National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# TO PROJECT AND PROTECT: INDIA'S UNDERDEVELOPED CYBERSPACE OPERATIONS PROGRAMME

**Major Caleb de Boer**

## JCSP 46

## Solo Flight

**Disclaimer**

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.



## PCEMI 46

## Solo Flight

**Avertissement**

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.



Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIEN

JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

# TO PROJECT AND PROTECT: INDIA'S UNDERDEVELOPED CYBERSPACE OPERATIONS PROGRAMME

By Major Caleb de Boer



Word Count: 5,446

Nombre de mots : 5.446

# TO PROTECT AND PROJECT:
# INDIA'S UNDERDEVELOPED CYBERSPACE OPERATIONS PROGRAM

## INTRODUCTION

The world is changing. Geopolitical reviews seem uniquely focused on China's ascendancy in a world in which US global hegemony is questioned. Other pundits opine how rapidly technology has pervaded almost every aspect of human existence. Quietly in the midst of all this, India is rising.

India, with nearly 1.4 billion people, is the second most populace country in the world and is expected to surpass China this decade, growing to have 655 million more people by the end of the century.[1] In part due to normal population growth, free of government restrictions, India will also soon have a younger, more educated workforce than China; by 2030 India will have roughly 117 million graduates to China's 97 million.[2] India's economy is growing too, it is currently eight times larger than Pakistan's with this gap expected to increase to sixteen times by 2030.[3] These figures are impressive, but do not necessarily translate into power and influence. Today's estimates place it a distant fourth in global power (behind the United States, China, and Europe); though by 2050 the gaps may have narrowed, with China leading.[4]

India faces two strategic rivals: Pakistan and China. Pakistan has long been a thorn in India's side; within months of Independence in 1948, war broke out between the

---

[1] United Nations, "World Population Prospects 2019: Highlights," last accessed 29 April 2020, https://www. un. org/development/desa/publications/world-population-prospects-2019-highlights. html; and, Marco Aliberti, "India in Space: Between Utility and Geopolitics," Cham, Switzerland: Springer,http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1690971&site=ehost-live&scope=site, 243.

[2] Ibid.

[3] Journal of Current Issues in Globalization, "Global Trends 2030: Alternative Worlds," 2013a. *Journal of Current Issues in Globalization* 6 (1): 1, 15.

[4] Global Trends 2030: Alternative Worlds, 16.

fledgling nations. The Jammu-Kashmir region continues to inflame tensions and features ongoing escalatory skirmishes and terrorism. Foreshadowing conflicts to come, India has also had to defend its interests in the region against China during the Sino-Indian war of 1968. More recently, there has been much consternation about China's military growth and the potential threat, at very least, to Asia. Complicating matters, though conflict in the region has been near constant, with the advent and normalization of cyberspace operations, the weapons of war itself are changing.[5]

The central question is: how is India adapting to these changes? Will India's growth result in another superpower, will it be a strategic counter-balance to China's rise, or will India be locally constrained? Blending geopolitics and technology, these questions can be answered through an extrapolation of India's ability to protect and project power in cyberspace; that is, India's ability to exert more than local influence will be approximated by its ability to conduct cyberspace operations.

It will be shown that India, though maturing in cyberspace operations, still has several significant challenges to overcome in order to have a fulsome, regionally relevant cyberspace operations capability. This will be demonstrated by exploration of defensive, intelligence and offensive operations in cyberspace. Regarding defense, the paper will describe the challenges within the Indian populace, its government and its military. It will be shown that India has a myriad of overlapping and non-integrated/inter-acting agencies at the national level leaving its military with an incident response posture. Regarding cyberspace intelligence operations, it will be seen that India's military has a minimal capacity and that the doctrine and priorities are lacking and lagging. Regarding offensive

[5] NPR, "How the U.S. Hacked ISIS," https://www npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis, last accessed 19 April 2020.

operations, though shrouded in secrecy, there are positive indications that India is developing and employing offensive cyber operations but the nature, scope, and national doctrine are insufficient for a global power. India is not now nor likely to be in the near future more than a defensive, local power in cyberspace – marginally able to protect and project military power in cyberspace.

Before delving into the analysis several definitions as well as the scope of the analysis must be established. Firstly, this analysis will consider cyberspace operations which consist of operations 'in' cyberspace (ie, those whose target is some form of technology) and of operations 'through' cyberspace (ie those whose target is information and the receipt thereof). There is some consideration of Information Warfare but the intent is not to delve into the implications of the 'cognitive' or 'information' domains as part of India's future global power status; it is sufficient to consider cyberspace without getting mired in unclear, nouveau terminology. Secondly, this review will not be a complete study of Indian, Pakistani or Chinese military power but will instead focus on Indian cyberspace capabilities, making reference to other nations as appropriate. Thirdly, due to the nature of cyberspace operations as a strategic capability, though this analysis is rooted in military operations, it will include consideration of national elements. This is in part due to the newness of cyberspace operations insofar as national strategic doctrine, programs and priorities continue to have a significant impact on national cyberspace power. Additionally, modern programs may not have had time to mature within the Indian Armed Forces.

**DEFENCE**

India's response to a barrage of cyberspace threats has been slow and though progress is being made there are underlying issues which inhibit the protection of cyberspace power. There are three components in the Indian context which shed light on the Indian approach: the Indian population; the government structures intended to protect the Indian populace and their interests; and finally the role and capabilities within the Ministry of Defence (MoD), with special emphasis on the Defence Cyber Agency (DCA).

**Background**

A nuance between cybersecurity and cyberspace defence is important to understand. Cybersecurity is focused on general measures to improve overall posture and reduce the likelihood of any incident (such as anti-virus software use to prevent crimeware or supply chain audit to prevent firmware infections).[6] Cyberspace defence operations are measures taken to respond specific incidents (such as neutralizing the source of an attack). With this distinction there are two key realizations. Firstly, cybersecurity and cyberspace defence are very closely related. Though national defence has an interest in cybersecurity the onus is not exclusively on them. The populace and other government structures bear some responsibility for cybersecurity and thus the Indian MoD has a tilted responsibility to respond to specific, vice general, threats. Secondly, the more a nation's cyberspace is secure, the easier it is to defend.

In this new world of global transition and information age warfighting domains, India is acutely experiencing a cybersecurity and cyberspace defence crisis.

[6] Crimeware examples include ransomware which encrypts a users computer and promises decryption for a price or malware which takes compromising pictures while visiting adult sites. Supply chain threats include manufacturers embedding backdoors within the hardware of the system as opposed to the software.

Cybersecurity experts at Symantec rank India as the second most vulnerable to cyberspace attack.[7] India's Cyber Emergency Response Team (CERT) experienced a year over year growth in incidents of over 50%, rising from 7 million to 13 million between 2013 and 2014 alone, with a 121% rise in losses.[8]

None of this is new, India has been aware of and subject to several cyberspace campaigns. Looming large in the region, China continues to conduct multiple campaigns against India;[9] in one example China re-purposed Stuxnet, a highly advanced malware, to degrade India's satellite communications.[10] In fact, defence officials are quoted as saying, "there is enough proof that [China has] a desire to damage our infrastructure in the future."[11] Pakistan, a perennial foe contesting the fate of Jammu-Kashmir, has executed both sophisticated and rudimentary campaigns against India. As early as 1998, Pakistan's Inter-Services Intelligence agency infiltrated India's nuclear program[12] and more recently, Pakistani nationals, in response to a border skirmish, defaced several Indian police and government websites.[13] Furthermore, as shockingly disclosed by Edward Snowden and causing significant concern in India, even the US's National Security

---

[7] Reda Baig, "Could Offensive Cyber Capabilities Tip India and Pakistan to War?" *The Diplomat,* https://search-proquest-com.cfc.idm.oclc.org/docview/2196606248?accountid=9867.

[8] E. Dilipraj, "*Cyber Enigma : Unravelling the Terror in the Cyber World*," Milton: Routledge. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail. action?docID=5784853, 189; Statista, "Total Number of Cyber Crimes Reported in India in 2018," last accessed 29 April 2020, https://www.statista.com/statistics/309435/india-cyber-crime-it-act/; and, Statista, "Cyber crime in India – Statistics and Facts," last accessed 29 April 2020, https://www.statista.com/topics/5054/cyber-crime-in-india/.

[9] ThaiCert, "Threat Group Cards: A Threat Actor Encyclopedia," last accessed 30 April 2020, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 27, 63, 75, 94 et al; and Crowd Strike, "Global Threat Report: 2020," 51.

[10] The Diplomat, "India's Response to China's Cyber Attacks," Last Accessed 2 April 2020, https://thediplomat.com/2019/07/indias-response-to-chinas-cyber-attacks/. The use of Stuxnet here is noteworthy; China demonstrated an ability to understand and modify a highly complex and power malware.

[11] The Economic Times. "Cyber Defence: How Prepared is India for Cyber Warfare," last accessed 4 May 2020, https://economictimes.indiatimes.com/tech/internet/cyber-defence-how-prepared-is-india-for-cyber-warfare/articleshow/19152928.cms.

[12] Dilipraj, 217.

[13] The Northlines, "How India-Pakistan Hackers Escalated Cyber War Post Surgical Strikes," https://search-proquest-com.cfc.idm.oclc.org/docview/1828174993?accountid=9867.

Agency has executed operations targeting India.[14] India's nuclear power program remains under attack, noting that a North Korean associated group has also been attributed as having ex-filtrated data.[15] Cybersecurity, though in development, is certainly something that India has been aware of for a very long time, their response is much more recent.

**Indian Populace**

At the individual level in India, there is low cybersecurity expertise and ability. There is an understandable lag between digitization, the uptake of information technologies and the realization of the concerns and threats that need to be addressed. In India's case here are several aggravating factors requiring attention. Firstly, India's digital economy is growing quickly and is expected to grow into a trillion-dollar sector of the Indian economy.[16] This in itself is remarkable given that the first Indian computers were derided and seen as potentially exacerbating unemployment – they are now seen as a solution to it.[17] Secondly, the anti-virus market in India is expected to grow by nearly 15% annually, though positive, this demonstrates a woefully unsaturated, unsecure society.[18] Furthermore despite an increasingly educated workforce, India is short hundreds of thousands and cybersecurity specialists, including reverse engineers.[19] This inhibits the security and defence sectors from being able to recruit professional talent to

---

[14] Russian International Affairs Council, "India in the Era of Cyber Wars," last accessed 2 April 2020, https://russiancouncil.ru/en/analytics-and-comments/analytics/india-in-the-era-of-cyber-wars/.

[15] Stephanie Findlay and Edward White, "India Confirms Cyber Attack on Nuclear Power Plant," *FT. Com,* https://search.proquest.com/docview/2310816105?accountid=9867.

[16] Aliberti, 255.

[17] Dilipraj, 201.

[18] 6WResearch, "India Antivirus Market to Grow Amidst Emerging Wave of Technologies and Massive Rise in Cybercrimes," last accessed 29 April 2020, https://www.6wresearch.com/press-release/india-antivirus-software-market-share-forecasts-size-growth-opportunity-shipments-cagr-players-trends-news-company-profile.

[19] PCQuest, "India to Prepare Army of Reverse Engineers to Counter Cyber Attacks," last accessed 5 April 2020, https://search.proquest.com/docview/1519705808?accountid=9867. Reverse engineers are essential in cyberspace defence. It is their skillset which uncovers the nature, capabilities and origin of the discovered malware; defeat of sophisticated malware is dependent on understanding its behaviors.

detect and respond to cybersecurity incidents.[20] Combined, these factors expose India as vulnerable to cyberspace espionage and attack. Tellingly, though there is significant investment in cybersecurity ($2 billion USD), the overall numbers are still much less than the value of the cybercrime market ($18.5 billion USD);[21] India will likely remain vulnerable to infiltration by modern, advanced cyberwarfare practitioners and cyber-criminals alike.

**Indian Government**

The Indian government is now well aware of the above challenges and has implemented reforms to address the deficiencies. These reforms are largely organizational. India has created more entities to address cybersecurity and defence, such as the DCA as recommended in the National Security Policy 2013,[22] and has allowed certain other ones to adopt a limited leadership role. However, India has not achieved coherence in these efforts.

In a democratic nation as large as India, it is understandable that there would be a number of stakeholders in national cybersecurity and defence policy; the issue is the overlapping nature of the stakeholders. The Prime Minister's Office (PMO) is responsible for the National Critical Information Infrastructure Protection Center (NCIIPC) whereas the Ministry of Electronics and Technology (MEITY) is responsible for the Computer Emergency Response Team-India (CERT-India) as well as the National Cybercrime

---

[20] Dilipraj, 221.

[21] CISO, "Enterprise Information Security Spending in India to Reach US$1.9 Billion by 2019: Gartner," last accessed 29 April 2020, https://ciso.economictimes.indiatimes.com/news/enterprise-information-security-spending-in-india-to-reach-us1-9-billion-by-2019-gartner/65604570; and, Dilipraj, 189.

[22] India, Ministry of Communication and Information Technology, "National Cyber Security Policy, 2013," last accessed 2 April 2020, https://meity.gov.in/content/national-cyber-security-policy-2013-1.

Coordination Center (NCCC). It is not clear who shows leadership and would be responsible to respond to cyberspace incidents and intrusions.

Exacerbating these overlaps, the Ministry of Home Affairs (MHA) is responsible for internal security and the MoD, largely through the DCA, is responsible for national security – who then takes the lead when the threat actor originates from outside India. Furthermore, the MoD is also conducting research into defence and security technologies, benefiting all, and also has a CERT structure.[23] Though the Indian and MoD CERTs could be leveraged as a nascent cyber defence capability they are mostly employed in an audit and forensics capacity; they are not responsible to respond to nor defeat intrusions, merely analyze the consequences thereof.[24] It should be taken as concerning that even Russian writers have commented on the preponderance of red tape and inability to mobilize resources and achieve effective outcomes.[25] The issue with the Indian bureaucracy is that it is, "tumultuous" and "confusing"; India's cybersecurity landscape is comprised of dogmatic fiefdoms which are not optimized for a collective, unified response.[26]

Despite the organizational challenges, MEITY appears to be taking some steps to improve the cybersecurity posture of Indian people and businesses. In direct response to the rise in cybercrime and in acknowledgement of the importance of anti-virus software use by Indians, MEITY provides, free of cost, an anti-virus solution accessible through

---

[23] Thapar Shuchita, "Mapping the Cyber Policy Landscape: India," Global Partners Digital, Februrary 2016, 9-13.

[24] Lieutenant General RS Panwar, "Towards and Effective and Viable Information Warfare Structure for the Indian Army," *The United Service Institution of India*, last accessed 2 April 2020, https://usiofindia.org/publication/usi-journal/towards-an-effective-and-viable-information-warfare-structure-for-the-indian-armed-forces/.

[25] Russian International Affairs Council, "India in the Era of Cyber Wars."

[26] Dilipraj, 223.

Internet Service Providers and banks.[27] MEITY has also mandated that businesses spend 10% of their Information Technology budgets on cybersecurity.[28] Unfortunately, that the Indian government must implement these programs is evidence of a lack of cybersecurity mindedness in India and thus of a persistent vulnerability.

A legal and policy challenge to address is the degree to which India's defence and security organizations coordinate responses and share information, not just internally but within the region.[29] In order to exert influence in cyberspace, India must intimately share threat intelligence with its allies. India has been active in the space and has established a large number of bi-lateral agreements with regional nations including Japan, Australia, Russia and Singapore as well as with the United States – an agreement which includes sharing of encryption technologies.[30] In order to establish itself as a regional cyberspace defensive power, India should continue to resolve internal inefficiencies whilst, as recommended, lead in the creation of a multinational center to aid in sustained and continuous sharing of threat information.[31]

**Ministry of Defence**

From a military perspective, the recently formed DCA is the centerpiece of evolving Indian cyberspace doctrine and capabilities. However, albeit confused and

---

[27] The Economic Times, "Government Launches Free Anti-Virus for PC, Mobile Phones," last accessed 29 April 2020, https://economictimes.indiatimes.com/tech/internet/government-launches-free-anti-virus-for-pc-mobile-phones/articleshow/57273608.cms.

[28] 6WResearch.

[29]The Diplomat, "India's Response to China's Cyber Attacks."

[30] Monch Publishing Group, "New Agreement Gives India Access to High-End US Defence Technology," last accessed 29 April 2020, https://www.monch.com/mpg/news/security/4109-bilateral-collaboration-us-india.html; Electronics Bazaar, "Cyber Attacks can Derail India from Projected Growth," Sep 04, 2017, https://search-proquest.com.cfc.idm.oclc.org/docview/1934993591?accountid=9867.

[31] United Nations Institute for Disarmament Research (UNIDIR), "Cyber Policy Portal: India," last accessed 2 April 2020, https://cyberpolicyportal.org/en/states/india; and, "The Diplomat, "India's Response to China's Cyber Attacks."

inefficient, the national institutions already have the responsibility for most of the defense of national cyberspace. This leaves the DCA with a more parochial, internal security mandate for MoD capabilities.[32] Not surprisingly then, the DCA and the Indian Armed Forces are more focused on offensive operations.[33]

The greatest challenge for India's military is governance and doctrine; it is difficult to build capabilities and train personnel on defence operations without a clear understanding of how they can (and cannot) execute given cyberspace defence (vice cybersecurity) duties. This is seen the lack of doctrine for preventative or proactive defence in the current Indian construct. Responsive doctrines being well beyond the scope of the current passive CERT cybersecurity paradigm. There is almost no commentary on actively pursuing and countering adversary operations within India. As will be examined later, there are offensive operations executed in response to Pakistani incidents, but these have not included technical operations to specifically and deliberately disrupt or degrade an attack.

Notwithstanding the above doctrine gap, there has been some work and emphasis on developing and improving the capabilities within India though the focus is anything but military application.[34] From a defensive perspective this is equivalent to a 'build it and they will come' strategy. Furthermore, there is a risk that proposed capabilities will

---

[32] In the Canadian context this is similar to the Canadian Forces Network Operations Center's role for the |Canadian Armed Forces wherein it is responsible to defend only certain networks and does not have a national defence mandate, this being part of the Communication Security Establishment's mandate under Bill C-59 to defend Canadian cyber approaches and critical cyber infrastructure.

[33] Kartik Bommakanti, "Electronic and Cyber Warfare: Comparative Analysis of the PLA and the Indian Army," Observer Research Foundation Occasional Paper, Last accessed 2 April 2020, https://www.orfonline.org/research/electronic-and-cyber-warfare-a-comparative-analysis-of-the-pla-and-the-indian-army-53098/, 19.

[34] Bommakanti, 19.

fall prey to the 'hype cycle.'[35] For example, there is a lot of hype regarding the impact of artificial intelligence and quantum technologies to the extent that there is the incorrect belief that quantum cryptography will be the ultimate maker and breaker of cryptography rendering all encryption obsolete.[36] Accepting that the DCA and its sister organizations adopt this strategy, great care will be required to avoid wasting limited resources and expertise on ill-informed or impractical solutions.

India is implementing measures to address its astoundingly poor cybersecurity posture, however foundational issues linger. Effective capability and doctrine development, and especially threat intelligence sharing are all contingent on a harmonizing the national structures around which economic growth, and thus global power, can be assured. Though the citizenry bears some responsibility the weight of the responsibility is on the Indian government; until it addresses the organizational gaps and overlaps India will not be able to effectively secure and defend even its own cyberspace from its adversaries.

**SIGINT**

Having detailed the challenges in India's cyberspace defence posture an analysis of India's cyberspace intelligence follows. As with cyberspace defence there are positive indications of India's growth and maturation. However, after reviewing India capabilities and doctrine it will be seen that India is challenged here as well, lacking significantly in capacity and sophistication for a nation of its size.

---

[35] The hype cycle is a conceptual model developed by the Gartner group to describe the adoption of technologies. Inflated initial expectations fall prey to disillusionment after which more modest, sustainable understanding is achieved. See also https://en.wikipedia.org/wiki/Hype_cycle

[36] TechBeacon, "Waiting for Quantum Computing: Why Encryption has Nothing to Worry About," last accessed 29 April 2020, https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about; and, Bommakanti, 35.

**Background**

Though all intelligence functions are essential to a fulsome understanding of the threat environment and the adversary operations therein, this paper will focus exclusively on Signals Intelligence (SIGINT).[37] SIGINT is divided into several components, the largest of which are COMINT (intelligence derived from human communications, such as emails) and ELINT (intelligence derived from machine communications, such as radar). SIGINT spans both the electromagnetic spectrum and computer networks and as such is the preeminent intelligence function supporting cyberspace operations. SIGINT ability is closely linked to offensive cyberspace operations capability and thus is considered before offensive operations.

India has a long history executing SIGINT operations. As British colony, during WWII India hosted and participated in providing critical wireless intercept intelligence to Bletchley Park. Immediately after independence, during the wars with Pakistan, Indian SIGINT had tactical COMINT successes providing battlefield movements and Pakistani damage assessments.[38] Over time, and not unlike the current state of defense and security structures, India has developed an inefficient and "incoherent" array of SIGINT organizations.[39] There are roughly thirty intelligence agencies at the national level, eleven of which are in the MoD alone.[40] Despite a wide range of domestic and imported

---

[37] The other domains also value in cyber intelligence; for example: HUMINT operators may be able to infiltrate hostile agencies or the telecommunications sectors which support them. IMINT operators may provide highly valuable information about the communications systems in use at designated military facilities. Regardless, the primary source of relevant cyberspace intelligence is SIGINT.

[38] Desmond Ball, "Signals Intelligence (SIGINT) in South Asia: India, Pakistan Sri Lanka (Ceylon)," Canberra Papers on Strategy and Defence No. 117, The Australian National University, Canberra, 3-40.

[39] Ball, 16.

[40] International Business Publications, *India, A "Spy" Guide,* (Washington: International Business Publications, USA), 76,79.

capabilities, due to the wide span of agencies India is unable to fully coordinate and deconflict its efforts. Regardless, there are positive indications of Indian SIGINT potential, though these fall below the expectations of even a regional power.

**Capabilities**

From a capabilities perspective, the Indian military is reasonably well positioned. India continues to invest in highly capable systems, albeit at capacity levels below what one would envisage for such threatened and wealthy country.

Each service within the India armed forces has their own SIGINT capability. As can be expected, the Indian Navy and Air Force have a force protection requirement to detect and locate hostile radar emissions which drives a focus on ELINT capabilities. Additionally though, select Indian naval vessels are equipped with COMINT capabilities, aiding in force protection requirements.[41] The Indian Army hosts India's largest SIGINT agency.[42] The Army also, largely through their Electronic Warfare (EW) units conducts a range of tactical SIGINT activities focused on ELINT and EW functions such as Electronic Sense. The Indian Air Force is quite capable and despite a focus on ELINT and radar detection is continuing to pursue highly capable aircraft able to collect against VHF, UHF, and SHF frequency bands.[43] Unfortunately, the recent proposal was reduced from nine to seven aircraft; a quite small number for a nation with the third largest GDP. In addition to terrestrial technologies, India has a space-based SIGINT. Much of the

---

[41] Ministry of Defence, "Annual Report 2015-2015," 86-87

[42] Ministry of Defence, "Annual Report 2015-2016," Government of India, 2016, 87; and, International Business Publications, *India, A "Spy" Guide*, 80.

[43] Monch Publishing Group, "EW/C4I: Indian Air Force in the Market for a New SIGINT Aircraft," last accessed 29 April 2020, https://www.monch.com/mpg/news/ew-c4i-channel/5412-indiansigint.html. VHF is used for tactical communications and broadcast signals; UHF for microwave communications, cellular communications and mobile devices; and SHF for radar and satellite communications.

focus of space-based SIGINT, as with the other services, is on ELINT. There are however indications of COMINT collection but because the orbits will restrict collection to the Indian sub-continent, the posture will be at most a regional.[44] ELINT and radio-frequency COMINT are very location centric whereas network based COMINT is better able to provide intelligence from across the world, considering this it is clear that the Indian Armed Forces are addressing cyberspace intelligence requirements for its approaches and for its border regions only.

The other modest success that should be supported is the domestic SIGINT industry. The Asia-Pacific region is expected to experience the fastest rise in defence spending on SIGINT technologies. For India this is partly driven by conflict and competition with the People's Republic of China and in part driven by domestic terrorism, having experienced nearly 1,000 terror incidents in 2017 alone.[45] Standing out as one of only three non-Western companies recently profiled, Rolta India is a jewel in the Indian SIGINT landscape, as is Bharat Electronics Limited.[46] These companies are clear evidence of the potential the India has, but has not fully realized in cyberspace.

**Doctrine**

Given the state of cyberspace defence in India it not surprising that the SIGINT posture and doctrine within the Indian Armed Forces is also challenged. Each service has their own SIGINT capabilities and therefore their own doctrine and priorities for the

---

[44] S. Chandrashekar, "Space, War, and Deterrence: A Strategy for India," *Astropolitics,* 14 (2-3): 141.

[45] Markets Insider, "Signals Intelligence (SIGINT): Worldwide Market Analysis & Outlook, 2019 to 2023 – Increasing Presense of Signals Intelligence in the Public Domain," last accessed 2 April 2020, https://markets.businessinsider.com/news/stocks/signals-intelligence-sigint-worldwide-market-analysis-outlook-2019-to-2023-increasing-presence-of-signals-intelligence-in-the-public-domain-1028031712.

[46] Ministry of Defence, "Annual Report 2015-16," 61; and, Markets Insider, "SIGINT Worldwide Market Analysis."

employment of SIGINT. This results in insufficient coordination between responsible organizations. The Observer Research Foundation identified the continued low integration of intelligence and operations within the Indian Armed Forces and specifically notes that,

> there is inadequate interaction between the Indian Army Training Command (ARTAC), which is responsible for formulating and updating service doctrine, and all the technical entities such as the Defence Intelligence Agency (DIA), the Corps of Signals, the Defence Information Assurance and Research Agency (DIARA), and the National Technical Reconnaissance Organization (NTRO).[47]

Counter-acting this, the highly accomplished Lieutenant General Panwar clearly defines specific issues within the Indian Army and its EW and Cyber Warfare posture and makes several recommendations, including to formally group EW with ELINT, deploying these capabilities forward with requisite mobility to support tactical operations, and urgently to revise SIGINT doctrine and training to include Cyber Warfare and EW.[48]

In-line with multinational cybersecurity agreements, India is a member of SIGINT Seniors Pacific, a US led body of seventeen SIGINT agencies with an interest in Asia.[49] SSPAC was originally formed to facilitate the sharing of terrorism related intelligence and thus provides benefit to India. India's membership here though is not equal and in fact was jeopardized as a result of unprofessional, repeated disclosures of US intelligence in response to the Mumbai bombings.[50]

---

[47] Bommakanti, 21 and 27.

[48] Lieutenant General RS Panwar, "Towards and Effective and Viable Information Warfare Structure for the Indian Army," The United Service Institution of India. last accessed 2 April 2020. https://usiofindia. org/publication/usi-journal/towards-an-effective-and-viable-information-warfare-structure-for-the-indian-armed-forces/. Lieutenant General Panwar holds PhDs in Computer Science and Engineering and had a long career in Communications, Electronic Warfare and Intelligence.

[49] Securitipedia, "SIGINT Seniors," last accessed 30 April 2020, http://securitipedia. com/terms/s/sigint-seniors/.

[50] The Intercept, "The Powerful Global Spy Alliance You Never Knew Existed," last accessed 30 April 2020, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.

At the MoD level, India has a certain ability to conduct SIGINT operations, in particular network based COMINT. Regarding India's Advanced Persistent Threats (APT), it remains clear that for a country of India's size, it is underperforming.

Though India's APT conduct operations their scope, scale and complexity are limited; significant growth in Indian capacity and capability is needed. India's two primary APTs are focused on Pakistan and the ongoing inter-state conflict and terrorism in Jammu-Kashmir. A third Indian APT conducts operations against Pakistan and China, targeting the government and defense sectors.[51] Though achieving a certain level of results, Indian APTs are not typically observed using creative toolsets and techniques. In fact, Indian APTs are routinely detected using previously seen, even if indigenously developed, exploits and malware even going so far as to have been using open-source exploits or purchasing malware.[52] In comparison, Russia has six APTs, China has nine APTs all of whom are known for innovative tools and techniques and all of whom achieve substantive results.

India's doctrine of dependence on unsophisticated, open source or sub-contracted capabilities is inhibiting the ability of their under resourced APTs to achieve success. Within Indian conventional forces, despite tactical capabilities and domestic industry, lack of unity and coherent doctrine continue to inhibit realization of Indian SIGINT potential. It is clear that India is likely to remain locally and tactically focused in their

---

[51]Crowd Strike, "Global Threat Report: 2020," last accessed 2 April 2020, https://www.crowdstrike. com/resources/reports/2020-crowdstrike-global-threat-report/, 61; and, Center for Security Studies (CSS), "Hotspot Analysis: Regional Rivalry Between India-Pakistan: Tit-for-tat in Cyberspace", Cyber Defence Project, Zurich: August 2018, 4; and ThaiCert, "Threat Group Cards: A Threat Actor Encyclopedia," last accessed 30 April 2020, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf.

[52] CSS, "Hotspot Analysis," 9.

SIGINT operations and thus will not be able to leverage SIGINT to protect and project Indian cyberspace interests.

## OFFENSE

Having considered the state of Indian cyberspace defence and cyberspace intelligence, the last component to analyze is the Indian ability to conduct offensive cyberspace operations. This examination will show that though India has demonstrated a limited, tactical ability in offensive cyberspace operations it has not demonstrated this ability at the military-strategic level and certainly not to the level of government led strategic deterrence.[53]

### Background

Before delving directly into offensive operations, those which cause an effect on the enemy, an appreciation of the relationship between SIGINT and offensive cyberspace operations is important. The reason that SIGINT is a pre-condition for offensive cyberspace operations is two-fold. Firstly, SIGINT is required to shape and inform exactly what should be targeted – that is, targets in cyberspace are identified through cyberspace intelligence, namely SIGINT. Secondly, SIGINT tools are often readily adapted for use as part of a cyberspace operations campaign, particularly for tools used against common Information Technology systems such as cell phones.[54] Given this, the maturity and execution of Indian SIGINT operations foreshadows the nature of Indian offensive cyberspace operations. Finally, since India is only in strategic conflict with

---

[53] Though lesser than the Mutual Assured Destruction doctrine (MAD) of the Cold War there is a growing understanding that offensive operations can be equally met with nationally debilitating cyberspace operations, much of it potentially undisclosed and officially unattributed to the parties of the conflict.

[54] Though the tools and techniques can be very similar the quintessential difference is the intent. SIGINT seeks no change in target behavior whereas offensive operations do. As well, once a network is compromised by SIGINT techniques it is trivial to conduct additional tasks beyond the exfiltration of information to deliver an effect, such as destroy (delete) information.

Pakistan and China, there is no expectation that Indian offensive cyberspace operations would be observed outside these theatres.

**Capabilities**

There have been a number of documented Indian cyberspace operations and capabilities. The majority of operations have been executed against Pakistan, particularly as part of the 'proxy war' in Jammu-Kashmir. These operations have not been very sophisticated. In general they are comprised of low-grade defacements of Pakistani government and military web sites.[55] Though of limited technical complexity, these operations are intended to have an affect on the populace and would fit within the conduct of a broader Information War. Unfortunately, it is clear that more sophisticated operations to combat Pakistan and the terrorists that it supports are beyond India's capabilities; capabilities it has professed to be seeking but has not obtained.[56] This is made obvious by considering the recent complete internet blackout imposed by India on Jammu-Kashmir and the statements of Indian's Foreign Minister Jaishankar questioning, "how do I cut off communications between the terrorists and their masters on the one hand but keep the Internet open for other people?"[57] There are other methods, such as: compromising threat actor communications devices (phones, computers, radios) to execute disruption operations;[58] or, even the more blunt act of blocking selected threat actor communication accounts (ie WhatsApp, Facebook, etc) – any of these options

---

[55] The Northlines, "How India-Pakistan Hackers Escalated Cyber War Post Surgical Strikes."

[56] *Indian Army Land Warfare Doctrine,* Army Headquarters, New Delhi 2018, p.10 in Bommakanti, 20-21.

[57] The Washington Post, "India's Internet Shutdown in Kashmir is the Longest Ever in a Democracy," last accessed 29 April 2020, https://www.washingtonpost.com/world/asia_pacific/indias-internet-shutdown-in-kashmir-is-now-the-longest-ever-in-a-democracy/2019/12/15/bb0693ea-1dfc-11ea-977a-15a6710ed6da_story.html

[58] Disruption operations could include blocking threat actor communications by modifying posted content, re-directing undesired content, or 'bricking' the device.

would have degraded the threat while protecting that Jammu-Kashmir populace. Furthermore, this is also evidence of an ineffective SIGINT capability; the Intelligence loss from such as drastic measure would have been high, but only if there had been pervasive SIGINT operations. Considering the state of Indian SIGINT and doctrine and capability development, this is no surprise.

**Doctrine**

Indian armed forces doctrine for the employment of offensive cyberspace operations, like its defensive and SIGINT counter-parts is also immature. Aside from capability development there are two main challenges facing the Indian Armed Forces: the role of the DCA and the relationship between Cyberwarfare, EW and Information Warfare. The DCA is organizationally separate from the services, reporting through the Inter-Services Division, resulting in reduced authority and influence.[59] This organizational distance is problematic, especially in light of the historic self-contained nature of the services and the 'autonomy' that each has enjoyed.[60] Furthermore, despite a trend in many nations towards establishing a co-equal branch of the armed forces, there is no such discussion in India.[61] These structural issues are likely influenced by the balkanization of Indian doctrine for cyberspace, EW and SIGINT operations.[62] The Indian Navy and Air Force remain focused on operations to support their own needs, in particular counter-radar operations.[63] Consequently, ceding any perceived authority or autonomy would also be perceived as infringing on their bespoke operations. Conversely,

---

[59] Bommakanti, 24.

[60] Russian International Affairs Council, "India in the Era of Cyber Wars."

[61] Bommakanti, 31; and, Lieutenant General Panwar; and, The Northlines, "How India-Pakistan Hackers Escalated Cyber War Post Surgical Strikes. "

[62] Bommakanti, 20.

[63] Ibid, 26.

though service specific operations are important, as with the historical kinetic domains, the sum is greater than the parts, and without closer integration and mutual support between services (and with the DCA and its associates) the Indian Armed Forces will continue to have unmet potential.[64] That which could drive closer integration of the services and the DCA would be a review of Indian doctrine with a view acknowledging that much of EW and offensive cyberspace operations are quite similar – this being the crux of Lieutenant General Panwar's recommendations.[65]

Though doctrine informs capability development, the converse is also true. Thus, it is encouraging to note that the earlier referenced SIGINT aircraft is also expected to carry offensive capabilities, being able to, "[introduce] misleading or false information into an adversaries' communications."[66] This is a marked departure from a purely ELINT capability and demonstrates a shift in Indian thinking, albeit tactical and likely focused on counter-terrorism operations in Jammu-Kashmir.[67]

Also inhibiting Indian development of offensive cyberspace capabilities is an overall lack of strategic doctrine or intent to develop offensive operations as part of strategic deterrence. Strategic deterrence speaks to the relationship between two states, and thus to be effective the deterrence must be organized around a coherent and cohesive national effort – an effort which would require political will and clear responsibilities of stakeholder organizations.[68] In the case of cyberspace deterrence this would require

---

[64] Kevin Woods, and Thomas Greenwoodm, "Multidomain Battle: Time for a Campaign of Joint Experimentation," Joint Force Quarterly, no. 88 (January 2018): 15.

[65] Bommakanti, 8. There remains much literature on overlapping nature of Cyberspace Warfare, Electronic Warfare and Information Warfare. The issue in India is not how they perceive the overlaps; it is that they continue to see these as separate.

[66] Monch Publishing Group.

[67] Bommakanti, 31.

[68] Cherian Samuel and Munish Sharma, "*India's Strategic Options in a Changing Cyberspace,"* Pentagon Press LLP: New Delhi, 2019, 158.

significant improvements and investments in the capabilities and capacities of cyberspace defence (to block attacks) and SIGINT (to detect incursions and enable targeting) – as previously shown, this is unlikely. It is however not impossible. In being a nuclear power and in having been engaged in a series of escalatory and de-escalatory conflicts with Pakistan over Jammu-Kashmir there is a body of knowledge in the Indian Armed Forces to develop cyberspace deterrence policies. One of the first areas in which to conduct cyberspace deterrence should be as part of active cyberspace defence; by using sophisticated offensive toolsets to directly counter cyberspace aggression and/or adversary SIGINT operations, India will be able, at the military strategic and national level, defend itself in cyberspace.[69] This would fulfil the MoD's responsibility for national cyberspace defence and would offset the burden on the governmental and popular cybersecurity programs. By conducting active defence India would demonstrate to its adversaries its strength and willingness to defend itself from cyberspace espionage and cyberspace attack.[70]

In order to exert significant influence and power regionally in cyberspace, India must be able to project cyberspace power through the conduct of offensive cyberspace operations. Though rudimentary operations have been executed, much effort would be required to establish India as cyberspace power. Indian doctrine and organizational approach to offensive operations remains incoherent which in turns inhibits India's power. The overall Indian cyberspace theme of capabilities without structure or doctrine

[69] An aspect of many clandestine cyberspace operations is for the source to be obfuscated by operating in and through other countries. In this regard the risk to India of directly countering a Chinese SIGINT operation through action within a third country sends both a clear message but also does not require a direct response on Chinese territory and thus would be less likely to invoke a strong or overt Chinese response.

[70] Samir Saran, "Strategic Motivations for India's Cyber-Security: Risks, Capabilities and Promises," In 1st ed, 320-330: Routledge, 2018, 320.

is also evident in Indian offensive cyberspace operations. The lack of unifying strategy continues to prevent the realization of Indian potential, relegating its offensive cyberspace operations to limited and bluntly executed border skirmishes.

**COUNTER POINTS**

There are three primary counter arguments to the assertion that India's cyberspace operations capabilities are limited and regional at best. The first is that any analysis which does not include classified information will be a misrepresentation. The second is that though the current state of India's cyberspace operations capability is currently accurate, if given enough time, India will have a large dominant posture. The third essentially discredits the underlying situation, asserting that India is not at risk.

Indian classified material is not required to make a sound assessment of India's capabilities, arguments to the contrary bely several key facts and nuances. The fact is that cited the commentary regarding the deficiencies in Indian cyberspace operations, doctrine and capabilities are provided by experts in their field. Regardless, it is not even the existence of a capability which is highly classified, noting the openness of the contract for SIGINT and cyberspace operations aircraft, it is the specific techniques and instances in which they are to be employed which can be highly classified. Finally, recalling the number of Indian APTs there is no reason that cybersecurity experts would not detect supposed classified Indian operations while also detecting Chinese or Russian operations; in truth it is not even the number of APTs which is most important – it is the relative numbers and the relative sophistication of their tools, which was shown to be deficient.

Another counter argument is simply one of time. This paper has already outlined the significant growth that India will experience over the coming decades and how it will

be a global economic powerhouse. The rebuttal is merely that given time, India will have the capabilities and will be, at minimum, a global cyberspace powerhouse. This argument is not just wishful thinking; it ignores the reality of today. No national capability of that scope, scale, complexity and effectiveness can be grown that quickly without significant investments today. To whit, consider the space-based or airborne SIGINT program – if India is going to conduct global SIGINT operations it is reasonable to see that they would need a commensurate investment in space-based capabilities, investments which would need to be made now but for which there is no or even contrary evidence. Finally, it is not just a matter of investment, it is also a matter of overlapping and therefore conflicting priorities. And though some agencies, such as MEITY, are taking a certain leadership role, there would need to a major overhaul of the intelligence, security and defense structures to optimize Indian cyberspace operations – this would not be simple and therefore would not be quick. Finally, with an long enough view and with highly optimistic assumptions, almost anything *could* happen, however the crux of the argument is that given India's proven abilities and given its established development, Indian cyberspace power is *unlikely* to result in global power.

The final counter-argument that security is achieved by the strength of Indian democratic institutions.[71] This ignores several important realities. Firstly, a nation focused on defending itself will be necessarily resigned to local and parochial interests. Further, and the more serious flaw, no nation that is serious about cyberspace defence believes in the myth of unassailable democracies. The recent election interference campaigns conducted by Russian actors against America not only evaded sophisticated

[71] Jan Kallberg, "Assessing India's Cyber Resilience: Institutional Stability Matters," Strategic Analysis, 40:1, 1-5, DOI: 10. 1080/09700161. 2015. 1116252.

American cyberspace defences, but also targeted the very foundations of democracy; a 'wrongfully' elected government is most a risk of being at the center of domestic chaos.[72] That India may have some resilience to cyberspace attack by adversary nations does not imply that it should not actively expand its capabilities as a means to protect and ultimately project power – it certainly does not mean that India is secure.

**CONCLUSION**

Cyberspace operations are part of modern warfare. Nations seeking to be able to protect and project their power must have a capable cyberspace operations capability. India is no exception. By examining Indian ability in cyberspace defence, intelligence and offensive operations it was clearly established that what capacity India has is lacking both in scale and in sophistication. Defensively, India is mired in a confusing web of national agencies each of whom have some responsibility leaving the MoD's DCA with minimal responsibly. From the SIGINT perspective, though tactically there are sophisticated, modern ELINT and EW capabilities, at the national and MoD level the Indian ability to conduct advanced operations is woefully limited. Furthermore, as with the defensive posture, India is hampered by a large number of overlapping agencies. The SIGINT deficiencies persist through into the Indian cyberspace offensive capability, preventing sophisticated operations. Until India takes cyberspace seriously, perhaps through pursuit of cyberspace deterrence, their cyberspace posture writ large will be lacking. That is, Indian capabilities, structures, and focus are not optimized, constraining it to be a local power struggling even to establish a minimal level of cybersecurity. It is

[72] Noting that some citizens would support the government as legitimate, others as illegitimate and that as less popular decisions get made, these divisions could be readily exacerbated, if not fracturing a nation, certainly distracting it from global affairs.

clear that the Indian ability to protect and project power in cyberspace is limited and below what is required of a global power. The world is changing; India is not changing fast enough.

**BIBLIOGRAPHY**

6WResearch. "India Antivirus Market to Grow Amidst Emerging Wave of Technologies and Massive Rise in Cybercrimes." Last Accessed 29 April 2020. https://www.6wresearch.com/press-release/india-antivirus-software-market-share-forecasts-size-growth-opportunity-shipments-cagr-players-trends-news-company-profile.

Aliberti, Marco. 2018. *India in Space: Between Utility and Geopolitics*. Cham, Switzerland]: Springer. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1690971&site=ehost-live&scope=site.

Baig, Reda. 2019a. "Could Offensive Cyber Capabilities Tip India and Pakistan to War?" *The Diplomat*. https://search-proquest-com.cfc.idm.oclc.org/docview/2196606248?accountid=9867.

Baezner, Marie. *Hotspot Analysis: Regional Rivalry Between India-Pakistan: Tit-for-tat in Cyberspace*. Center for Security Studies. https://www.researchgate.net/publication/326866504_Regional_rivalry_between_India-Pakistan_tit-for-tat_in_cyberspace.

Bogdanoski, Mitko and Metodi Hadji-Janev. 2016. *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*. Hershey, PA: Information Science Reference. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1093980&site=ehost-live&scope=site.

Bommakanti, Kartik. "Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army." Observer Research Foundation Occasional Paper. Last Accessed 2 April 2020. https://www.orfonline.org/research/electronic-and-cyber-warfare-a-comparative-analysis-of-the-pla-and-the-indian-army-53098/

Brose, Robert. "Cyberwar, Netwar, and the Future of Cyberdefense," in M. Maybaum, A.M. Osula, and L. Lindström, eds., 7th International Conference on Cyber Conflict: Architectures in Cyberspace, Tallin: NATO CCD COE Publications, 2015, 25-38.

Bryant, Willam D. "Surfing the Chaos: Warfighting in a Contested Cyberspace Environment." Joint Force Quarterly, no. 8 (January 2018). 28-33.

Center for Strategic & International Studies. "Significant Cyber Incidents Since 2006." Last accessed 2 April 2020. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

Chandrashekar, S. "Space, War, and Deterrence: A Strategy for India." *Astropolitics* 14 (2-3): 135-157.

Cherian Samuel and Munish Sharma. *India's Strategic Options in a Changing Cyberspace*. Pentagon Press LLP: New Delhi, 2019.

CIOL. 2017. "India, Pakistan Braving State-Sponsored Cyber-Attack." *Ciol*. https://search.proquest.com/docview/1933469975?accountid=9867.

CIOL. "India, Pakistan Braving State-Sponsored Cyber-Attack." Last Accessed 3 April 2020. https://www.ciol.com/india-pakistan-braving-state-sponsored-cyber-attack/.

CISO. "Enterprise Information Security Spending in India to Reach US$1.9 Billion by 2019: Gartner." Last Accessed 29 April 2020. https://ciso.economictimes.indiatimes.com/news/enterprise-information-security-spending-in-india-to-reach-us1-9-billion-by-2019-gartner/65604570.

Crowd Strike. "Global Threat Report: 2020." Last Accessed 2 April 2020. https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/.

Defence Notes. "Pakistan and India: Cyber Security Strategy." Last Accessed 2 April 2020. https://www.academia.edu/7935735/Pakistan_and_India_Cyber_Security_Strategy.

Dilipraj, E. *Cyber Enigma : Unravelling the Terror in the Cyber World*. Milton: Routledge. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=5784853.

Dutta, Baishakhi. "Digital Drive Puts India at Greater Cyber Attack Risk." *Electronics Bazaar*, n/a. https://search.proquest.com/docview/1919499053?accountid=9867.

Electronics Bazaar. "Cyber Attacks can Derail India from Projected Growth." Sep 04, 2017. https://search-proquest-com.cfc.idm.oclc.org/docview/1934993591?accountid=9867.

Findlay, Stephanie and Edward White. "India Confirms Cyber Attack on Nuclear Power Plant." *FT.Com*: https://search.proquest.com/docview/2310816105?accountid=9867.

Government of Canada. JDN 2017-02, Canadian Armed Forces Joint Doctrine Note — Cyber Operations. Ottawa: Canadian Forces Warfare Centre.

IANS English. "India Witnessing Heavy Cyber Attacks from Russia, US, China." Last Accessed 3 April 2020. https://www.business-standard.com/article/news-ians/india-witnessing-heavy-cyber-attacks-from-russia-us-china-118111100285_1.html.

India, Ministry of Communication and Information Technology. "National Cyber Security Policy, 2013." Last accessed 2 April 2020. https://meity.gov.in/content/national-cyber-security-policy-2013-1.

International Business Publications. *India, A "Spy" Guide.* (Washington: International Business Publications, USA).

Journal of Current Issues in Globalization. "Global Trends 2030: Alternative Worlds." 2013a.*Journal of Current Issues in Globalization* 6 (1): 1.

Kallberd, Jan. "Assessing India's Cyber Resilience: Institutional Stability Matters." Strategic Analysis. 40:1, 1-5, DOI: 10. 1080/09700161. 2015. 1116252.

Keen, Jason F. 2015. "Conventional Military Force as a Response to Cyber Capabilities: On Sending Packets and Receiving Missiles." *The Air Force Law Review* 73: 111-150. https://search.proquest.com/docview/1717978773?accountid=9867.

Knowles, J. 2012. "India Seeks Ew and Sigint Aircraft." *Journal of Electronic Defense* 35 (5): 23. http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=75339276&site=ehost-live&scope=site.

Kumar, Satish. 2018. *India's National Security: Annual Review 2016-17*. London: Routledge India. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1693182&site=ehost-live&scope=site.

Lieutenant General Panwar, RS. "Towards and Effective and Viable Information Warfare Structure for the Indian Army." The United Service Institution of India. Last Accessed 2 April 2020. https://usiofindia.org/publication/usi-journal/towards-an-effective-and-viable-information-warfare-structure-for-the-indian-armed-forces/.

Markets Insider. "Signals Intelligence (SIGINT): Worldwide Market Analysis & Outlook, 2019 to 2023 – Increasing Presense of Signals Intelligence in the Public Domain." Last Accessed 2 April 2020. https://markets.businessinsider.com/news/stocks/signals-intelligence-sigint-worldwide-market-analysis-outlook-2019-to-2023-increasing-presence-of-signals-intelligence-in-the-public-domain-1028031712

Mint. "TechSagar, National Repository of India's Cyber Tech Capabilities Launched." 2019. *Mint*. https://search.proquest.com/docview/2307148379?accountid=9867.

Monch Publishing Group. "EW/C4I: Indian Air Force in the Market for a New SIGINT Aircraft." https://www.monch.com/mpg/news/ew-c4i-channel/5412-indiansigint.html.

Monch Publishing Group. “New Agreement Gives India Access to High-End US Defence Technology.” https://www.monch.com/mpg/news/security/4109-bilateral-collaboration-us-india.html.

Newstex. "Benzinga: FireEye Reveals Cyber Attacks on India, Neighbouring Nations." https://search.proquest.com/docview/1705641425?accountid=9867.

Newstex. “The Hindu Business Line: A Cashless Economy Needs Robust Cyber Security Capabilities: KPMG India Chief." Newstex, https://search.proquest.com/docview/1935589027?accountid=9867.

Nordquist, Keith B. “The New Matrix of War: Digital Dependence in Contested Environments.” Air & Space Power Journal 32, no. 1 (Spring 2018): 109-117.

North Atlantic Treaty Organization. *11th International Conference on Cyber Conflict: Silent Battle*. Tallinn, Estonia: NATO CCD COE Publications, 2019. https://ccdcoe.org/library/publications/11th-international-conference-on-cyber-conflict-silent-battle-proceedings-2019.

NPR. “How the U.S. Hacked ISIS.” Last Accessed 19 April 2020. https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

PCQuest. "India to Prepare Army of Reverse Engineers to Counter Cyber Attacks." Last Accessed 5 May 2020. https://search.proquest.com/docview/1519705808?accountid=9867.

Rehman, Iskander. "A Himalayan Challenge: India's Conventional Deterrent and the Role of Special Operations Forces Along the Sino-Indian Border." *Naval War College Review* 70 (1): 104-142. https://search-proquest-com.cfc.idm.oclc.org/docview/1861254501?accountid=9867.

Russian International Affairs Council. “India in the Era of Cyber Wars.” Last accessed 2 April 2020. https://russiancouncil.ru/en/analytics-and-comments/analytics/india-in-the-era-of-cyber-wars/.

Saran, Samir. “Strategic Motivations for India’s Cyber-Security: Risks, Capabilities and Promises.” In 1st ed, 320-330: Routledge. 2018.

Securitipedia. “SIGINT Seniors.” Last Accessed 30 April 2020. http://securitipedia.com/terms/s/sigint-seniors/.

Shuchita, Thapar. “Mapping the Cyber Policy Landscape: India.” Global Partners Digital, February 2016, 9-13.

Statista, "Cyber crime in India – Statistics and Facts," Last Accessed 29 April 2020. https://www.statista.com/topics/5054/cyber-crime-in-india/.

Statista. "Total Number of Cyber Crimes Reported in India in 2018" Last Accessed 29 April 2020. https://www.statista.com/statistics/309435/india-cyber-crime-it-act/.

TechBeacon. "Waiting for Quantum Computing: Why Encryption has Nothing to Worry About," Last Accessed 29 April 2020. https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about.

ThaiCert. "Threat Group Cards: A Threat Actor Encyclopedia." Last Accessed 30 April 2020. https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf

The Associated Chambers of Commerce and Industry of India, "India Security Summit: Towards New National Cyber Security Strategy." *Assocham Bulletin* 44, no 9 (September 2019). 36-38. https://www.assocham.org/defaultpage.php?pageId=62

The Diplomat. "India's Response to China's Cyber Attacks." Last Accessed 2 April 2020. https://thediplomat.com/2019/07/indias-response-to-chinas-cyber-attacks/.

The Economic Times. "Government Launches Free Anti-Virus for PC, Mobile Phones." Last Accessed 29 April 2020. https://economictimes.indiatimes.com/tech/internet/government-launches-free-anti-virus-for-pc-mobile-phones/articleshow/57273608.cms.

The Economic Times. "Cyber Attacks can Derail India from Projected Growth." Last Accessed 3 April 2020. https://cio.economictimes.indiatimes.com/news/digital-security/cyber-attacks-can-derail-india-from-projected-growth/60356379.

The Economic Times. "Cyber Defence: How Prepared is India for Cyber Warfare." Last Accessed 4 May 2020. https://economictimes.indiatimes.com/tech/internet/cyber-defence-how-prepared-is-india-for-cyber-warfare/articleshow/19152928.cms.

The Intercept. "The Powerful Global Spy Alliance You Never Knew Existed." Last Accessed 30 April 2020. https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.

The Northlines. "How India-Pakistan Hackers Escalated Cyber War Post Surgical Strikes." 2016. *The Northlines*. https://search-proquest-com.cfc.idm.oclc.org/docview/1828174993?accountid=9867.

Ullekh, N. P. 2013. "Cyber Defence: How Prepared is India for Cyber Warfare [Internet]." *The Economic Times*, n/a. https://search-proquest-com.cfc.idm.oclc.org/docview/1319764694?accountid=9867.

United Nations Institute for Disarmament Research (UNIDIR). "Cyber Policy Portal: India." Last Accessed 2 April 2020. https://cyberpolicyportal.org/en/states/india.

Warf, Barney, Fekete Emily. "Relational Geographies of Cyberterrorism and Cyberwar." Space and Polity, 20, 2 (2016): 143-157.

Woods, Kevin M., and Thomas C. Greenwood. "Multidomain Battle: Time for a Campaign of Joint Experimentation." Joint Force Quarterly, no. 88 (January 2018): 14-21.