India's International Cyber Operations:

Tracing National Doctrine and Capabilities

Arindrajit Basu

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study was produced by an external consultant on behalf of the Security and Technology Programme's Cyber Stability workstream, which is funded by the Governments of France, Germany, the Netherlands, Norway and Switzerland, and by Microsoft. Gratitude is extended to Alisha Anand, Andraz Kastelic, Giacomo Persi Paoli, Gunjan Chawla, Pukhraj Singh, Sameer Patil and Samuele Dominioni for offering their thoughts on this research paper.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

About the Author

ARINDRAJIT BASU is a Non-Resident Research Fellow at the Centre for Internet and Society, India.

TABLE OF CONTENTS

On the Research Paper Series

The number of States that possess the capability to conduct international cyber operations against or through foreign information and communications technology (ICT) infrastructure is on the rise. These cyber operations could signal a mounting large-scale threat to the security of States and be understood as a violation of sovereignty that may lead to an escalation.

To facilitate transparency, advance trust among States and thus promote stability in international cyberspace, the UNIDIR Security and Technology Programme commissioned a series of research papers outlining national capabilities to conduct international cyber operations and the relevant national doctrines regulating the conduct of such operations. In the resulting papers, 9 scholars and practitioners provide an overview of the capabilities and doctrines of 15 States across different regions: Australia, Brazil, Canada, China, France, Germany, India, the Islamic Republic of Iran, Israel, Japan, the Republic of Korea, the Russian Federation, Saudi Arabia, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

To read more about the research paper series, please refer to the "International Cyber Operations: National Doctrines and Capabilities" paper, available at www.unidir.org/cyberdoctrines.

Andraz Kastelic

Lead Cyber Stability Researcher,
Security and Technology Programme, UNIDIR

Background and scope

Cybersecurity has been recognized by Indian decision makers as a key foreign policy and security priority. However, at this stage, there has been no clear public articulation of any intention by India to conduct international cyber operations. There is no publicly known overarching declaratory doctrine, policy or legislative framework that captures India's strategic interests, ambitions and restraints in this arena. However, the cyber institutional machinery and policy landscape are evolving rapidly, with several new institutions set up in the last decade and several policies in the nascent stages of development or due to be released soon, including notably the National Cyber Security Strategy. Further, public statements by public officials on India's cyber doctrine and operations could serve as evidence of intent to conduct international cyber operations. Therefore, at this stage, India's present capabilities and strategy can be inferred from an informed analysis of existing State practice and institutional architecture and a combined reading of existing laws and policies.

For the purpose of this paper, "international cyber operation" refers to the use of cyber capabilities with the intention of advancing the defensive or offensive strategic objectives of a country or to project power in and through foreign cyberspace by "[compromising] the confidentiality, integrity, or availability of an adversary's information technology systems or networks; devices controlled by these systems or networks; or information resident in or passing through these systems or networks".[1]

This paper is divided into three sections. Section 1 unpacks India's institutional structure governing cybersecurity, focusing on entities that may be most relevant for articulating a governing doctrine or that possess the material capabilities for conducting international cyber operations. Section 2 explores domestic law and policy to identify evidence of India's capabilities, evaluating the conclusions through the analysis of secondary literature. Finally, section 3 evaluates military doctrines and statements made by public officials along with secondary literature to identify evidence on India's doctrine on international cyber operations.

From a methodological standpoint, this paper relies on desk research that includes the analysis of both primary sources (i.e., government policies and official statements) and secondary sources (including media reports and expert commentary). In line with its objective as a transparency-fostering exercise, this paper only relies on sources that are publicly available. To strengthen this approach, interviews discussing the paper and its implications were conducted with key stakeholders.

1 Lin and Zegart (2017, 2).

Institutions in India's cyber ecosystem

As noted, there is a lack of both clarity on India's capabilities to conduct international cyber operations and a clear relevant cyber doctrine. However, India has a robust cyber institutional set-up, which could provide indications of the developing capabilities and future doctrines. Understanding India's institutional structure could help understanding of the evolving framework of the doctrine and capabilities governing cyber international operations.

Broadly, four sets of institutions make up India's cyber ecosystem.[2] The first consists of defence institutions under the aegis of the Ministry of Defence (MOD). Second is the Prime Minister's Office, which advises the Prime Minister and coordinates the activities of several entities within its remit.[3] Third is the Ministry of Electronics and Information Technology (MeitY), which houses several cybersecurity institutions and agencies. Finally, the Ministry of External Affairs (MEA), India's foreign ministry, coordinates cyber diplomacy efforts. Although there is no public evidence to suggest that the MEA is involved in framing India's international cyber operations doctrine, statements made by MEA representatives at national, bilateral and multilateral forums remain relevant when determining India's capabilities to conduct international cyber operations and the relevant doctrine.

MINISTRY OF DEFENCE

The MOD oversees India's military capabilities and capacities in the cyber context through several entities within its remit.

The Defence Cyber Agency (DCA) is the most relevant MOD entity in terms of international cyber operations. The DCA was first announced by the Prime Minister at the Combined Commanders Conference in 2018, along with similar agencies for space and special operations.[4] In a written response to a parliamentary question, the Minister of State for Defence, Shripad Naik, stated that the DCA was set up to "control and coordinate the Joint Cyber operations".[5] Governed by the Integrated Defence Staff, the DCA draws 1,000 personnel from the three branches of the armed forces.[6] Media reports have stated that the DCA will be able to conduct cyber operations, including hacking, surveillance, laying honey traps and breaking into encrypted communications channels.[7] Retired army officials also expect the DCA to address challenges beyond conventional warfare and to articulate a cyber doctrine for the armed forces that would integrate cyberwarfare with conventional operations.[8] Similarly, external experts also herald the DCA as a key institution for upgrading India's attack techniques.[9]

2 Saslow, Ebert and Wetzling (2020, 10); Chawla (2020).
3 Saslow, Ebert and Wetzling (2020, 10).
4 ET Bureau (2018).
5 Ministry of Defence (2019).
6 Sagar (2019).
7 Sagar (2019).
8 Sagar (2019); Hooda (2019); Singh (2019).
9 Leyden (2021).

In addition, a number of armed forces entities have established Cyber Emergency Response Teams (CERTs).[10] According to Naik, the armed forces aim to ensure a "robust cyber posture" through cyber audits, physical checks and policy guidelines.[11] At the same time, the minister also ensured adequate budgetary allocation for "cyber operations and capability development".[12]

PRIME MINISTER'S OFFICE

The Prime Minister's Office, which works directly with and assists the Prime Minister, includes several agencies and key individual positions with a cyber portfolio, such as the National Cybersecurity Coordinator (NCSC).[13]

The National Technical Research Organisation (NTRO), set up in 2004, is a technical intelligence organization that directly reports to the National Security Advisor (NSA) in the Prime Minister's Office.[14] According to secondary sources, the NTRO has the capabilities to punish an act in cyberspace, including by taking countermeasures.[15] Reports emerged in 2012 that the NTRO was tasked with carrying out offensive cyber operations if necessary.[16] No public articulation of the NTRO's offensive capabilities or of policy governing the organization have emerged since then.

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

MeitY was established as a ministry in 2016.

The Indian Computer Emergency Response Team (CERT-In) falls within MeitY's jurisdiction.[17] It is tasked with responding to and mitigating cybersecurity threats while also coordinating with the CERTs of other countries. CERT-In's mandate is a proactive one as defined in the 2000 Information Technology Act and the 2013 CERT-In Rules.[18] The focus of this body is on forecasting and raising alert about cybersecurity incidents and on preventing such incidents.[19] The CERT-In Rules do not entrust this body with conducting any form of international cyber operation.

CERT-In also includes a multi-stakeholder cybersecurity agency, the National Cyber Coordination Centre (NCCC), that can track threats in cyberspace and coordinate the functioning of the various stakeholders in India's institutional set-up.[20] As stated by the MeitY in response to a question posed by the parliamentary Standing Committee on Information Technology, the NCCC was set up to "generate near real time macroscopic views of the cyber security threats in the country. The centre scans the cyberspace in the country at metadata level and generates near real time situational awareness."[21] The NCCC was expected to be fully operational by 2022[22] but there has been no confirmation of this at the time of writing.

MINISTRY OF EXTERNAL AFFAIRS

The MEA manages and coordinates India's cyber diplomacy efforts.[23] It has a cyber diplomacy division, which is tasked with representing India at bilateral and multilateral forums.

In addition, the New and Emerging Strategic Technologies (NEST) division was set up to "to engage in technology diplomacy and deal with the foreign policy and international legal aspects of new and emerging technologies".[24] It seeks to enable India's more active participation in global forums in the area of technology governance and to promote India's national interests in that context.[25] It also focuses on specific topics such as fifth-generation telecommunications (5G) and artificial intelligence (AI) technologies.[26]

---

10 Ministry of Defence (2019).
11 Ministry of Defence (2019).
12 Ministry of Defence (2019).
13 Saslow, Ebert and Wetzling (2020, 10).
14 Bedi (2015).
15 Samuel and Sharma (2019, 44).
16 Sridhar (2012).
17 Chawla (2020).
18 Deb (2019, 24).
19 Deb (2019, 24).
20 Saslow, Ebert and Wetzling (2020, 10). The Ministry of Home Affairs has also set up an Indian Cybercrime Coordination Centre (I4C) that focusses more on domestic cyber threats and works with law enforcement agencies to combat these threats.
21 Standing Committee on Information Technology (2021, 37).
22 Standing Committee on Information Technology (2021, 37).
23 Saslow, Ebert and Wetzling (2020, 10).
24 Ministry of External Affairs (2020).
25 Ministry of External Affairs (2019).
26 Chaudhury (2020).

Capabilities

This section explores India's capacity to conduct international cyber operations. It investigates the evidence for such a capacity by examining domestic law and policy related to international cyber operations as well as statements made by public officials in domestic and international forums.

EVIDENCE OF CAPABILITIES TO CONDUCT INTERNATIONAL CYBER OPERATIONS

Evidence of India's capabilities to conduct cyber operations remains scant, although a former NSA has publicly written that India has "considerable" capacity to conduct "extensive cyber sabotage and cyber warfare".[27] Reports by security researchers also support this assertion.[28] Although there is no explicit primary evidence of India carrying out concerted cyber operations against its adversaries,[29] Oxford Analytica notes that there has been an observed increase in cyber operations carried out by allegedly India-based non-State actors like 'Dropping Elephant'.[30] Analysis by Kaspersky Labs confirms this by stating that, although "there are indicators pointing to the fact that this actor operated from India ..., there is no solid proof ... that a nation-State might be involved in this operation".[31] Kaspersky Labs further states that the modus operandi is not sophisticated but instead relies on social engineering and simple but effective tools.[32]

No official Indian statement has acknowledged these actors, and the precise contours of the relationship between these actors and the Indian State are not publicly known. Broadly, these non-State actors can be characterized as hacktivists, patriotic hackers and Advanced Persistent Threats (APTs).[33] Allegedly, these groups have engaged in information operations such as espionage.[34] Their methods include hacking mobile phones and other gadgets of government and military officials and website defacement.[35]

27 Narayanan (2016).
28 Oxford Analytica (2018).
29 Singh (2020).
30 Oxford Analytica (2018).
31 Kaspersky (2016).
32 Kaspersky (2016).
33 ETH Zurich (2018). An APT is an attack campaign through which an intruder illicitly establishes a presence on a certain network to extract sensitive data.
34 See Fazzini (2019).
35 Khan (2020); Times of India (2019).

More recent evidence indicates that the armed forces may be considering building capacity and developing capabilities to conduct more sophisticated cyber operations. For example, in 2021, the Indian Army conducted its first hackathon to consolidate its cyber warfare capabilities.[36] The hackathon involved a number of challenges including secure coding, software-defined radio exploitation and cyber-offensive skills.[37]

DOMESTIC LAW AND POLICY

India's cybersecurity policy framework consists of a combination of different policies that could serve as evidence of intent to conduct international cyber operations.

National Cyber Security Policy (2013)

In June 2013, the Department of Electronics and Information Technology (now MeitY) promulgated India's first National Cyber Security Policy. The policy is quite abstract and mainly articulates broad guiding principles. However, it was instrumental in recommending the creation of several of the institutions that make up India's cybersecurity ecosystem, most notably the National Critical Information Infrastructure Protection Centre.[38] Moreover, the focus of the policy is restricted to creating a framework for responding to security threats (e.g., early warning and vulnerability management), pointing out the need to conduct regular cybersecurity drills and exercises, but it neither lays out a framework for these nor makes any reference to international cyber operations.[39]

National Cyber Security Strategy (in progress)

In 2019, the National Security Council Secretariat created a task force to develop a National Cyber Security Strategy. The strategy was supposed to be released in March 2020 but has been delayed due to the COVID-19 pandemic.[40] The task force sought inputs from the public in December 2019 to inform the contents of the National Cyber Security Strategy. The call for comments mentioned three pillars that the strategy will incorporate:

1. Strengthen national cyberspace;
2. Strengthen structures, people, processes and capabilities;
3. Synergize resources including through cooperation and collaboration.[41]

However, the call for comments does not indicate whether the new National Cyber Security Strategy would provide any information on the conduct of international cyber operations.

STATEMENTS BY PUBLIC OFFICIALS

A few statements by public officials in both domestic and international forums have hinted at the existence of capabilities to conduct international cyber operations or of the intent to develop them. In 2016, the Deputy NSA, Arvind Gupta, stated that "We [India] also need to closely analyse the patterns of cyber-attacks against us and build suitable response measures including the capability to conduct cyber operations if required."[42]

Further, in response to a parliamentary question in November 2019 on "whether the Government has taken steps and allocated funds to enhance the capability for undertaking offensive cyber warfare attacks", Naik, the Minister of State for Defence, stated that "[s]ufficient budgetary allocation is being provided for Cyber operations and capability development".[43] This is in line with a 2019 report by a think tank task force of veterans, which encouraged India to rapidly develop capabilities to conduct international cyber operations but urged India not to disclose them until the capabilities were in place.[44]

36 Times News Network (2022).
37 Times News Network (2022).
38 Ministry of Communication and Information Technology (2013).
39 Bhalla (2019).
40 Agrawal and Pahwa (2020).
41 Bhalla (2019).
42 Gupta (2016).
43 Ministry of Defence (2019).
44 VIF Task Force (2019, 110).

Doctrine

Gupta, the Deputy NSA, argued in 2016 that "India would need to take note of the increasingly assertive cyber security doctrines that are being adopted by other countries. This will help in working out our own cyber security doctrines."[45] To date, India is yet to articulate a doctrine for conducting international cyber operations. This section therefore relies on the analysis of publicly available military documents.

The clearest acknowledgment of cyberwarfare as a strategic necessity emerges from military doctrines, although these strategies stop short of articulating clear goals or red lines.

The Basic Doctrine of the Indian Air Force states that "[c]yber warfare is an attractive low cost war-waging model because it has some notable features such as: low entry cost, blurred traditional boundaries" and that "[o]ffensive cyber warfare can be conducted across the entire range of military and nonmilitary operations to achieve national objectives".[46] The document considers and evaluates cyberwarfare separately from information warfare, with no explicit links between the two.

The 2017 Joint Doctrine of the Armed Forces refers to both cyber defence and cyber offence, as it hints at the significance of offensive operations during military operations.[47] It states that "exploiting information technology and Integrated Reconnaissance, Surveillance and Command, Control, Communications, Computers, Information and Intelligence systems will win battles".[48] This could signal the acknowledgement of the utility of such capabilities when employed in tandem with existing military functions.

The 2018 Land Warfare Doctrine articulates the strategic necessity of cyber capabilities and stresses the need for cyber operations to augment existing military operations.[49] Referring to cyberwarfare as a subcategory of information warfare, it states that the Indian Army will develop capabilities to carry out information warfare operations over the "entire spectrum of conflict".[50] It further states that cyberspace will be a "key battle winning factor in future conflict" and "all elements/forces must retain the capability to fight through a disruptive Cyber Warfare domain/environment".[51] It also affirms that the Indian Army will upgrade its existing cyberwarfare capabilities while also "devising means of eliminating such threats".[52]

45 Gupta (2016).
46 Indian Air Force (2012, 132).
47 Headquarters Integrated Defence Staff Ministry of Defence (2017).
48 Headquarters Integrated Defence Staff Ministry of Defence (2017, 49).
49 Indian Army (2018).
50 Indian Army (2018, 1).
51 Indian Army (2018, 10).
52 Indian Army (2018, 10).

The Indian Navy's 2014 Vision Statement refers to conducting effective networked operations across multiple domains including cyberspace.[53] Further, the Indian Navy's Maritime Security Strategy recognizes the critical importance of cyberspace and cybertechnologies in India's security architecture.[54] The bibliography in this publication includes a 2013 document titled *Cyber Doctrine: Flag Officer Doctrines and Concepts*.[55] While this document is not in the public domain, its existence coupled with its inclusion in a report published by the Indian Navy indicates some thinking on a cyber doctrine among the naval establishment.

Overall, these documents shed light on the strategic thinking of the military establishment in terms of crafting India's national security posture. They clearly indicate a recognition that international cyber operations are becoming increasingly critical to military functions and a desire to implement "techno-centric combat".[56]

53 Indian Navy (2014, 6).
54 Indian Navy (2015, 134).
55 Indian Navy (2015, 181).
56 Indian Army (2018, 2).

Conclusion

This paper demonstrated that, despite the number of institutions and policies that work on India's cyber strategy, there is little public evidence of India's capabilities to conduct international cyber operations. Further, there is no clearly articulated public doctrine on the opportunities, challenges and restraints of international cyber operations by India.

It is possible that the upcoming National Cyber Security Strategy will provide some clarity. At present, any credible evaluation of India's strategy on international cyber operations must scrutinize a range of publicly available sources, as this paper attempts to do. However, India's approach to cybersecurity is rooted in its appraisal of strategic interests.[57] As these interests and threats evolve, India may more proactively disclose capabilities and frame a governing doctrine in order to robustly project power in cyberspace.

57 Basu and Nachiappan (2020).

References

Agrawal, Aditi and Pahwa, Nikhil. 2020. "Lt Gen. (Dr) Rajesh Pant on India's National Cyber Security Strategy, Indo-US cooperation, end-to-end encryption and more". *Medianama*, 2 June. As of 11 March 2020: https://www.medianama.com/2020/06/223-rajesh-pant-interview-national-cyber-security-coordinator

Basu, Arindrajit and Nachiappan, Karthik. 2020. "Will India negotiate in cyberspace?" Leiden security and global affairs blog. 16 December. As of 11 March 2022: https://www.leidensecurityandglobalaffairs.nl/articles/will-india-negotiate-in-cyberspace

Bedi, R.S. 2015. "NTRO: India's Technical Intelligence Agency". *India Defence Review*. 23 April. As of 11 March 2022: http://www.indiandefencereview.com/spotlights/ntro-indias-technical-intelligence-agency

Bhalla, Kritti. 2019. "Govt. calls for citizen feedback on National Cybersecurity Strategy". *Inc42*. 2 December. As of 11 March 2021: https://inc42.com/buzz/govt-calls-for-citizen-feedback-on-national-cybersecurity-strategy

Chaudhury, Roy Dipanjan. 2020. "MEA sets up emerging technologies division," *Economic Times*, 2 January. As of 11 March 2021: https://telecom.economictimes.indiatimes.com/news/mea-sets-up-emerging-technologies-division/73064250

Chawla, Gunjan. 2020. "The architecture of cybersecurity institutions in India". *Medianama*. 19 February. As of 11 March 2021: https://www.medianama.com/2020/02/223-architecture-cybersecurity-institutions-india-structure

Deb, Siddharth. 2019. "Towards a cyber-security roadmap for digital payments: Best Practices and Recommendations". *Observer Research Foundation*, 12 April. As of 11 October 2021: https://www.orfonline.org/wp-content/uploads/2019/04/ORF_Report_Roadmap_Digital_Payments.pdf

ET Bureau. 2018. "PM Narendra Modi attends Combined Commander's Conference in Jodhpur". *Economic Times*. 28 September. As of 11 March 2021: https://economictimes.indiatimes.com/news/defence/pm-narendra-modi-attends-combined-commanders-conference-in-jodhpur/articleshow/65996826.cms

ETH Zurich. 2018. "Regional rivalry between India-Pakistan: tit-for-tat in cyberspace". *CSS Cyber Defense Project*. As of 11 March 2021: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf

Fazzini, Kate. 2019. "In India–Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides". *CNBC Markets*. 27 February. As of 11 March 2021: https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html

Gupta, Arvind. 2016. "Keynote address by Dr Arvind Gupta, Deputy National Security Advisor at the 18th Asian Security Conference on 'Securing Cyberspace: Asian and International Perspectives.'" Manohar Parrikar Institute for Defence Studies and Analyses. As of 14 March 2021: https://idsa.in/keyspeeches/18asc-securing-cyberspace-asian-and-international-perspectives_deputy-nsa

Headquarters Integrated Defence Staff Ministry of Defence. 2017. *Joint Doctrine Indian Armed Forces*. As of 11 March 2021: https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf

Hooda, DS (Lt Gen Retd).2019." India's new defence cyber agency will have to work around stovepipes built by army,navy&air force". *News18.com*, June 26.As of November 7th,2022. https://www.news18.com/news/opinion/new-defence-cyber-agency-will-have-to-work-around-stovepipes-built-by-army-navy-air-force-lt-gen-hooda-2204033.html

Indian Air Force. 2012. *Basic Doctrine of the Indian Air Force*. As of 11 October 2021: https://www.scribd.com/doc/109721067/Basic-Doctrine-of-Indian-Air-Force-2012-PDF

Indian Army. 2018. *Land Warfare Doctrine*. As of 11 March 2022: http://www.ssri-j.com/MediaReport/Document/IndianArmyLandWarfareDoctrine2018.pdf

Indian Navy. 2014. *The Indian Navy's Vision Statement 2014*.

Indian Navy. 2015. *Ensuring Secure Seas: Indian Maritime Security Strategy*. Naval Strategic Publication (NSP) 1.2. As of 14 March 2022: https://www.indiannavy.nic.in/sites/default/files/Indian_Maritime_Security_Strategy_Document_25Jan16.pdf

Kaspersky. 2016. "Dropping Elephant: Cyber-espionage group hunts high profile targets with low profile tools". *Kaspersky*. As of 21 October 2021: https://www.kaspersky.com/about/press-releases/2016_dropping-elephant-cyber-espionage-group-hunts-high-profile-targets-with-low-profile-tools

Khan, Omar. 2020. "Pakistan army claims major cyber attack by Indian intel". *Times of India*, 13 August. As of 11 March 2021: https://timesofindia.indiatimes.com/world/pakistan/pakistan-army-claims-major-cyber-attack-by-indian-intel/articleshow/77515250.cms

Leyden, John. 2021. "Indian cyber-espionage activity rising amid growing rivalry with China, Pakistan". February 2021. *The Daily Swig*. As of 11 March 2021: https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan

Lin, Herbert and Zegart, Amy. 2017. "Introduction to the special issue on strategic dimensions of offensive cyber operations". *Journal of Cybersecurity* 3(1).

Ministry of Communication and Information Technology. 2013. *National Cyber Security Policy-2-13* (NCSP-2013). File No: 2(35)/2011-CERT-In. As of 11 March 2022: https://www.meity.gov.in/writereaddata/files/National%20Cyber%20Security%20Policy%20%281%29%20%281%29.pdf

Ministry of Defence. 2019. Cyber Warfare Threats. Lok Sabha Starred Question No.138. 27 November. As of 11 Match 2021: http://164.100.24.220/loksabhaquestions/annex/172/AS138.pdf

Ministry of External Affairs. 2019. *Statement delivered by India at the Organisational Session of the Open-Ended Working Group (OEWG) on 'Developments in the field of Information and Telecommunications in the context of International Security'* 3 June. As of 11 March 2021: http://meaindia.nic.in/cdgeneva/?8251?000

Ministry of External Affairs. 2020. "Question No.552 New and Emerging Strategic Technologies Division". 5 February. As of 14 March 2022: https://mea.gov.in/lok-sabha.htm?dtl/32359/QUESTION_NO552_NEW_AND_EMERGING_STRATEGIC_TECHNOLOGIES_DIVISION

Narayanan M.K. 2016. "The best among limited options". *The Hindu*, 1 November. https://www.thehindu.com/opinion/lead/The-best-among-limited-options/article14990381.ece

Oxford Analytica. 2018. “New players join race for offensive cyber capabilities”. *Oxford Analytica Daily Brief*. 20 August. As of 11 March 2021: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Egloff_2018_Oxford-Analytica-New-players-join-race-for-offensive-cyber-abilities-.pdf

Sagar, Pradip. 2019. “Three pronged-plan”. *The Week*. 1 June. As of 11 March 2021: https://www.theweek.in/theweek/current/2019/05/31/three-pronged-plan.html

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

Saslow, Kate, Ebert Hannes and Wetzling Thorsten. 2020. “Cyber resilience and diplomacy” *Digital Dialogue*. 14 July. As of 24 October 2021: https://eucyberdirect.eu/content_research/cyber-resilience-and-diplomacy-in-india

Singh, Nidhi. 2019. “India’s new defence cyber agency”. *The CCG Blog*. 10 May. As of 11 March 2021: https://www.medianama.com/2019/05/223-indias-new-defence-cyber-agency-nidhi-singh-ccg-nlud

Singh, Pukhraj. 2020. “On China, it’s time to consider cyber operation”. *Hindustan Times*. 23 June. As of 11 March 2021: https://www.hindustantimes.com/analysis/on-china-it-s-time-to-consider-cyber-operations/story-crMraUyDc64taDRHMhEnhP.html

Sridhar, R. 2012. “DIA and NTRO to head offensive cyber warfare wing of India”. *Defence Forum India*. 4 July. As of 11 March 2021: https://defenceforumindia.com/threads/dia-and-ntro-to-head-offensive-cyber-warfare-wing-of-india.38589

Standing Committee on Information Technology. 2021. *Demand for Grants (2021–22)*. Twenty-Fourth Report presented to the Lok Sabha.

Times of India. 2019. “Pulwama attack: Pakistani websites hacked, here’s the list”. *Times of India*. 18 February. As of 11 March 2021: https://timesofindia.indiatimes.com/gadgets-news/pulwama-attack-pakistani-websites-hacked-heres-the-list/articleshow/68042727.cms

Times News Network. 2022. “Army holds 1st hackathon to boost cyber warfare”. *Times of India*. 11 February. As of 11 March 2022: https://timesofindia.indiatimes.com/india/army-holds-1st-hackathon-to-boost-cyber-warfare/articleshow/89490444.cms

VIF Task Force. 2019. *Credible Cyber Deterrence in Armed Forces of India*. Vivekananda International Foundation. As of 11 March 2022: https://www.vifindia.org/sites/default/files/Credible-Cyber-Deterrence-in-Armed-Forces-of-India_0.pdf

India's International Cyber Operations:

Tracing National Doctrine and Capabilities

Cybersecurity has been recognized by Indian decision makers as a key foreign policy and security priority. However, at this stage, there has been no clear public articulation of any intention by India to conduct international cyber operations.

There is no publicly known overarching declaratory doctrine, policy or legislative framework that captures India's strategic interests, ambitions and restraints in this arena. However, the cyber institutional machinery and policy landscape are evolving rapidly, with several new institutions set up in the last decade and several policies in the nascent stages of development or due to be released soon, including notably the National Cyber Security Strategy.

Further, public statements by public officials on India's cyber doctrine and operations could serve as evidence of intent to conduct international cyber operations.

Therefore, at this stage, India's present capabilities and strategy can be inferred from an informed analysis of existing State practice and institutional architecture and a combined reading of existing laws and policies. However, India's approach to cybersecurity is rooted in its appraisal of strategic interests. As these interests and threats evolve, India may more proactively disclose capabilities and frame a governing doctrine in order to robustly project power in cyberspace.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH