12. India

Despite the geostrategic instability of its region and a keen awareness of the cyber threat it faces, India has made only modest progress in developing its policy and doctrine for cyberspace security. Its approach towards institutional reform of cyber governance has been slow and incremental, with the key coordinating authorities for cyber security in the civil and military domains only established in 2018 and 2019 respectively. They work closely with the main cyber-intelligence agency, the National Technical Research Organisation. India has a good regional cyber-intelligence reach but relies on partners, including the United States, for wider insight. The strengths of the Indian digital economy include a vibrant start-up culture and a very large talent pool. The private sector has moved more quickly than the government in promoting national cyber security. The country is active and visible in cyber diplomacy but has not been among the leaders on global norms, preferring instead to make productive practical arrangements with key states. From the little evidence available on India's offensive cyber capability, it is safe to assume it is Pakistan-focused and regionally effective. Overall, India is a third-tier cyber power whose best chance of progressing to the second tier is by harnessing its great digital-industrial potential and adopting a whole-of-society approach to improving its cyber security.

Strategy and doctrine

The main lines of India's current approach can be found in ministerial speeches and in government regulations or legislation, rather than in policy documents. In 2013, however, the Ministry of Communications and Information Technology did release the country's first National Cyber Security Policy,[1] a short document affirming the need to protect the government, businesses and citizens from cyber attacks either by state or non-state actors. It presented basic recommendations for government organisations and private companies, including the allocation of budgets and personnel for cyber-security purposes and the drafting of information-security policies. It also set out national objectives, including the training of 500,000 cyber-security professionals over the following five years, the development of indigenous cyber-security technologies, the establishment of public–private partnerships, and the promotion of a culture of cyber security and privacy that would encourage responsible behaviour by internet users.

India's thinking on cyber policy for the civil sector continues to develop. Government officials had planned to issue a new national cyber-security strategy in 2020

List of acronyms

CERT-In	Computer Emergency Response Team India
DCA	Defence Cyber Agency
DIA	Defence Intelligence Agency
DSCI	Data Security Council of India
IB	Intelligence Bureau
ICT	information and communications technology
NCCC	National Cyber Coordination Centre
NCIIPC	National Critical Information Infrastructure Protection Centre
NTRO	National Technical Research Organisation
RAW	Research and Analysis Wing

to address developments in 5G, ransomware and the Internet of Things.[2] That effort appears to have stalled but the government is actively reframing all areas of cyber-security policy, including education, skills, import controls and national security. The military confrontation with China in the disputed Ladakh border area in June 2020, followed by a sharp increase in Chinese activity against Indian networks, has heightened Indian concerns about cyber security, not least in systems supplied by China. In a speech on Independence Day in August 2020, Prime Minister Narendra Modi devoted a paragraph to the new cyber-security strategy, promising it would soon emerge.[3] In January 2021 a high-level government meeting was held to discuss a security strategy for the telecoms sector.[4] Key planks of India's cyber-security policy will probably align quite closely with the priorities laid out in a consultation paper released by the Data Security Council of India (DSCI), the principal private-sector organisation in the field.[5] The paper addresses 21 different areas of policy while depicting a backdrop of increasing threats and, in the opinion of the DSCI, insufficient government action.

As for the approach taken by India's armed forces, in 2017 they publicly released a joint doctrine in which cyberspace, though subsumed under the rubric of information warfare, was afforded a prominent role.[6] Placing strong emphasis on the integration of capabilities across the armed forces, cyber power – defined as 'the ability to use cyberspace freely and securely to gain an advantage over the adversary while denying the same to him in various operational environments' – was presented as equal in importance to land, sea, air and space power and special-forces operations. Treating cyber capabilities as one of a triad of integrated strategic forces alongside space and special operations, the doctrine presaged the establishment of a Defence Cyber Agency, eventually created in 2019. It also emphasised the importance of cyber security for India's economy and critical national infrastructure, placing the defence of the country's cyberspace on a par with the defence of its territory, airspace and trade routes. Moreover, the doctrine identified cyber warfare as a component of hybrid warfare, which it described as a key element in 'current fifth generation war' (though there was no clear definition of hybrid warfare or fifth-generation war from India's perspective).

Cyber capabilities also featured prominently in the new Land Warfare Doctrine released by the Indian Army in late 2018.[7] Again subsumed within information warfare, cyberspace was designated as a new dimension of warfare and an important factor in winning future battles. The document foreshadowed the increasing integration of cyber capabilities into the conventional and sub-conventional realms, including for covert operations. In it, the army set itself the task not only of developing or upgrading cyber-deterrence and cyber-defence capabilities, but also of retaining the capability to fight in the face of prolonged attempts at cyber disruption.

Governance, command and control

India's cyber command-and-control structure has been under development since the early 2000s but remains decentralised. Cyber-security powers are spread across a number of agencies, with reports of overlapping competencies and bureaucratic turf wars.[8] The situation is further complicated by the country's federal political structure. Several key institutions were set up between 2004 and 2008, all operating under the direction of ministers and coming together in the National Security Council of the Cabinet, which sits at the apex of security decision-making. The main cyber agency, the National Technical Research Organisation (NTRO), set up in 2004 and modelled on the US National Security Agency, reports to the national security advisor and is tasked with technical intelligence-gathering, signals interception and influence operations.[9] A National Information Board, responsible for information security, was established in 2004 as an advisory committee, in part to formulate a national policy on information warfare.[10] In 2003 the government set up a national Computer Emergency Response Team (CERT-In) which operates under the Ministry of Electronics and Information Technology.

In 2008, amendments to the Information Technology Act of 2000 gave government agencies wide-ranging powers to 'issue directions for interception, monitoring or decryption of any information through any computer resource'.[11] The legislation also sought protections for 'critical information infrastructure' networks. It was also in 2008 that the main private-sector body representing the ICT sector, the National

Association of Software and Service Companies, set up the DSCI, which has proved an effective advocate in mobilising more effective government responses in the area of cyber security.

A security review in 2011–12, ordered by the prime minister, identified cyber security as a key area of development and recommended the establishment of a centralised cyber command and analogous civilian entities with oversight powers across government agencies.[12]

By 2013, following allegations about cyber espionage conducted against India by several countries (including the United States and China) and leaks concerning India's own offensive cyber capabilities, the government was keenly aware of the need for improved policy and action. However, institutional development over the next few years was quite piecemeal. A National Critical Information Infrastructure Protection Centre (NCIIPC) was established in 2014 under the direction of the NTRO.[13] A National Cyber Coordination Centre (NCCC), subordinate to CERT-In, finally began operations in 2018 (having first received ministerial approval in 2013). The NCCC is responsible for intelligence-sharing between government agencies and for coordinating government responses to cyber attacks.[14]

The Defence Cyber Agency (DCA), created in 2019, is central to the command and control of India's military cyber capabilities. Its intended role is to integrate and coordinate the cyber, space and special-forces capabilities of the three armed services. It is part of the Integrated Defence Staff, a tri-service headquarters which includes civilian representation from the Ministry of External Affairs and other ministries. It comprises a sizeable tri-service staff of about 1,000, divided into several teams based at a command centre in Delhi and in other locations around the country.[15] By operationalising the 2017 joint doctrine's focus on capability integration, the DCA represents both an important institutional evolution and a significant maturing of India's approach to military uses of cyberspace.

Core cyber-intelligence capability

India's intelligence priorities are deeply shaped by internal and external terrorist threats, internal political violence and the ongoing conflict with Pakistan over Kashmir. The internally focused Intelligence Bureau (IB) is responsible for counter-terrorism and counter-intelligence, in cooperation with the state police and national paramilitary forces.[16] India's foreign intelligence agency is the Research and Analysis Wing (RAW). The Defence Intelligence Agency (DIA), created in 2002, now coordinates all defence-intelligence assets, including the Signals Intelligence Directorate and the DCA. Intelligence collection by these three main agencies is digitally enabled via a real-time intelligence grid (NATGRID) that links citizen-data sources across multiple government and private databases to facilitate the monitoring of terrorist activities that pose a threat to banking, finance and transportation networks. In addition, the IB and RAW are empowered to monitor internet traffic through a system enabling the interception of internet communications, including social media.[17] While the IB, RAW and DIA each represent a part of India's cyber-intelligence capability, they are all heavily reliant for core capability on the technical-intelligence agency, the NTRO. Various parts of the Ministry of Home Affairs, including the Cyber Crime Wing and Central Forensics Science Laboratory, are also important sources of cyber intelligence.

Beyond the domestic threats, India's cyber-intelligence capabilities have unsurprisingly been focused on its near abroad, particularly Pakistan

Beyond the domestic threats, India's cyber-intelligence capabilities have unsurprisingly been focused on its near abroad, particularly Pakistan. For example, there are indications that, since about 2010, Indian cyber teams have been targeting IP addresses in Pakistan (and to a lesser extent in China), as well as secessionist movements within India itself, in a significant cyber-surveillance and cyber-espionage operation.[18] Further afield, however, India's cyber-intelligence reach appears weak: it tends to rely on partnerships such as those with the US, the United Kingdom and France for a higher level of cyber

situational awareness and to help it develop a greater reach of its own in future.

Mirroring the UK, the Indian government has set up a Joint Intelligence Committee attached to the office of the prime minister, tasked with collecting, assessing and prioritising inputs from all the country's intelligence agencies.[19] A Multi-Agency Centre (MAC) has also been established under the IB, together with subsidiary MACs in different states, with the aim of enhancing the sharing of information between intelligence units, including finance and defence ministries at the state and national levels.

Cyber empowerment and dependence

India is an ICT powerhouse, with a digital economy estimated in value at US$190 billion[20] and a tech start-up sector assessed to be the third largest in the world.[21] According to one estimate, core digital sectors such as ICT-enabled services and electronics manufacturing will contribute around 10% of GDP by 2025.[22] However, only slightly more than half of India's 1.4bn people have access to the internet, and the levels of mobile-phone ownership and internet use are far higher among men than women.[23] Most Indians who access the internet do so by mobile phone, though download speeds are below the global average. Agriculture, which still provides the livelihoods of hundreds of millions of Indians, is undergoing some digitisation and employing tools and techniques that rely on automated and autonomous machines. However, the vast majority of the population (about 90%) lack basic digital skills.[24] As one way of addressing the issue, the government has been increasing the availability of apps and digital services in a greater number of local languages.

Foreign investment plays a large part in India's digital economy, with the country providing outsourced IT services around the world and serving as a major production hub for global brands, such as Dell computers. From 2014 to 2020, US ICT investment totalled US$30bn and Japanese investment US$12bn.[25] As for Chinese ICT investment, it surpassed US$4bn in the same period, with Alibaba and Tencent accounting for three-quarters of the total.[26]

The infrastructure at the heart of India's digital economy is built largely from imported equipment – for example, four of the top five mobile devices by market share are manufactured by Chinese companies.[27] Almost all the country's most popular mobile apps – such as Facebook Messenger, PlayerUnknown's Battlegrounds (PUBG), SHAREit, TikTok (at least until India's ban on Chinese apps in 2020), Truecaller, UC Browser and WhatsApp – were designed abroad. One exception, in 2020, was Aarogya Setu, the Indian government's COVID-19 contact-tracing app. As a result, and despite breakthroughs by Indian companies in app development and plans to develop 5G systems, the government has limited agency over the way in which devices and platforms manage the flow of data through their systems.

In the field of artificial intelligence (AI), India's research capability has been placed quite highly in global rankings, achieving ninth[28] and 13th[29] position, for example, in two authoritative studies. The lion's share of AI research and development (about 85%) is conducted by universities rather than industry.[30] The Indian Institute of Technology (IIT) Hyderabad has collaborated with Nvidia, an American multinational technology company, to establish India's first AI Technology Centre, aimed at accelerating research and its commercial adoption.[31] The centre intends to focus on advanced AI research in areas of agriculture, smart cities and language-understanding, in line with the priorities stated in India's national strategy for AI.[32] In terms of the application of AI to industrial processes, it is notable that India was ranked third, after the US and China, in a 2018 study by the Boston Consulting Group.[33] The country's AI start-ups received total investment of US$762m in 2019, a 44% increase in comparison with 2018.[34]

The space industry is led by the Indian Space Research Organisation (ISRO), which is one of the world's six largest space agencies and owns one of the largest fleets of communication and remote-sensing satellites used for civil and military purposes.[35] ISRO also operates satellites for surveillance and navigation purposes – including the Indian Regional Navigation Satellite System;[36] dual-use surveillance satellites in the Cartostat and RISAT series;[37] and EMISAT, launched in 2019, which can detect an adversary's electromagnetic signals.[38] Owing to capacity limitations in its own agencies,[39] the Indian government has begun to rely

more on commercial enterprises to develop and produce space equipment such as satellites and propulsion systems. Like many other countries, India still relies on foreign suppliers for the space sector, with Hughes Communications India appointed to provide a high-performance satellite broadband system for India's Naval Communication Network.[40] It has, however, achieved self-reliance in the production of launch vehicles and some satellite technologies.[41]

A unique characteristic of the Indian cyber economy is the huge number of graduates in ICT-related subjects entering the job market every year: in 2019 the figure was almost 600,000, which was five times more than in the US.[42]

Cyber security and resilience

India's state administrations have numerous cyber-security-related offices with large numbers of staff, and much attention has been paid to cyber crime since 2009, when the country became one of the first to introduce cyber-crime courts and cyber police stations. But perhaps the most distinctive feature of India's cyber-security infrastructure is the importance of the private sector, which has led the way in developing strong policies and standards. The rapid integration of the internet into everyday economic life, albeit from a low base, has created the need for new cyber-security capabilities on a scale and at a pace unseen in any other country – hundreds of millions of Indians have begun to participate in e-commerce in the last five years, for example.[43] The main challenges lie in policy coordination, ensuring consistency around the country, and addressing the general lack of depth in cyber-security skills relative to the size of the population and the needs of industry.

India has frequently been the victim of cyber attacks, including on its critical infrastructure, and has attributed a significant proportion of them to China or Pakistan. CERT-In reported, for example, that there were more than 394,499 incidents in 2019,[44] and 2020 saw an upsurge in attacks from China.[45] Of particular concern to the Indian government are cyber attacks by North Korea that use Chinese digital infrastructure.[46] The vast majority of the cyber incidents flagged by CERT-In appear to have been attempts at espionage,[47] but they could also have resulted in serious damage to the integrity of Indian networks and platforms. In 2020, India had the second-highest incidence of ransomware attacks in the world[48] and the government banned 117 Chinese mobile applications because of security concerns.[49]

India regards its financial institutions as particularly vulnerable to cyber attack.[50] In August 2018, in a persistent attack on Cosmos Bank by a North Korean group, US$13.5m was siphoned off from customers' accounts.[51] A United Nations Security Council panel of experts, appointed to study North Korea's attempts to evade UN sanctions, suggested in a July 2019 report that Indian banks may have been the victims of cyber theft by North Korea amounting to nearly US$200m over a three-year period.[52] On the other hand, thanks to stringent guidelines from the Reserve Bank of India (RBI), the financial sector is more secure than other areas of the Indian economy. For example, two-factor authentication, strictly audited by the RBI, is the norm in internet banking and e-commerce.[53]

Although India's central government has been slow in addressing cyber security, the private sector has been far more active and more effective. The DSCI, which promotes best practices and standards for cyber security and privacy, undertakes capacity-building projects with a focus on training and certification, including for the government sector. In 2020 it said there was a 'dire need' for the government to play its part in promoting cyber security in the country, and recommended a quadrupling of government expenditure on cyber security as the country's digital economy expands.[54] India was ranked 47th out of 175 countries in the International Telecommunication Union's 2018 Global Cybersecurity Index, well behind its geopolitical rival China (27th).[55]

In cyber-resilience policy and preparedness for emergencies, India has some foundations in place, with the NCIIPC active in promoting policies and procedures throughout the country since it was created in 2014. Progress in emergency-response planning has in many cases been slower at the state level, with Tamil Nadu, for example, only introducing a cyber-security strategy in 2020.[56] In contrast, the state of Maharashtra, which contains the commercial and financial hub of Mumbai, has a well-established cyber-security team in its police force and dedicated cyber 'police stations' in various parts of Mumbai.

However, compared with equivalent bodies in some wealthier countries, the NCIIPC is not well equipped to handle cyber emergencies and wider resilience-planning – for example, as of 2018, there was only one sector (power) where it had been able to organise stakeholders around those objectives.[57] There are also indications that the NCIIPC has not coordinated well with other government bodies.[58] It is unclear, for example, if steps have been taken to improve cyber defences at the Unique Identification Authority of India, after its database of citizens' biometric information (the second-largest in the world) was reported to have been breached in 2017, or the Kudankulam Nuclear Power Plant, which in 2019 was the target of a serious cyber attack that it initially denied and then downplayed.[59] In Maharashtra, where the power sector was targeted by Chinese hackers (dubbed the Red Echo group) from early 2020, it seems the cyber-security department in the state police were informed of the threat by CERT-In in November 2020 but the NCIIPC only alerted the Ministry of Power on 12 February 2021.[60]

Though the National Cyber Security Coordinator conducts periodic whole-of-government audits involving relevant agencies, the government has faced an uphill battle in trying to make new entities such as the NCIIPC work seamlessly alongside long-established public-sector bodies that are in various stages of digitising their infrastructure. The NCIIPC has taken private enterprises under its wing, including oil and gas companies, and tries to ensure that the public and private sectors work in tandem on cyber security.

The first reported cyber exercise in the Indian Armed Forces, *CyberEx*, was conducted by the Indian Defence University on 29–30 April 2019.[61] It involved the NTRO, the three services, the National Security Council Secretariat, CERT-In, the Defence Research and Development Organisation, the National Informatics Centre, academia and industry.

Global leadership in cyberspace affairs

As a nuclear power with large conventional forces, a burgeoning digital economy and a determination to increase its geopolitical influence, India is the target of cyber espionage by a wide range of states. However, it knows its defensive capabilities are relatively weak. As a result, it pursues diplomatic efforts to bring the governance of cyberspace within the rules-based international order, while maintaining a realistic approach to dealing with the states that are targeting its networks.

In its National Cyber Security Policy of 2013, India's diplomatic goals included the development of bilateral and multilateral cyber-security relationships as well as global cooperation between national law-enforcement agencies, security services, judicial systems and armed forces.

Unsurprisingly, the challenges involved in defending its open networks (and largely imported infrastructure) have prompted India to advocate international norms of restraint. It appears to have abandoned its previous opposition to emerging international legal principles such as the possible voluntary norms on security in cyberspace put forward by the UN Group of Governmental Experts (GGE) in 2015.[62] As a member of the 2016–17 GGE, India endorsed the inclusion in the final report of a right to self-defence in cyberspace, although the draft did not receive the unanimous consent of all participating experts.[63] It is unclear whether India will further endorse the right to retaliatory measures for acts that fall below the thresholds that qualify as a 'threat or use of force' or 'armed attack' under international law.

India knows its defensive cyber capabilities are relatively weak

India's most developed bilateral cyber partnership is with the US. The two countries have held a regular cyber dialogue since the early 2000s, intensifying in 2015 with the decision to convene a 'Track 1.5' programme that seeks to convene government officials and business leaders to collaborate on cyber questions. Cyber is also envisioned as a component of several other US–India agreements, including on intelligence-sharing and mutual legal assistance.[64]

India has also pursued bilateral cyber dialogues with several other partners, including the European Union, Russia and the UK. The cyber partnership with the UK is particularly well developed, with a regular dialogue dating back to 2012. In April 2018 the two countries

signed a framework agreement identifying avenues for bilateral cooperation on cyber security and establishing working groups on cyber diplomacy, cyber crime, incident response and the digital economy.[65] They have also agreed in principle to establish a joint Cyber Security Training Centre of Excellence.[66]

Offensive cyber capability

Public statements by Indian officials and other open-source material indicate that India has developed relatively advanced offensive cyber capabilities focused on Pakistan. It is now in the process of expanding these capabilities for wider effect.

India reportedly considered a cyber response against Pakistan in the aftermath of the November 2008 terrorist attacks in Mumbai, with the NTRO apparently at the forefront of deliberations.[67] A former national security advisor has since indicated publicly that India possesses considerable capacity to conduct cyber-sabotage operations against Pakistan,[68] which appears credible.

It is difficult to gauge the extent or orientation of India's current investment in offensive capabilities but there are some indications that the focus may have shifted more to countering China, given its growing economy and regional power.[69] There is also evidence dating back to 2014 of Prime Minister Modi's interest in creating a 'Digital Armed Force', in part for deterrent purposes.[70] A 2019 report commissioned by an influential Indian think tank with close links to the ruling Bharatiya Janata Party urged the rapid development of offensive cyber capabilities but cautioned against any public declaration until those capabilities were in place.[71]

Overall, India's focus on Pakistan will have given it useful operational experience and some viable regional offensive cyber capabilities. It will need to expand its cyber-intelligence reach to be able to deliver sophisticated offensive effect further afield, but its close collaboration with international partners, especially the US, will help it in that regard.

Notes

1 Ministry of Communications and Information Technology, 'National Cyber Security Policy 2013', 2 July 2013, https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

2 Aditi Agrawal, 'India's cybersecurity strategy policy in 2020, says National Cybersecurity Coordinator Rajesh Pant', Medianama, 22 June 2019, https://www.medianama.com/2019/06/223-indias-cybersecurity-strategy-policy-in-2020-says-national-cybersecurity-coordinator-rajesh-pant.

3 Elizabeth Roche, 'PM Modi says India to have new cyber security policy soon', Livemint, 15 August 2020, https://www.livemint.com/news/india/pm-modi-says-india-to-soon-have-cyber-security-policy-11597461750194.html.

4 'Govt formulating new action plan, Chinese telecom giants could be out of game', *Economic Times*, 21 January 2021, https://telecom.economictimes.indiatimes.com/news/govt-formulating-new-action-plan-chinese-telecom-giants-could-be-out-of-game/80391251.

5 Data Security Council of India, 'National Cyber Security Strategy 2020: DSCI submission', 2020, https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%202020%20DSCI%20submission.pdf.

6 Headquarters Integrated Defence Staff, Ministry of Defence, 'Joint Doctrine – Indian Armed Forces', 2017, https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf.

7 Indian Army, 'Land Warfare Doctrine 2018', http://www.ssri-j.com/MediaReport/DocumentIndianArmyLandWarfareDoctrine2018.pdf.

8 Tarun Krishnakumar, 'Cyber Insecurity: Regulating the Indian Financial Sector', Oxford University Faculty of Law, 21 August 2017, https://www.law.ox.ac.uk/business-law-blog/blog/2017/08/cyber-insecurity-regulating-indian-financial-sector.

9 B. Raman, 'Possible Misuse of New TECHINT Capabilities', *Indian Defence Review*, 5 December 2011, http://www.indiandefencereview.com/spotlights/possible-misuse-of-new-techint-capabilities.

10 Saikat Datta, 'Low on the IQ', *Outlook*, 4 July 2005, https://magazine.outlookindia.com/story/low-on-the-iq/227823.

11 'Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009', The Centre for Internet & Society, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009.

12 Vinod Anand, 'Defence Reforms and Naresh Chandra Task Force Review', Vivekananda International Foundation, 13 September 2012, https://www.vifindia.org/article/2012/september/13/defence-reforms-and-naresh-chandra-task-force-review.

13 Government of India, National Technical Research Organisation, https://ntro.gov.in/welcome.do.

14 'India now has a National Cyber Coordination Centre (NCCC) to monitor cyber threats', India Today, 11 August 2007, https://www.indiatoday.in/education-today/gk-current-affairs/story/nccc-cyber-india-1029203-2017-08-11.

15 Rahul Bedi, 'India setting up tri-service commands for special forces, cyber security, and space', *Jane's Defence Weekly*, 16 May 2019.

16 See Mahendra Kumawat and Vinay Kaura, 'Building the resilience of India's internal security apparatus', Observer Research Foundation, Occasional Paper 176, November 2018, https://www.orfonline.org/wp-content/uploads/2018/11/ORF_OccasionalPaper_176_Security_NEWFinalPDF.pdf.

17 See Udbhav Tiwari, 'The Design & Technology Behind India's Surveillance Programmes', The Centre for Internet & Society, 20 January 2017, https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes#_ftnref13.

18 Snorre Fagerland et al., 'Operation Hangover: Unveiling an Indian Cyber Attack Infrastructure', Norman Shark, May 2013, http://docshare.tips/unveiling-an-indian-cyberattack-infrastructure_58a3ff6db6d87f499c8b462d.html.

19 See Musa Tuzuner (ed.), *Intelligence Cooperation Practices in the 21st Century: Towards a Culture of Sharing* (Amsterdam: IOS Press, 2010).

20 'How the IT sector has emerged as a pillar of modern India', *Hindu*, 14 August 2020, https://www.thehindubusinessline.com/news/national/how-the-it-sector-has-emerged-as-a-pillar-of-modern-india/article32357389.ece. This estimate is based on a classic narrow view of the ICT sector, as usually reported in national accounts. However, the Organisation for Economic Co-operation and Development and other research institutions have been adopting a definition of the digital economy based on a broader set of indicators. According to one of these broader estimates, India's digital economy was worth US$570bn in 2019, equivalent to about 20% of GDP.

21 Trisha Ray et al., *The Digital Indo-Pacific: Regional Connectivity and Resilience*, The Australian Government for the Quad Tech Network, February 2021, p. 8, https://www.orfonline.org/wp-content/uploads/2021/02/thedigitalindopacific.pdf.

22 McKinsey Global Institute, 'Digital India: Technology to Transform a Connected Nation', March 2019, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/digital-india-technology-to-transform-a-connected-nation-full-report.ashx.

23 Romita Majundar, 'Gender gap in mobile and internet usage in India as per GSMA report', *Business Standard*, 9 March 2019, https://www.business-standard.com/article/economy-policy/gender-gap-in-mobile-and-internet-usage-in-india-as-per-gsma-report-119030900696_1.html.

24 Digital Empowerment Foundation, 'About', undated, https://www.defindia.org/national-digital-literacy-mission.

25 Ray et al., *The Digital Indo-Pacific: Regional Connectivity and Resilience*, p. 9.

26 *Ibid*.

27 Sam Byford, 'Realme Takes Chunk of India Mobile Market as Samsung Slides', The Verge, 11 November 2019, https://www.theverge.com/2019/11/11/20958932/india-mobile-marketshare-q3-2019-idc-realme-samsung-xiaomi.

28 JJiqiang Niu et al., 'Global research on artificial intelligence from 1990–2014: Spatially-explicit bibliometric analysis', *ISPRS International Journal of Geo-Information*, vol. 5, no. 5, p. 8, https://www.mdpi.com/2220-9964/5/5/66/pdf.

29 Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216.

30 Richa Bhatia, 'Where Artificial Intelligence Research in India Is Heading', Analytics India Magazine blog, 27 March 2018, https://analyticsindiamag.com/where-artificial-intelligence-research-in-india-is-heading.

31 Anisha Kumari, 'IIT Hyderabad, NVIDIA Establish First AI Research Centre in India', NDTV, 9 July 2020, https://www.ndtv.com/education/iit-hyderabad-nvidia-establish-first-ai-research-centre-in-india.

32 Canadian Institute for Advanced Research, 'Building an AI World: Report on National and Regional AI Strategies Second Edition', May 2020, p. 22, https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf.

33 'India Ranked Third in Terms of Artificial Intelligence Implementation: Report – ET CIO', ETCIO, 26 April 2018, https://cio.economictimes.indiatimes.com/news/business-analytics/india-ranked-third-in-terms-of-artificial-intelligence-implementation-report/63922875.

34 AIMResearch, 'Report: Indian AI Startup Funding in 2019', 28 January 2020, p. 4, https://analyticsindiamag.com/report-indian-ai-startup-funding-in-2019.

35 Indian Space Research Organisation, 'About ISRO', https://www.isro.gov.in/about-isro.

36 The Indian Regional Navigation System Satellite is made up of seven satellites that serve civil purposes but also provide encrypted data to the Indian armed forces. See G.D. Sharma, *Exploiting Indian Military Capacity in Outer Space* (New Delhi: Centre for Joint Warfare Studies, 2016), https://cenjows.in/pdf/issue/Layout_Exploiting%20Indian%20Military.pdf.

37 See Government of India, Department of Space, Indian Space Research Organisation, 'List of Earth Observation Satellites', https://www.isro.gov.in/spacecraft/list-of-earth-observation-satellites.

38 Manu Pubby, 'Navy to Buy Rs 1,589 Crore Satellite From ISRO', *Economic Times*, 18 July 2019, https://economictimes.indiatimes.com/news/defence/navy-to-buy-rs-1589-crore-satellite-from-isro/articleshow/70283927.cms?from=mdr.

39 Narayan Prasad Nagendra and Prateep Basu, 'Demystifying Space Business in India and Issues for the Development of a Globally Competitive Private Space Industry', *Space Policy*, vol. 36, 2016, pp. 1–11, https://www.sciencedirect.com/science/article/abs/pii/S0265964616300078.

40 John Sheldon, 'Indian Military Space: Hughes India and Sterlite Tech Enable Satcom Connectivity for Indian Navy', Spacewatch, January 2019, https://spacewatch.global/2019/01/indian-military-space-hughes-india-and-sterlite-tech-enable-satcom-connectivity-for-indian-navy.

41 Rajeswari Pillai Rajagopalan, Pulkit Mohan and Rahul Krishna, 'India in the Final Frontier: Strategy, Policy and Industry', ORF Special Report no. 100, Observer Research Foundation, 29 January 2020, https://www.orfonline.org/research/india-in-the-final-frontier-strategy-policy-and-industry-60834.

42 Organisation for Economic Co-operation and Development, *Measuring the Digital Transformation*: *A Roadmap for the Future* (Paris: OECD Publishing, 2019), p. 144, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

43 In 2016 the government set up the Unique Identification Authority of India, which provided a new foundation for biometric identification to support more secure electronic banking and e-commerce across the country, especially by mobile phone. While the organisation had been conducting business under another name since 2010 and issuing IDs, there has been an explosion of the process since 2016, with 1.24bn citizens now registered. See Unique Identification Authority of India, 'About UIDAI', https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html.

44 Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, 'CERT-In Annual Report (2019)', p. 3, https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2020-0001.pdf.

45 Manu Kaushik, '200% rise in cyberattacks from China in a month; India tops hit list post Galwan face-off', *Business Today*, 24 June 2020, https://www.businesstoday.in/technology/news/200-percent-rise-in-cyberattacks-from-china-in-a-month-india-tops-hit-list-post-galwan-face-off/story/407806.html.

46 Interview with former official in the Indian government, New Delhi, 4 October 2019.

47 Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, 'CERT-In Annual Report (2018)', p. 6, https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2019-0123.pdf.

48 National Critical Information Infrastructure Protection Centre, 'NCIIPC Newsletter', January 2021, p. 2, https://nciipc.gov.in/documents/NCIIPC_Newsletter_Jan21.pdf.

49 'India bans PUBG, 117 other Chinese apps for "stealing, transmitting users' data" to servers outside India', FirstPost, 20 September 2020, https://www.firstpost.com/india/india-bans-pubg-117-other-chinese-apps-for-stealing-transmitting-users-data-to-servers-outside-india-8778561.

50 'Banks Most Vulnerable to Cyber Threats: National Cyber Security Coordinator', *New Indian Express*, 20 February 2019, https://www.newindianexpress.com/business/2019/feb/20/banks-most-vulnerable-to-cyber-threats-national-cyber-security-coordinator-1941363.html.

51 Rashmi Rajput, 'UN Security Council Panel Finds Cosmos Bank Cyber Attack Motivated by N Korea', *Economic Times*, 27 March 2019, https://economictimes.indiatimes.com/industry/banking/finance/banking/un-security-council-panel-finds-cosmos-bank-cyber-attack-motivated-by-n-korea/articleshow/68589549.cms?from=mdr.

52 United Nations Security Council, 'Report of the Panel of Experts established pursuant to Resolution 1874 (2009)', 5 March 2019, S/2019/171, https://www.

securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3CF6E4FF96FF9%7D/s_2019_171.pdf.

53 Reserve Bank of India, 'Master Direction on Digital Payment Security Controls', 18 February 2021, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF.

54 DSCI, 'National Cyber Security Strategy 2020: DSCI submission'.

55 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

56 Raja Simhan, 'TN govt working on giving the "cyber resilience" edge to governance', The Hindu Business Line, 24 December 2020, https://www.thehindubusinessline.com/info-tech/tn-govt-working-on-giving-the-cyber-resilience-edge-to-governance/article33409737.ece.

57 Munish Sharma and Cherian Samuel, *India's Strategic Options in a Changing Cyberspace* (Delhi: Pentagon Press, 2018), p. 110, https://idsa.in/system/files/book/book_indias-strategic-options-in-cyberspace.pdf.

58 See, for example, Saikat Datta, 'Defending India's Critical Information Infrastructure', Internet Democracy Project, 2016, https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf; and Shatabdi Mazumder, 'The Need for Re-conditioning of India's Cyber Security', Apeksha News Network, 28 September 2020, https://apekshanews.com/the-need-for-re-conditioning-of-indias-cyber-security.

59 Sushovan Sircar and Vakasha Sachdev, 'Kudankulam Cyber Attack Did Happen, Says NPCIL a Day After Denial', The Quint, 1 November 2019, https://www.thequint.com/news/india/kudankulam-nuclear-power-plant-malware-attack-correct-confirms-npcil.

60 'Chinese cyber attack foiled: Power Ministry', *Hindu*, 1 March 2021, https://www.thehindu.com/news/national/attacks-by-chinese-groups-thwarted-power-ministry/article33965683.ece.

61 Press Information Bureau, 'Cyber Exercise on Scenario Building & Response', 29 April 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=189871.

62 James Crawford, Jacqueline Peel and Simon Olleson, 'The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: Completion of the Second Reading', *European Journal of International Law*, vol. 12, no. 5, 2001, pp. 963–91, http://www.ejil.org/pdfs/12/5/1557.pdf. Since a UN General Assembly resolution in 2004, a UN Group of Governmental Experts (GGE) has convened for two-year terms to address international-security aspects of cyberspace. It was known as the GGE on 'Developments in the Field of Information and Telecommunications in the Context of International Security' until 2018, when it was renamed the GGE on 'Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. In cyberspace-policy circles it is common to refer to it simply as 'the GGE'. See UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

63 Interview with a member of the 2016–17 GGE, August 2017.

64 Nayantara Ranganathan, 'Cybersecurity and bilateral ties of India and the United States: A very brief history', Internet Democracy Project, 30 September 2015, https://internetdemocracy.in/reports/cybersecurity-and-india-us-bilateral-ties-a-very-brief-history.

65 Rahul Roy-Chaudhury, 'India–UK cybersecurity cooperation: The way forward', International Institute for Strategic Studies blog, 22 November 2019, https://www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation.

66 Rahul Roy-Chaudury, 'India–UK cyber security cooperation: The way forward', India Global Business, 15 November 2019, https://www.indiaglobalbusiness.com/igb-archive/india-uk-cyber-security-cooperation-the-way-forward-india-global-business.

67 Raj Chengappa and Sandeep Unnithan, 'How to Punish Pakistan', India Today, 22 September 2016, https://www.indiatoday.in/magazine/cover-story/story/20161003-uri-attack-narendra-modi-pakistan-terror-kashmir-nawaz-sharif-india-vajpayee-829603-2016-09-22.

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

69 Arditi Agrawal, 'India's Cybersecurity Strategy Policy in 2020, Says National Cybersecurity Coordinator Rajesh Pant', Medianama, 22 June 2019, https://www.medianama.com/2019/06/223-indias-cybersecurity-strategy-policy-in-2020-says-national-cybersecurity-coordinator-rajesh-pant.

70 Narendra Modi, 'PM's Address at the Combined Commanders' Conference', 17 October 2014, https://www.narendramodi.in/amp/pms-address-at-the-combined-commanders-conference.

71 Vivekananda International Foundation, 'Credible Cyber Deterrence in Armed Forces of India', March 2019, https://www.vifindia.org/sites/default/files/Credible-Cyber-Deterrence-in-Armed-Forces-of-India_0.pdf.