



ORF SPECIAL REPORT

MARCH 2016



The Cyber Command: Upgrading India's National Security Architecture

Arun Mohan Sukumar and Col. R.K. Sharma

Source: Perspecsys Photos

ABSTRACT

India is increasingly vulnerable to cyber attacks that range from intrusions that affect the integrity of data to large-scale attacks aimed at bringing down critical infrastructure. This vulnerability is largely a function of India's digital economy, which is a “net information exporter” that relies heavily on devices manufactured outside the country. Another complicating factor is the density of India's cyberspace, which does not permit a uniform legal or technical threshold for data protection laws. This paper proposes a security architecture that can improve inter-

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, academics and business leaders.



To know more about ORF scan this code

agency coordination, help respond to cyber attacks, and prevent them in many circumstances. The primary goals of the National Cyber Security Agency – a “Cyber Command” that brings together the Armed Forces and civilian agencies – are twofold: improve the country's resilience and defence systems against serious electronic attacks, while enhancing its own intrusive, interceptive and exploitative capabilities.

INTRODUCTION

Cyberspace is now as relevant a strategic domain as are the other four naturally occurring domains of land, air, sea and space. As the Union Minister for Defence Manohar Parikkar recently highlighted, India's defence capabilities must be strengthened against disruptive and highly sophisticated cyber-attacks.¹ Moreover, the country's Armed Forces must be geared to fight future wars in cyberspace, whether standalone skirmishes or in conjunction with kinetic battles.² Unlike conventional arenas of warfare, cyberspace has seen, and will continue to witness the proliferation of non-state actors, widely ranging in profile and capabilities. Instances of 'weaponising' the internet are on the rise – using its technologies for activities like recruitment of terrorists, radicalisation on the basis of specific narratives, disruption of crucial public services like electricity grids and the financial sectors, and the theft of commercial secrets. It is no exaggeration to claim that the integrity of India's digital networks can affect the strategic trajectory of a nation: cyberspace can be used to mould, even determine political outcomes; spur or stunt the growth of its economy; and strengthen or destabilise its critical information infrastructure.

India's burgeoning digital economy hosts the world's second largest user base on the internet.³ The Union government's flagship initiatives like 'Digital India', as well as the emphasis on governance premised on connectivity, are raising the stakes for the country's information infrastructure. It is conceivable that the integrity of India's cyber platforms will increasingly be subjected to threats and suffer vulnerabilities in the immediate future. Vice Admiral Girish Luthra, former Deputy Chief (Operations) in Headquarters Integrated Defence Staff (HQ IDS), recently suggested that a “cyber-race” is currently underway: with incidents of commercial espionage, IPR theft, denials of service, and other kinds of attacks being perpetrated on a daily basis.⁴ Safeguarding India's cyberspace – defined by this paper as infrastructure physically located within the nation's borders, as well data hosted by Indian individuals, corporations and governments anywhere in the world – requires not only a coherent conceptualisation of India's strategic interests, but a clear outlining of methods to secure them, as well as time-bound plans of action. As the country's cyber security apparatus is slowly being put in place, there is a need for policy and operational coherence.

STRATEGIC CHALLENGE

India's strategic challenge in cyberspace stems not just from external threats but the design and density of its digital ecosystem. While technology is moving from the

West to the East, information is flowing in the reverse direction, offering law enforcement agencies few options to protect and, where warranted, extract the data of Indian citizens. The overseas custody of data also exposes the sensitive information of citizens vulnerable to foreign attacks: for example, were a foreign database—located in foreign soil but hosting the information of Indian citizens—be attacked by a third party, Indian authorities have limited jurisdiction to investigate and prosecute the perpetrators. While a National Cyber Security Agency or a Cyber Command would offer institutional, inter-agency architecture to cooperate, defend and respond to attacks on Indian infrastructure, a broader strategic framework is required to protect Indian assets overseas, both civilian and strategic. This paper makes an assessment of India's strategic interests in cyberspace, and proposes an agile architecture that will be responsible for formulating cybersecurity policy and operationalising its key objectives. Such an architecture must take the form of a National Cyber Security Agency, an apex command organisation at the national level.

THREATS AND VULNERABILITIES

Cyber threats fall into four broad categories: espionage; warfare; terrorism; and crime. Remarkably, few international rules or norms currently exist to regulate the first three, while cyber crime is largely a concern of state law enforcement agencies, with limited legislative guidance on investigative processes. In 2015, 72 percent of Indian firms faced at least one cyberattack.⁵ Critical information infrastructure in India has also been subject to espionage campaigns like the Ghost net hacking of Defence Research and Development Organisation computers in 2012.⁶ By one estimate, India was among the countries most targeted by cyber criminals through social media in 2014.⁷ According to data from the Computer Emergency Response Team (CERT), some 8,311 security breach incidents were reported in the country in January 2015, as against 5,987 in November 2014.⁸ Meanwhile, the number of websites 'defaced' during the same period increased from 1,256 to 2,224.⁹ The CERT report ranked India as the third most vulnerable country in Asia for 'ransomware' attacks (malware that curtails access to the infected device in return for a ransom). As the Indian internet landscape becomes populated by first-time users of the internet, cyber threats are likely to become not only more frequent, but also increasingly sophisticated.

COMPARATIVE APPROACHES

Countries that are a step ahead in creating cyber security architecture have done so on the basis of their own threat perceptions. The United States and the United Kingdom, for instance, perceive cyber threats from the lens of national security, and thus pursue threat management strategies involving the military. The European Union, meanwhile, views vulnerabilities in cyberspace primarily as an irritant for commerce and data integrity, leaving their management to mostly civilian authorities. This is not to say that the militaries of constituent EU nations are not

involved in the crafting and implementation of strategies. The broad and doctrinal approach to cyber threats and attacks, nevertheless, influence operational roles of government agencies. The following section highlights comparative approaches to threats assessment and management in cyberspace.

USA

The US Cyber Command, based in Fort Meade, Maryland was established under the US Strategic Command (STRATCOM) on directions issued by the US government in June 2009. It achieved initial operational capability on 21 May 2010.¹⁰ Service elements in the Command include the Army Forces Cyber Command, the 24thUSAF Fleet Cyber Command, and the Marine Forces Cyber Command. “The Cyber Command plans, coordinates, integrates, synchronises, and conducts activities to direct the operations and defense of specified DoD's information networks and its critical infrastructure.”¹¹ The Cyber Command operates with several key mission partners, namely, the National Security Agency and its affiliated Central Security Service (NSA/CSS). A four-star General heads the Cyber Command commander while serving as the Director of the NSA/Chief CSS in what is referred to as a 'dual-hat' arrangement.¹² This arrangement of 'dual-hatting' has lent synergy to cyber operations. The Command also works with other federal government agencies, particularly the Department of Homeland Security and the Department of Justice and Federal Bureau of Investigation (FBI).

US military strategy for cyberspace was first promulgated in May 2011 by the US Department of Defence (DoD), which guided operations for nearly four years. In April 2015, the DoD released a new iteration of this strategy¹³ which outlines the goals and objectives in the cyber domain to be achieved over the next five years. This strategy identifies the following missions:

- (a) Defending US own networks, systems and data.
- (b) Defending US national interests against cyberattacks of “significant consequences”.
- (c) Supporting military operations and contingency plans with cyber operations, including by disrupting the adversary's military related networks.

The following goals are laid out in the strategy:¹⁴

- (a) Build and maintain “ready forces and capabilities” to conduct cyber operations.
- (b) Defend and mitigate risks to DoD networks and data.
- (c) Use “cyber options to control conflict escalation and shape the conflict environment at all stages.”
- (d) Defend against cyberattacks of “significant consequence”.
- (e) Create “international alliances and partnerships” to defend against threats and increase international security and stability.

To turn strategy and plans into operational outcomes, US CYBERCOM aims to build a workforce of 133 Cyber Mission Teams comprising 6,200 personnel by 2016.¹⁵ These 133 teams will be organised into three distinct Cyber Mission Forces: “cyber protection forces” that will defend military's own computer networks; “combat mission forces” that will support the mission of troops; and “national mission forces” to conduct specified missions to defend national critical infrastructure.¹⁶

The United States government has made substantial commitments to ensuring its military and intelligence architecture is responsive to the strategic dimensions of cyberspace. This is best exemplified by the recent measure within the US National Security Agency to “subsume” its Information Assurance Division (IAD) and Signals Intelligence Division (SID) into one Operational Directorate. In plain terms, the IAD focuses on defensive measures to protect the integrity of US systems data, while the SIG invests in resources and personnel for offensive, interceptive and exploitative operations.¹⁷

China

China's draft cyber security law and strategic architecture expressly refer to the need to promote and project state power in cyberspace.¹⁸ China is not hesitant to embed national security measures and language in the context of “economic and social development”, and it is no different in the case of cyberspace. While its national cyber security law was introduced as a draft in 2015 and is yet to be enacted, one analyst emphasises two cyber policy planning goals unique to the Chinese context:¹⁹

- a) Promoting economic growth through means not limited to “industrial economic cyber espionage of foreign targets”
- b) Ensuring the longevity of the Chinese Communist Party “through information control, propaganda, and targeting of domestic sources of potential unrest.”

Cyberspace, in addition to posing the same challenges and opportunities as for any powerful nation-state, is also crucial to sustaining China's unique political and economic order. Amy Chang and other analysts have also highlighted the “fragmented” decision-making structures within China that seem to be delaying the roll out and implementation of cyber security strategies.²⁰

The People's Liberation Army has made some progress in institutionalising its Cyber Command architecture, and more recently, integrating it with China's current armed forces. The PLA Cyber Command is reportedly under the 3rd Department of General Staff Department (GSD), which offers “operational guidance on signals intelligence, foreign language proficiency and defence information systems.”²¹ Unit 61398, which specialises in computer networking operations, is housed within the GSD. The cybersecurity firm, Mandiant's report 'APT-1', has estimated the PLA Cyber Command to have 130,000 personnel divided between its various operational divisions.²²

On 1 February 2016, China announced its biggest military reform since the 1950s, including the creation of a Strategic Support Force. According to observers, the SSF will form the core of China's information warfare force and as its specific missions will include “target tracking and reconnaissance, daily operation of satellite navigation, operating Beidou satellites, managing space-based reconnaissance assets, and attack and defense in the cyber and electromagnetic spaces.”²³ Another analysis, based on the words of a Strategic Support Force Commander, suggests that the SSF will integrate “planning, mechanisms, resources, programs, operations, and human resources,” with the other branches of the PLA, and be its “cloud think tank.”²⁴ It remains unclear how the Strategic Support Force will coordinate operations with the PLA's Cyber Command or constituent units.

MAPPING INDIA'S CYBER LANDSCAPE

Policy landscape

The broad contours of cyber security in India have been set by the National Cyber Security Policy, as promulgated by the Ministry of Communications and Information Technology in 2013. The policy aims to facilitate the creation of a secure cyberspace eco-system and strengthen the existing regulatory framework.²⁵ The policy, nevertheless, leaves room for improvement.

The National Security Council Secretariat, the nodal agency for cyber security and internet governance in India, should articulate an updated policy that builds on the 2013 document. The current policy does not offer high-level guidelines to protect strategic digital assets and critical information infrastructure. The realm of cyber security lies at the broad intersection of both military and commercial networks. The relevance of cyberspace both as a site and instrument of warfare should be addressed in subsequent iterations of the policy. The 2013 policy approaches cyber security from a transactional perspective, with a view to protect the data of individuals and corporations. This is a laudable goal, as is the policy's emphasis on streamlining cooperation between ministries and other sectoral agencies involved in cyber security. Nevertheless, new strategies must build on a grand narrative that evaluates how India's military, civil and commercial infrastructure can be leveraged to enhance the country's capabilities as a cyber power.

The 2013 cyber security policy was largely the output of deliberations within a single ministry. Given that the responsibilities of securing India's civil and military infrastructure have been distributed among several ministries, agencies and departments, it is important that the next version must involve inter-ministerial consultations. Where appropriate, multi-stakeholder input should be considered in the articulation of national cyber security policies.

Organisational landscape

The following agencies have been entrusted with Cyber Security management at various levels:

- (i) National Information Board
- (ii) National Security Council Secretariat (NSCS)
- (iii) National Crisis Management Committee
- (iv) National Cyber Response Centre
- (v) National Technical Research Organisation (NTRO) (includes the National Critical Information Infrastructure Protection Centre)
- (vi) National Disaster Management Authority (NDMA)
- (vii) National Cyber Security and Coordination Centre
- (viii) National Intelligence Grid (NATGRID)

While this is a comprehensive set of institutions designed to tackle specific cyber concerns, a second layer of governance functions is also carried out by the Ministries of Home Affairs, External Affairs, Defence, and Communications & Information Technology. A Joint Working Group has been created among these ministries to coordinate internet governance policies, but this multi-ministerial agency is still in its infancy, and its ambit remains unclear. The overlapping of organisational charters, the duplication of efforts, and hurdles to coordinating cyber operations among various stakeholder entities are all concerns that must be addressed urgently.

RECOMMENDATIONS

India's rise as a cyber power will likely be driven by the following key factors:

- (i) The articulation of a comprehensive national cyber space strategy;
- (ii) The technological development of cyber security capabilities;
- (iii) The development of human resources and human capital at operational levels;
- (iv) A synchronised governance/organisational structure;
- (v) Training and assimilating a cyber force for offensive and defensive operations.

National Cyber Strategy

The government relies on digital infrastructure for a wide range of critical services. This reliance is going to increase manifold when projects associated with the Digital India initiative begin to fructify. A high-level document outlining India's strategy to protect its cyberspace and harness its economic potential could serve as a base document for various ministries, PSUs, and other government agencies to draw out their own Standard Operating Procedures. Such a strategy document should outline two goals: first, send the signal to state and central government functionaries that

cyber security is a subject seriously considered at the highest levels in New Delhi, and second, the need to develop “cyber-hygiene” – safe practices to protect individual user data and systems – cuts across all sections of the economy and government, irrespective of position or rank.

Need for a National Cyber Set Up

As the US Department of Defence cyber strategy identifies, the trend of “using cyberattacks as a political instrument reflects a dangerous trend in international relations.”²⁶ For this reason, the scale and scope of attacks may vary from wanting to infiltrate networks without causing damage, to shutting down critical operational systems. Thwarting all forms of cyberattacks – especially ones that are intended to go undetected—is difficult and unrealistic. However, the more serious attacks can be deterred and effectively responded to, if there is an organisational set up that can assess the imminence of such threats and is technically capable of defending and responding to them. This paper proposes the creation of a National Cyber Security Agency – a Cyber Command—that would be responsible for a wide range of tasks, from policy formulation to implementation at the national level.

The organogram of the proposed agency is enclosed in Appendix A.

The NCSA would report to the Prime Minister's Office and will preferably be headed by Chief of Defence Staff (as and when approved by government). In the interim, the Chairman of the Chiefs of Staff Committee could lead the organisation. The NCSA may comprise the following wings:

- (a) Policy Wing
- (b) Operations Wing
- (c) Advanced Research Centre

The Policy Wing, headed by a bureaucrat (Additional Secretary-level) would be responsible for:

- (a) Strategic and long-term assessment of cyber threats and vulnerabilities.
- (b) Articulating the strategic use of cyberspace to further India's political and military objectives.
- (c) Vetting MoUs with other governments.
- (d) Laying out a roadmap for national cyber capacity building.
- (e) Facilitating coordination among various government agencies.
- (f) Proposing changes to India's legal and regulatory framework as it relates to information security.

The membership could comprise the following:

- (a) Chairperson—Additional Secretary-level (chosen on rotation from the National Security Council Secretariat and constituent ministries)

- (b) Representatives of following ministries/agencies:
- Ministry of Defence
 - Ministry of Home Affairs
 - Ministry of External Affairs
 - National Security Council Secretariat
 - Ministry of Communications and Information Technology
 - Defence Research and Development Organisation
 - National Technical Research Organisation
 - Ministry of Law and Justice
 - Private sector (where required)
 - Academia and representatives from think-tanks

Operations Wing: Implementing decisions taken by the Policy Wing will be the responsibility of an operations wing. It may be headed by a Lt. Gen. or equivalent from the Armed Forces and will comprise both Assurance and Exploitation Groups.

- a. The Assurance Group undertakes cyber defence measures to protect military and civilian critical infrastructure. Its mandate would also include capacity building and investment to build resilience. The group would further comprise two sub-teams:
- i. The Protection Section would involve CERT-In and sectoral CERTs from state governments and PSUs. The CERT, which is presently under the Ministry of Communications and Information Technology would join the Assurance group under NCSA.
 - ii. The Resilience Section would be responsible for disaster management and data recovery. Among other goals, it will be the primary task of this section to retrieve or salvage data from affected systems and render the moperational within the shortest timeframe.

The Assurance Group should be under a Joint Secretary or equivalent. This section should be populated by civilians (CERT employees), with defence systems to be manned by defence personnel. Private industry and representatives from Research & Development organisations may also form part of Assurance section.

- b. Exploitation Group: This is the arm of the agency focusing on intrusive, interceptive and exploitative operations, with an aim being to infiltrate social media and other information networks of target organisations, agencies and countries. The section is proposed to be headed by Major General or equivalent. Two sub-teams, relating to social media and network exploitation, would populate this group.
- The Network Exploitation section would include internal (to handle and subject domestic networks to penetration testing *a la* “red teams”) and

external (to deal with overseas networks) sub-teams. Its main functions would include:

- Undertaking reconnaissance of networks during peacetime to prepare for conflict.
- Scoping vulnerabilities of identified infrastructure/ networks, both internal and external.
- Maintaining a database of critical infrastructures/networks of targets.
- Exploiting target networks with speed and precision.

The network exploitation group would be manned by technically qualified individuals from the armed forces, DRDO, the NTRO and other R&D organisations, where appropriate.

- The Social Media section, too, would consist of sub-teams responsible for internal and external networks.
 - The Internal Team would monitor domestic social media, share data with organisations as deemed appropriate for remedial action.
 - External Teams: To exploit social media of target networks, and where necessary, engage in counter-narrative building and information gathering.

The social media sections could be populated by individuals on deputation from the MoD, MHA, and state police. Specialists can also be hired on contract or recruited for this purpose.

Advanced Research Centre(ARC)

The ARC is proposed to be a resource for research and analysis of gathered intelligence and data that has been farmed. The composition of the ARC will not be very different from that of the policy wing, and will prominently feature India's intelligence agencies.

Territorial Army (Cyber) Battalions: Cyber is a specialised capability that needs a dedicated cadre. Raising Territorial Army(TA) battalions to cater for the requirement of skilled cyber manpower would go a long way in meeting this requirement. TA battalions can be made responsible for tasks as envisioned for NCSA. Trained manpower will also be available for boosting national cyber resources in the hour of need.

Assessing Organisational Effectiveness: Merits v. Demerits

Responsibilities clearly demarcated, as specific agencies are in charge of research, defence and exploitation of networks.	Consolidation of resources under one organisation may lead to an all pervasive “super” cyber agency.
The structure lends operational synergy, with policy and ARC wings lending support to cyber operations.	Leadership style of individual heading the organisation will likely influence its overall functioning.
Faster response times, as an integrated organisation is likely to cut through bureaucratic hurdles.	
Cost-effective with minimal duplication of efforts, as is the case currently.	
Will generate a highly trained and qualified cyber force that will be a valuable asset in all circumstances/ crises. The proposed organisation will permit flexibility and adaptability to changing circumstances, regarding its own structure and constituencies/ departments involved.	

Roadmap for Implementation

The US Cyber Command, conceived in 2009, achieved limited operational capability by May 2010 and will be fully operational by 2016. China, Russia and Iran created similar structures in 2010. A conservative estimate would suggest that India's NCSA may take anywhere between six and 10 years to be fully operational. The most important concern is the recruitment of skilled individuals and human resources required to sustain the NCSA's operations. This paper offers a roadmap for the NCSA's achieving full operational status.

Limited Operational Capability by 2020

The formulation of a National Cyber Strategy, which would outline the broad goals and parameters for the NCSA to function, should be taken up as a high priority. By 2020, the Policy Wing and the Advanced Research Centre of the NCSA can be set up, which would involve identifying nominees from various ministries, agencies, and organisations. Given that this stage does not involve additional appointments or recruitment from new posts, it can be achieved within a few months from the date of approval of the NCSA proposal. The first step towards creating the operational nucleus of the NCSA can be made during this period; this would involve re-designating the existing CERT-In and Sectoral CERTs as part of the NCSA's Assurance Group. Guidelines to recruit individuals and technical specialists to the Operations Wing and the ARC should be drafted during this period, and an initial “call for experts” may be sent before 2020.

Full Operational Capability: 2025 Milestone

Full operational capability requires enhancing the operational core of the NCSA. The biggest task in this regard would be to populate the wings of the organisation with full-time staff. If recruitment guidelines were in place, and implemented during this period, the NCSA's functioning would be aided by the fact that the Policy Wing and ARC would already be providing qualitative inputs to guide operations.


CONCLUSION

The next five years are expected to be crucial to the conception, evolution, and maturation of international cyber norms. The UN Group of Governmental Experts, which has been convening since 2012, in its last report outlined the basic principles of engagement during peacetime. Initiatives like the Tallinn Manual – issued by a group of non-governmental experts under the aegis of the NATO Cooperative Cyber Defence Centre of Excellence – have attempted to outline rules of engagement during war. It remains to be seen whether these processes will converge into a comprehensive, codified set of norms, but international efforts seem to be working on the assumption that it is impossible to prevent all manners of cyber attacks. Indeed, the sophistication and rapid advancement of exploitative technologies suggest that norms of behaviour in cyberspace are aimed at fostering restraint. This is a political exercise, which assumes that engagement in cyberspace between state and non-state actors can be conditioned by international relations.

There are lessons to be learned from such an approach: the proposed National Cyber Security Agency (NCSA) is premised on the principle that while cyber attacks may not always be fully thwarted, they can at least be more accurately predicted through sustained intelligence gathering. The Policy Wing and Advanced Research Centre of the NCSA are its critical limbs: they fulfil the functions of inter-agency coordination and information-sharing which is absent in India's current cyber security apparatus. Keeping a close tab on trends in cyber warfare is crucial to preventing attacks, and so is understanding the political context in which they occur, and the nature and capabilities of global non-state actors. The Operations Wing responds to attacks, but also serves the important function of “cyber deterrence” through its exploitative capabilities. Deterrence, unlike in the context of nuclear weapons, cannot be based on a quantitative threshold given the varying nature of cyber attacks. India's efforts should therefore be to enhance its intrusive and exploitative capabilities that restrain other actors from carrying out large-scale attacks.

While China has sought what it calls the “informationisation” of warfare – broadly acknowledging the role of information as weapons in battle – India should first seek to harvest data to enhance its capabilities. The strengthening of India's digital forensics capabilities, signature detection sensors and attributive capacity is just as important as building an arsenal of cyber weapons.

This paper offers a structure along which the country's cyber security apparatus may be aligned. Irrespective of the final shape that this organisation takes, what

remains unchanged is the role and relevance of key stakeholders and government agencies. The convergence of key departments or wings of the armed forces should create an architecture that is more than the sum of its parts. The NCSA, with its constituents articulating and implementing cyber security policies, is a first step in this regard. 

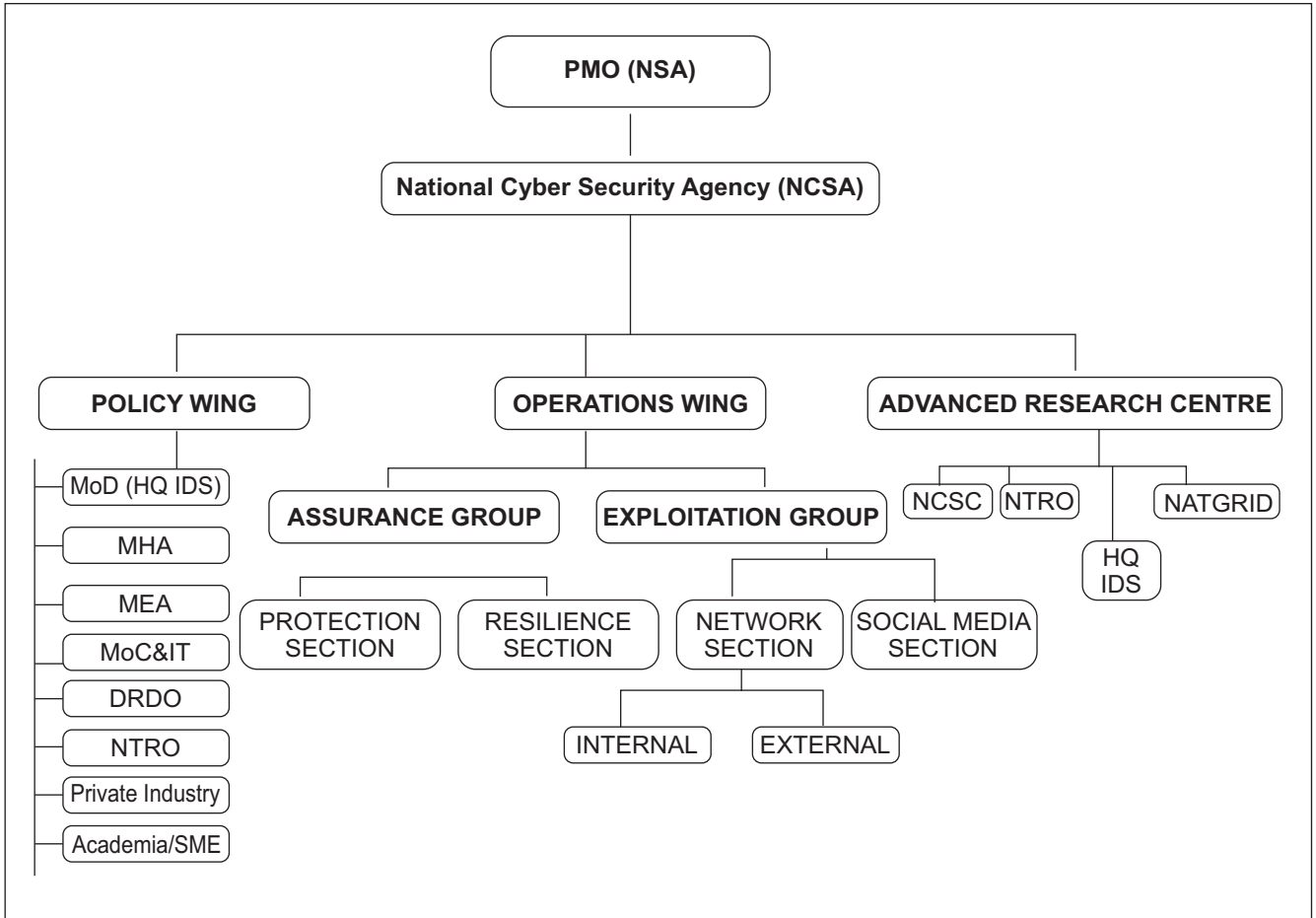
ABOUT THE AUTHORS

Arun Mohan Sukumar heads the Cyber Initiative at the Observer Research Foundation, New Delhi.

Col. R.K. Sharma holds the Chair of Excellence for Defence Forces in 2015 at the Observer Research Foundation, New Delhi.

(The views expressed here by both authors are personal and should not be attributed to any organisation.)

Appendix A



ENDNOTES:

1. *Armed Forces vulnerable to cyber attacks, says Defence Minister*, The Hindu, November 23, 2015 <http://www.thehindubusinessline.com/info-tech/armed-forces-vulnerable-to-cyber-attacks-says-defence-minister/article7909315.ece> [last accessed February 17, 2016]
2. *See generally*, Scott D. Applegate, *The Dawn of Kinetic Cyber*, https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf
3. *IAMAI: India's internet user base to hit 402 million, second-highest in the world*, <http://timesofindia.indiatimes.com/tech/tech-news/IAMAI-Indias-internet-user-base-to-hit-402-million-second-highest-in-the-world/articleshow/49816190.cms> [last accessed February 17, 2016]
4. Liam Nevill, *Cyber Wrap*, <http://www.aspistrategist.org.au/cyber-wrap-94/> [last accessed February 17, 2016]
5. Rica Bhattacharyya, *72% Indian companies faced cyber attack in 2015: KPMG survey*, The Economic Times, December 1, 2015 http://articles.economictimes.indiatimes.com/2015-12-01/news/68688315_1_cyber-risks-cyber-forensics-kpmg-survey [last accessed February 17, 2016]
6. Anirudh Bhattacharyya and Pramit Pal Chaudhuri, *Was Beijing behind it and why?*, Hindustan Times, April 12, 2010 <http://www.hindustantimes.com/india/was-beijing-behind-it-and-why/story-kR31Jmfg0b6sCEYxExDSJN.html> [last accessed February 17, 2016]
7. Yuthika Bhargava, *India ranks second in cyber attacks through social media*, The Hindu, April 22, 2015, <http://www.thehindu.com/news/national/india-ranks-second-in-cyber-attacks-through-social-media/article7130961.ece> [last accessed February 17, 2016]
8. *India a soft target for cyber criminals, says study*, Business Standard, May 10, 2015, http://www.business-standard.com/article/current-affairs/india-a-soft-target-for-cyber-criminals-symantec-115050900513_1.html [last accessed February 17, 2016]
9. *Ibid.*
10. Mike Lennon, *Cyber Command (CYBERCOM) Reaches Full Operational Capability*, Security Week, November 4, 2010 <http://www.securityweek.com/cyber-command-cybercom-reaches-full-operation-capability> [last accessed February 17, 2016]
11. Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, before The House Committee On Armed Services: Subcommittee On Emerging Threats And Capabilities, 4 March 2015 in *Cyber Operations: Improving The Military Cyber Security Posture In An Uncertain Threat Environment U.S. House Committee On Armed Services One Hundred Fourteenth Congress, First Session*, <https://www.hsdl.org/?view&did=764880> [last accessed February 17, 2016]
12. *Ibid.*
13. *Department of Defence Cyber Strategy*, April, 2015 http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [Last accessed February 18, 2016]
14. *Ibid.*
15. *Id.*
16. *Id.*
17. *See generally*, Susan Hennessey, *Good Defense is Good Offense: NSA Myths and the Merger*, Lawfare, <https://www.lawfareblog.com/good-defense-good-offense-nsa-myths-and-merger> [Last accessed February 18, 2016]; Ellen Nakashima, *National*

- Security Agency Plans Major Reorganisation*, The Washington Post, February 2, 2016
https://www.washingtonpost.com/world/national-security/national-security-agency-plans-major-reorganization/2016/02/02/2a66555e-c960-11e5-a7b2-5a2f824b02c9_story.html [Last accessed February 18, 2016]
18. *See generally*, Draft cybersecurity law of the People's Republic of China, http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm [Last accessed February 18, 2016]
 19. Amy Chang, *Warring State: China's Cybersecurity Strategy*, Centre for a New American Security, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf [Last accessed February 18, 2016]
 20. *Ibid*; Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press (2015), p.9.
 21. *Exposing One of China's Cyber Espionage Units*, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [Last accessed February 18, 2016].
 22. *Ibid*.
 23. John Costello, *The Strategic Support Force: China's Information Warfare Service*, China Brief Volume: 16 Issue: 3, The Jamestown Foundation http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=45075&cHash=9758054639ab2cb6bc7868e96736b6cb#.Vs7B63197s0 [Last accessed February 18, 2016].
 24. Lincoln Davidson, *China's Strategic Support Force: The New Home of the PLA's Cyber Operations?*, Council on Foreign Relations, <http://blogs.cfr.org/cyber/2016/01/20/chinas-strategic-support-force-the-new-home-of-the-plas-cyber-operations/> [Last accessed February 18, 2016].
 25. *The National Cyber Security Policy 2013*, Department of Electronics and Information Technology, July 2013, [http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20\(1\).pdf](http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf) [Last accessed February 18, 2016].
 26. *Ibid* at n.13.



Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773

E-mail: contactus@orfonline.org

Website: www.orfonline.org