Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
47/17

ORGANISATIONAL FRAMEWORK OF INDIA'S CYBER DEFENCE AND RESPONSE

E.Dilipraj and Ramnath Reghunadhan

The rapid developments of information and communication technologies (ICTs) as well as the emerging interconnectivity among different actors in the cyberspace have transcended the traditionally demarcated political and physical boundaries. But this has also led to seemingly exponential increase in the form of virtual threats and attacks, in particular towards the nation-states. In fact, it was opined by Dr. A.P.J. Abdul Kalam, the former President of India, that "Cyber warfare is the biggest threat to national security which will render even the Inter Continental Ballistic Missiles (ICBM) insignificant as a security threat."[1] The sources of the threats and attacks have increasingly adopted strategies that are relatively of low-risk and low-cost in nature specifically focusing on the susceptible targets.

An overt cyber offensive/warfare capability is effective in severely disrupting or destroying the critical information infrastructures (CIIs), breaching critical data, disrupting the financial security or even paralyzing the country to such an extent that it might not be able to respond with an effective conventional attack. On the other hand, covert cyber operation(s) specifically entail the infiltration of assets of target nations, and are more devised to gain actionable intelligence or even, if needed, cripple the communications, command and control infrastructure of the target. Over the years, there is an increase in covert operations and clandestine activities[2] by major actors especially the five eyes[3], which have greatly overwhelmed the cyber defence capabilities and preparedness of most of the countries.

India is one of the victims of some serious cyber intrusions and attacks in the past not only to their civilian cyber infrastructure but also to their sensitive defence establishments. In February 2009, around 600 computers of the Ministry of External Affairs were reported to have been hacked. In the subsequent year, in the month of April, Chinese hackers reportedly broke into classified files related

to India's missile and armament systems from the network of the Ministry of Defence (MoD) and Indian embassies. Once again in December 2010, the Central Bureau of Investigation's (CBI) official website was hacked and its data was compromised by Pakistani hackers group known as Pakistan Cyber Army (PCA). Two years later, in July 2012, a malware, entered through an infected USB drive, compromised the computers and systems in the Eastern Naval Command HQ, resulting in the siphoning of sensitive data to sources located outside the country. In July 2012 more than 10,000 email addresses of Indian government officials were purportedly hacked, including that of officials part of the Prime Minister's Office (PMO), as well as other ministries, departments and intelligence agencies. More recently, in March 2013, there were reports about the Defence Research and Development Organization (DRDO) being compromised, and a large quantity of sensitive data being supposedly uploaded to a server located in Guangdong province in China.[4]

The various incidents listed above stand proof of the fact that the country and its cyber infrastructures, even in the defence sector, are vulnerable to persistent cyber attacks. The country, however, has from time to time taken considerable steps in boosting its cyber security in all spheres. In this direction, the recent addition to bolster the country's cyber preparedness especially from a defence perspective is by setting up of a new Cyber Unit under the HQ Integrated Defence Staff (IDS) organisation, which would be a first of its kind.[5]

However, there exists an ambiguity in terms of the effectiveness of the existing cyber defence and response architecture in the country. Therefore, there is a need to visualize an organisational framework, which has led to the creation of visual representation as shown in the image below.

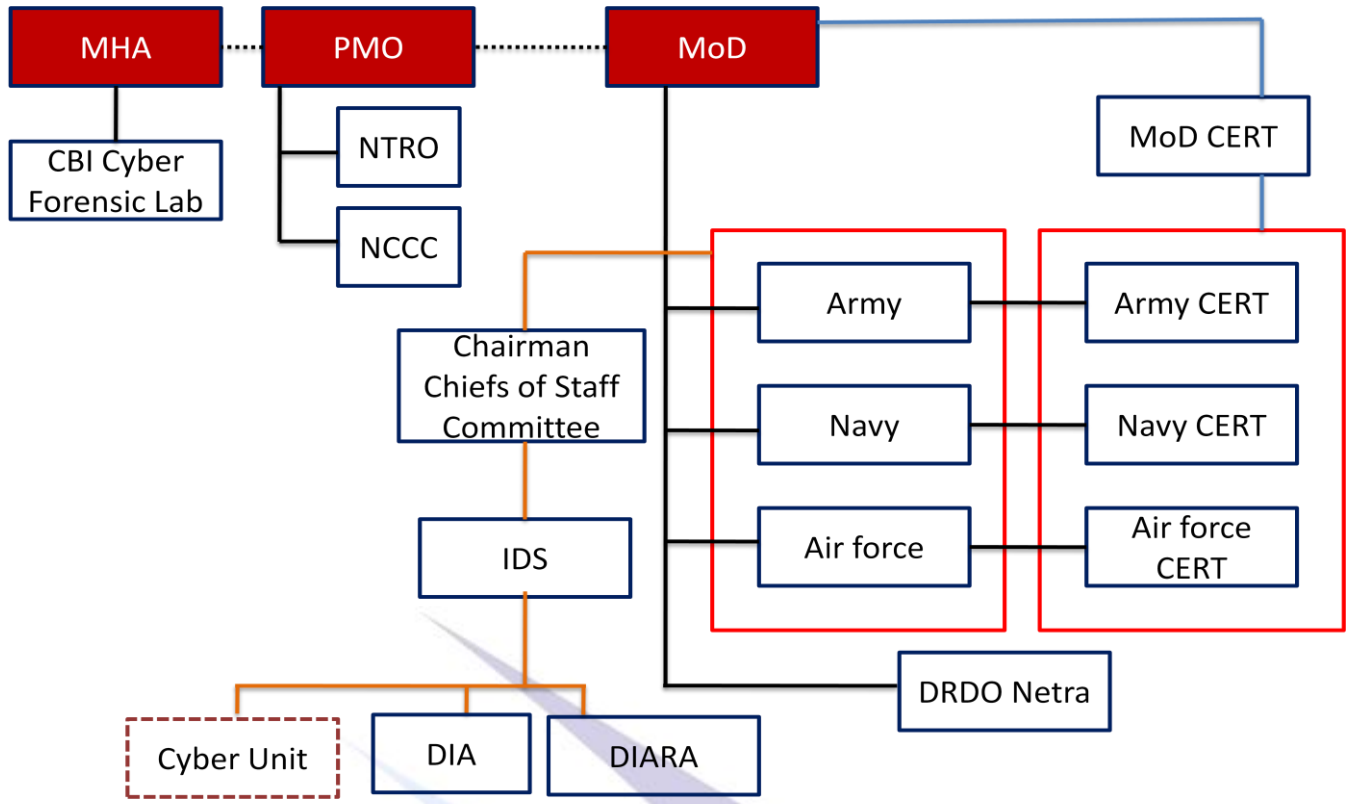

Image: Pictorial Representation of the organizational Framework of India's Cyber Defence and Response

The study helps in identifying different organisations spread across three Ministries that can effectively collaborate and cooperate in installing a robust cyber defence mechanism in the country. Firstly, MoD plays the major part with regard to defence, response and resilience of the nation in case of an impending cyber attacks. The respective Computer Emergency Response Teams (CERTs) of Army, Navy and Airforce are interlinked with each other and come under the ambit of the MoD-CERT, which is largely a coordinating agency. The HQ Integrated Defence Staff (IDS) which comes under the aegis of the Chairman of Chiefs of Staff Committee, houses three important organizations, namely Defence Information Assurance and Research Agency (DIARA), Defence Intelligence Agency (DIA) and the upcoming Cyber Unit. The DIA is responsible for providing and coordinating actionable cyber intelligence to the armed forces. The upcoming Cyber Unit will be composed of personnel from all the three services,[6] Ministry of Defence (MoD), Ministry of External Affairs (MEA) and the like.[7] The Cyber Unit is expected to have defensive capabilities along with considerable response capabilities in the cyber domain. Defence Research and Development Organisation (DRDO), which is also part of the MoD, plays an important role, as it manages the Network Traffic and Analysis (NETRA) programme in order to deal with malafide messages, blogs, social networks, images and in capturing any dubious internet voice traffic.[8]

Under the Prime Minister's Office (PMO), the National Technical Research Organisation (NTRO), which is responsible for technical intelligence, and the National Cyber Coordination Centre (NCCC), which is the country-wide coordinating agency on all cyber matters, are very much part of the cyber defence and response architecture of the country mainly due to their pan India focus and also their unique responsibilities.

Finally, the Ministry of Home Affairs (MHA) houses the Central Forensics Science Laboratory (CFSL) under the Central Bureau of Investigation (CBI), which is regarded as an important asset mainly due to their attributing capability to deal with any form of cyber attack.[9]

In conclusion, after having identified the cyber defence and response architecture of India, it could be stated that there exists a robust organisational framework which would be effective in engaging with sophisticated adversaries in cyberspace and building impressive plans to defend the organisations, operations and strategic objectives of the country. The architecture provides coordination and cooperation at the inter-organisational level so as to undertake accurate and effective responses to conflicts, threats, crises and even war. Also, there is scope for the country to expand the existing architecture as per the demands in the future.

E.Dilipraj is an Associate Fellow and Ramnath Reghunadhan is a Research Intern in Centre for Air Power Studies.

Notes

[1]Air Marshal Anil Chopra PVSM AVSM VM VSM (Retd). Cyber: The Next Cold War, 2016. Available online at http://www.defstrat.com/cyber-next-cold-war, accessed on June 1, 2017

[2] Barton Gellman and Greg Miller. 'Black budget' summary details U.S. spy network's successes, failures and objectives, 2013. Available online at https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08, accessed on May 30, 2017/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html?utm_term=.4be245473705

[3] The US and the UK are two of the so-called Five Eyes -- along with Canada, Australia and New Zealand -- that share a broad range of intelligence in one of the world's tightest multilateral arrangements.

Jason Hanna. What is the Five Eyes intelligence pact?, 2017. Available online at http://edition.cnn.com/2017/05/25/world/uk-us-five-eyes-intelligence-explainer/, accessed on May 30, 2017

[4] Significant Cyber Incidents Since 2006, Center for Strategic and International Studies (CSIS), 2017. Available online at https://www.csis.org/programs/technology-policy-program/cybersecurity/other-projects-cybersecurity/significant-cyber, accessed on May 31, 2017

[5]Ajit Kumar Dubey. Case of nosy neighbours: India to set up new defence unit to fight cyber attacks, 2017. Available online at http://indiatoday.intoday.in/story/cyber-attacks-pakistan-china-india-defence-ministry/1/896511.html, accessed on May 31, 2017

[6] Ajit Kumar Dubey. Case of nosy neighbours: India to set up new defence unit to fight cyber attacks, 2017. Available online at http://indiatoday.intoday.in/story/cyber-attacks-pakistan-china-india-defence-ministry/1/896511.html, accessed on May 31, 2017

[7]About IDS. Available online at http://ids.nic.in/aboutids.htm, accessed on June 1, 2017

[8]Amitav Ranjan. Home seeks system to intercept Net chatter, 2013. Available online at http://archive.indianexpress.com/news/home-seeks-system-to-intercept-net-chatter/1132688/, accessed on May 31, 2017

[9] CFSL-Central Forensics Science Laboratory. Available online at http://cbi.nic.in/cfsl/cfsldivision.htm, accessed on June 1, 2017