall Fiscal Management	✓	✓	--	--	--	--	--	--

CONCLUSION

Given the ubiquitous and dynamic characteristics of cyber power laced with the connotation of transgression at the national and global level, there are several issues that would require governmental consideration. India's inaugural National Cyber Security Policy (NCSP) is, on the whole, a step in the right direction. The policy hints at organisational mapping with references to CERT-IN and the NCIIPC but the roles and responsibilities of the armed forces, other government agencies as well as the private sector are not clearly articulated thereby making the nation vulnerable to cyber attacks. India has been acknowledged as the information backyard of the world; however, the government's efforts to address cyber security over the last two decades have only been reactive and piecemeal. Unless the stated policy lacunae and organisational structure are not adapted along the proposed lines, India will continue to remain vulnerable to marauding cyber attacks.

❀ ❀ ❀

About the Author

Capt Sanjay Chhabra, an alumnus of 6th NEC, was commissioned on 27 Nov 1993. The officer's afloat appointments include Senior Engineer and Commander 'E' of INS Betwa. He was commended by the FOC-IN-C (West) in 2006 for OP-Sukoon. He has been an instructor and commissioned the maiden FTTH-based network in any defence establishment at INS Shivaji. His experience also includes tenures at Mumbai Dockyard and Design Directorate. The officer has completed MTech from IIT Kanpur and was awarded two Gold Medals for excellence in research. He has also completed TMC and NHCC courses from Naval War College and was awarded CNS gold and FOC-in-C silver medals respectively. Capt Chhabra is presently DGM(Steam) at Naval Dockyard, Mumbai. The author can be reached at sanjaychhabra_in@yahoo.com