CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

MARCH 2025

Interpreting India's Cyber Statecraft

Joe Devanny and Arthur P.B. Laudrain

Interpreting India's Cyber Statecraft

Joe Devanny and Arthur P.B. Laudrain

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Introduction

This paper explores India's cyber statecraft by illustrating how India uses its cyber capabilities, policies, and engagement in cyber diplomacy to further its national strategic objectives. The paper focuses principally on the international diplomatic and operational dimensions of India's cyber statecraft, but it also explains the connection between domestic and international aspects of Indian strategy. India is widely seen as an influential emerging power of the Global South and as a committed advocate for reform of global institutions. However, there is considerable ambiguity surrounding India's cyber doctrine.

Following a series of similar studies for the Carnegie Endowment's Technology and International Affairs Program, this paper focuses on cyber diplomacy in so-called middle ground states.[1] These are states in the Global South perceived as being pivotal in the competition for influence between liberal like-minded and authoritarian states. Like previous studies on Brazil, South Africa, and Mexico, this paper situates India's approach to cyber statecraft in the context of contemporary global debates in cyber diplomacy, principally regarding responsible state behavior in cyberspace. The complexity of India's bilateral relationships with China and Russia and the intricacies of its approach to managing "multi-alignment" are further reasons for the considerable Western interest in understanding the objectives and mechanisms of Indian cyber statecraft.[2]

The United States and its like-minded partners compete with Russia and China to influence the positions which India adopts in different forums of regional and multilateral cyber diplomacy, for example regarding internet governance and norms of responsible state behavior in cyberspace. Yet, it is crucial for policymakers to understand that, like those of other members of the middle ground, India's cyber policies emerge from a domestic political context, with Prime Minister Narendra Modi's administration's conception of India's national interest as the focal point for its decisionmaking.[3] To understand India's cyber diplomacy and its wider approach to cyber statecraft, it is necessary to consider the full politico-strategic context.

India's Ministry of External Affairs (MEA) leads the country's engagement with the agenda of global cyber diplomacy. While the MEA feeds into the wider national cyber strategy process, the most important institutional actors lie elsewhere in the executive apparatus. In India's case, this is highlighted by the strong institutional role of the agencies within the Prime Minister's Office regarding the most sensitive operational aspects of India's cyber statecraft. All this plays out amid a relative lack of public debate about the strategic value of cyber operations as a tool of India's national strategy.

The paper explores the limits of Western states' influence over India's cyber strategy, providing context about what India actually wants to achieve in its cyber diplomacy and through its wider cyber statecraft, including its development and use of cyber capabilities. As with other security issues pursued bilaterally and via the Quadrilateral Security Dialogue (a partnership between Australia, India, Japan, and the United States more often known as the Quad), these states will likely find that focusing on engaging with India on the basis of shared cybersecurity interests—rather than shared values—is the most astute path.[4] Unsurprisingly, India is keener to engage diplomatically where it perceives a domestic advantage in doing so, and conversely more circumspect on issues where it wishes to retain more autonomy.

This paper argues that India's cyber statecraft should be interpreted as the outcome of overlapping priorities that differ from those of other states in the middle ground of cyber diplomacy: domestically, to use digital technology to drive economic growth and social development; geopolitically, to reduce dependence on China and develop internal balancing capacity through improved cybersecurity, resilience, and cultivation of offensive cyber capabilities;[5] and globally, to play a constructive or even a leading role in multilateral normative deliberations about responsible behavior in cyberspace, emphasizing the importance of respect for sovereignty and the need for cyber capacity-building. A comprehensive appraisal of the determinants of India's cyber statecraft is complicated by the lack of evidence regarding its current cyber operations capabilities and campaigns. Without transparency, it is difficult to gauge India's progress to date in converting its latent cyber power into actual, operationally active cyber power.

Origins of India's Cyber Statecraft

The tools of cyber statecraft, such as diplomacy and cyber operations (which can be defined as "operations in cyberspace that are principally intended to deliver an effect rather than gather intelligence or provide 'goal-line' protection to networks"[6]), are used instrumentally to further a given state's national strategy. As such, all cyber statecraft emerges from a domestic political context that reflects a particular state's threat perceptions and its national strategic objectives. India's national security objectives have been shaped by its history, its geopolitical context, and the evolving nature of contemporary threats.[7] The traditional imperatives of national security are unsurprisingly prominent. India prioritizes maintaining territorial integrity and national sovereignty, countering terrorism and insurgency, and securing its critical infrastructure. India's national strategy has long used foreign policy to create space for the country to pursue its domestic objectives, particularly regarding economic growth and development.[8] None of this is unique to cyber statecraft, but it is very clearly the prism through which India's cyber statecraft is perceived, shaped, and executed.

India's strategy is also inevitably shaped by its bilateral relationships with neighboring countries, most prominently with Pakistan and China—both of which have long-running territorial disputes with India. While Pakistan was historically the more immediate threat, including in cyberspace,[9] Indian strategy has transitioned to focus increasingly on the threat posed by its largest and most powerful neighbor: China.[10] China's rise has been a long-term concern of Indian strategic thinking, but it has become a more urgent priority during Modi's premiership. This shift in China-related policies has also materialized in other countries during this period, given concern about the new direction of China's strategy.[11] But it creates a most difficult policy dilemma for India, given its reliance on Chinese imports and likely continued need for some Chinese expertise and investment to help achieve its economic goals.[12] As this paper argues below, threat perceptions regarding China—including perceptions of specifically cyber-related threat activity[13]—are likely to drive much of India's development of sovereign cyber capabilities and emerging doctrine about the employment of these capabilities, especially as India experiences rapid digital transformation.

Within this wider context, the Indian government has gradually increased the priority of cybersecurity as an integral part of its national security, creating new domestic roles and institutions (such as the national cyber security coordinator and coordination center in 2015) and implementing new national cyber security policies (2013) and regulations over the last decade.[14] In the same period, it has professionalized its approach to cyber (and other emerging technologies) diplomacy, building up expertise (and new sub-units) in the MEA and cultivating international partnerships to improve cyber capacity-building, for example via the rejuvenated Quad partnership.[15] India has also recognized the role of operational cyber capabilities as part of the tool kit of modern statecraft—although this is more apparent in emerging armed forces cyber doctrine than it is in public statements about the country's evolving approach to nonmilitary cyber operations.[16]

As is the case for many other states, the rise of cyber threats from both state and non-state actors underscores the need for India to adopt robust cybersecurity policies. Cybersecurity policies encompass the protection of critical information infrastructure, preventing cyber espionage, and mitigating the impact of cyber attacks on economic stability. Like many other states, India recognizes that effective cybersecurity requires both an active governmental role and the effective participation of a range of other stakeholders, such as civil society and the private sector.[17] Again like many other states, India has found it easier to recognize the importance of this approach than to implement it effectively.[18]

The following section on the origins of India's cyber statecraft highlights the principal shaping factors at the domestic level: the impact of India's national security bureaucracy and associated politics; the modalities of domestic cyber threats; and the consequent strategy and apparatus India has developed in response to those threats. By understanding the historical, institutional, and political context in which India's cyber statecraft has evolved, observers can better interpret the logic shaping India's positions and actions in the international aspects of its cyber statecraft.

The Politics of National Security in India

Historical context and recent evolutions

To give further context to India's strategy of cyber statecraft, it is important to understand the geostrategic environment shaping its national security strategy; India's defense strategy has been persistently preoccupied with neighboring Pakistan and China. India's domestic politics and political personalities also exert an impact on its wider strategy.[19] Prime ministers are powerful albeit constrained national security actors.[20] In recent years, for example, there have been concerns about Modi's centralization of authority, controversial use of surveillance tools, and alleged use of assassination as an instrument of state policy.[21]

India's national security concerns are largely shaped by its relationships with neighboring countries, particularly Pakistan and China. Territorial disputes with these nations are central to India's security policy. Cross-border terrorism complicates India's relationship with both states.[22] Consequently, India's military doctrine has evolved to address both conventional and unconventional threats. Reflecting India's long-standing pursuit of strategic autonomy and effective deterrence, since 1998 it has been a declared nuclear weapons state, sitting outside of the Nuclear Non-Proliferation Treaty but agreeing to international inspection of its civilian nuclear facilities.[23]

In recent years, India has launched significant defense modernization efforts, focusing on indigenization and self-reliance under the "Make in India" initiative.[24] Reforms such as the creation of a chief of defense staff have aimed to enhance military coordination and strategic planning, which is an ongoing process.[25]

India's national security policy also involves strategic partnerships and alliances. India's deepening ties with the United States, illustrated by defense agreements like the Logistics Exchange Memorandum of Agreement and participation in the Quad, indicate a strategic pivot to mitigate China's influence and threat in the Indo-Pacific region. Simultaneously, India's engagement with other states, such as Russia, highlights a persistently diversified approach to defense procurement and diplomatic alignments.

Russia remains a strategic partner, part of India's balancing against China. At times this has made India somewhat dependent on Russian military imports, which is still reflected in the current composition of India's armed forces.[26] Nonetheless, the Modi government has recently tried to diversify defense procurement and reduce this dependency.[27] France is another important defense partner. Over the past forty years, India's partnership with France has included flagship projects like the Mirage and Rafale fighter jets and more recently procurement of submarines and helicopters.[28] The current Indian government highlights its strategic approach as being multi-vectoral, situating India outside the conception of a "two camps" approach to cyber diplomacy, in which the world is divided between Western liberal states and those spinning in orbit of a China-Russia authoritarian axis.[29] As yet, India does not have to and does not want to make that choice.

National security and domestic politics

Modi's ruling Bharatiya Janata Party (BJP) has leveraged national security narratives to consolidate its political base, particularly emphasizing a strong stance against terrorism and cross-border threats. The Pulwama attack in 2019 and the subsequent Balakot airstrike exemplify how national security incidents influence public opinion,[30] to the point that Modi's doctrine has been described as seeking to "securitise politics and politicise security."[31] There is no doubt that Modi's administration speaks the language of realism, emphasizing the importance of power, but there is debate about the extent to which Modi has effectively pursued the enhancement of India's hard power.[32] Some researchers argue that it is more accurate to describe Modi's approach as pragmatic and acutely aware of India's relational weakness vis-à-vis China.[33] In addition to the veil of uncertainty that already surrounds India's current employment of cyber operations, this ambiguity about what motivates and constrains Modi's wider decisions about the use of (covert and overt) force makes the operational element of India's cyber statecraft very difficult to interpret.

Turning from external threat perception to domestic politics, another prominent issue relevant to India's wider cyber strategy relates to the tension between digital freedom and censorship. India is far from alone in navigating this relationship, between the freedom of citizens online and efforts to enhance security in and through cyberspace. This is a global issue, but among democracies India is among the most assertive when it comes to such interventions. Under Modi, the Indian government has increasingly exercised its power to restrict speech, particularly on digital platforms. India has, for example, recently had one of the highest rates of internet shutdowns anywhere in the world.[34] While such shutdowns are generally localized and relate to areas of unrest, their increasing frequency and duration has implications both for digital freedom and for the economy.[35] This arguably reflects the domestic risk appetite, realist outlook, and acute threat perception that is noted above—and which appears, in a different context, to have led to India's rising bilateral tensions with Canada.[36]

More broadly, content deemed to threaten public order or national security can be removed from the internet, leading to concerns about overreach and suppression of dissent. For example, Section 69A of India's IT Act empowers the government to block online content in the interest of national security and public order, although in practice its application lacks uniformity.[37] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 impose stringent compliance requirements on social media platforms and digital news media. The government argues that these regulations are necessary to combat information manipulation, hate speech, and illegal content. However, critics claim they threaten privacy, encourage self-censorship, and provide the government with tools to suppress dissent.[38] This aspect of domestic policy highlights a perennial challenge for modern governments in navigating the balance between digital freedom and security. It reflects the Indian government's threat perception and its willingness to use the levers of executive power to address these threats in ways that compromise individual liberties. This does not make India an exception among the world's democracies, but simply highlights the importance of context and contingency in explaining how democracies respond to these dilemmas.

The politics and security implications of spyware

The use and abuse of commercial spyware has become an increasingly salient topic in global cyber diplomacy. The United States and its allies, such as the United Kingdom and France, have tried to build global agreement on principles of responsible state use of spyware and regulation of the spyware industry. India has not thus far participated in these initiatives.[39] Spyware controversies have affected many countries and India is no exception. In India's case, spyware issues have manifested in two ways: the use of spyware by the Indian government and the growth of an indigenous commercial spyware industry in India that has attracted a global clientele and attendant controversy.[40]

One of the most significant and controversial instances of spyware use in India involves Pegasus, a sophisticated spyware developed by the Israeli NSO Group. Pegasus has come to be associated with widespread global allegations of misuse by the NSO Group's customers. In India, reports have emerged from 2019 onward revealing that Pegasus was used to target individuals, including journalists, activists, opposition politicians, and even government officials.[41]

The Indian government has neither confirmed nor denied purchasing or using Pegasus,[42] often citing national security concerns.[43] Again, mirroring similar situations elsewhere—such as in the European Union—the ambiguity and lack of transparency surrounding spyware allegations have led to widespread demands in India for accountability and independent investigation. The Supreme Court of India, in response, established a technical and an oversight committee in 2021 to investigate these allegations, reporting the following year that stronger safeguards were needed, but without publicly apportioning blame to the government—which had not cooperated with the inquiry.[44]

In parallel, India's national spyware industry has grown, driven by both government demand and global private sector opportunities. Indian companies are developing a range of surveillance and monitoring tools, catering to the needs of law enforcement agencies and private clients. Indian law enforcement and intelligence agencies also rely on domestically developed spyware for various purposes, including criminal investigation, counterterrorism, and maintaining public order. The cyber-related private sector in India also appears to have been used for digital intelligence against foreign targets.[45] For example, the DoNot Team (also known as APT-C-35) has been associated with targeting apparently aligned with Indian state interests.[46] The ecosystem of companies associated with such threat activity appears to have grown over the past twenty years; techniques and targeting have similarly evolved across this period.[47]

India has participated in neither the U.S.-led effort nor the UK- and France-led effort to build agreement on how states should responsibly use and effectively regulate commercial spyware.[48] In theory, India's nonparticipation might be explained by its traditional emphasis on strategic autonomy and its reluctance to embrace Western initiatives to which it has not contributed as an original, shaping partner.[49] But there is nothing to stop India from driving a parallel initiative—for example, one pursued under the more congenial auspices of a Global South forum such as India-Brazil-South Africa (IBSA).[50] Its failure to do so suggests that strategic autonomy and upholding India's sovereign right to make decisions about when and how it uses spyware are significant priorities that shape India's decision not to engage further on this issue.[51] It should also be noted that, in this, India is not alone in international politics: a striking aspect of both the U.S.-led and UK- and France-led processes is that they have, thus far, attracted relatively small numbers of states. But so long as India remains outside of such initiatives, the country's large commercial spyware industry is somewhat insulated against these efforts to constrain it.

National security, bureaucracy, and cyber statecraft

Cyber statecraft emerges from a political process, and its operational aspects are shaped by the state's national security decisionmaking apparatus.[52] The bureaucratic politics of national security in India inevitably involve multiple powerful ministries and agencies, each with a different stake in cyber statecraft. The Ministry of Defence (MOD), the Ministry of Home Affairs (MHA), the MEA, and the intelligence agencies are the main departments and institutional actors. The influence of these entities is shaped by their responsibility for specific aspects of national security. This is all coordinated under the authority of the prime minister, assisted by the national security adviser (NSA). The NSA is the prime minister's principal adviser and leads on institutional coordination, strategic planning, and crisis management.[53] The NSA also plays a role in international security affairs.[54]

The National Security Council (NSC), chaired by the prime minister, is the principal advisory body and has strategic oversight for cybersecurity policy. For cyber operations, including digital espionage, whether conducted by a part of the Indian state or (conceivably) by proxies at its behest, the NSC is the relevant top-level, formal decisionmaking apparatus.

Regarding cyber policy, different departments have different policy or operational equities, with the MOD holding the equities for cyber defense and the use of cyber capabilities to support the armed forces. The integration of capabilities within the armed forces is part of ongoing efforts to improve inter-service coordination and to streamline defense affairs.[55] In contrast, cyber-relevant aspects of domestic security and counter terrorism are within the purview of the MHA. Outside of the operational space, the MEA influences national security through diplomatic agreements and engagements that involve defense and security. Formally, however, the MEA is not part of the national security apparatus.[56] Similarly, while not directly involved in security operations, the Ministry of Finance allocates budgets for defense and internal security. The financial control it exercises over defense spending gives it indirect but substantial influence nonetheless.

Like many other states, India has developed the institutional, policy, and regulatory components of its cyber statecraft over the past twenty years. The early 2000s saw emergent cyber institutionalization, with the creation of a national computer emergency response team (CERT-In) and a national cyber intelligence agency (the National Technical Research Organisation) in 2004.[57] Legislative reform followed in 2008, focused on improving the lawful basis for cyber operations and ensuring the protection of critical infrastructure.[58] India's first National Cyber Security Policy (NCSP) was formulated in 2013. This was the first dedicated policy document providing general measures protecting cyberspace from state and non-state threats and ensuring information infrastructure security.[59] The policy outlined strategic objectives, guiding principles, and specific actions to enhance India's cybersecurity posture. The primary objectives of the NCSP were securing cyberspace by safeguarding critical information infrastructure, reducing the vulnerabilities of information and communications technology by implementing robust cybersecurity measures, promoting public-private partnerships and international cooperation, and spreading awareness about cybersecurity across all sectors of society.

The National Cyber Security Coordinator's (NCSC) Office—part of the NSC Secretariat—emerged out of the 2013 reform and has the primary coordinating role for domestic cybersecurity. The NCSC leads the NSA in shaping domestic cybersecurity policies, mitigating current threats and preparing to address future cyber threats.[60] The NCSC is responsible for overseeing the National Cyber Coordination Centre (NCCC) and the National Critical Information Infrastructure Protection Centre (NCIIPC). The NCCC generates vital situational awareness and facilitates timely information-sharing to protect against cyber threats, while the NCIIPC focuses on safeguarding critical infrastructure from cyber attacks. Army Lieutenant General M.U. Nair, the current NCSC, has emphasized the importance of a collaborative approach to cybersecurity.[61] The NCSC also plays a key role in advising and assisting the government on policy and strategic issues related to cybersecurity. This includes working closely with CERT-In, which issues alerts and advisories on cyber threats and coordinates the national response to cyber incidents.

CERT-In and the Cyber Crime Coordination Centre (I4C) are important entities in the country's domestic cybersecurity landscape, each playing distinct yet complementary roles. CERT-In, established in 2004, operates under the Ministry of Electronics and Information Technology (MeitY). It is the national nodal agency for responding to cybersecurity incidents. The I4C was launched in 2018 and operates under the MHA. It is designed to combat cyber crime in a comprehensive and coordinated manner.

Specific responsibilities for wider cyber-related policy and operations are managed by a variety of different institutions. Government agencies such as MeitY and the National Technical Research Organisation (NTRO) play key roles in implementing cybersecurity measures. Additionally, the government has launched initiatives such as the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to combat cyber threats at the national level.[62]

MeitY is primarily responsible for promoting the country's digital ecosystem, which includes ensuring cybersecurity. MeitY oversees several key areas, such as the development and enforcement of cyber-related legislation, advancing research and development in cybersecurity, and enhancing the digital infrastructure to safeguard against cyber threats.[63] One of MeitY's prominent initiatives is the National Cyber Security Policy. But MeitY also administers important projects and frameworks such as CERT-In, which is responsible for responding to cybersecurity incidents and providing early warnings on potential threats. The ministry is the primary beneficiary of the recent doubling of India's cybersecurity budget, highlighting its importance in the national apparatus.[64]

These domestic, cybersecurity-focused national efforts are separate from India's military cyber, strategic cyber, and cyber diplomacy activities. India's military cyber operations are pursued operationally within the Defence Cyber Agency (DCYA)—a relatively new, tri-service entity, created in 2018, that focuses specifically on cyber defense and cyber operations as these apply to the armed forces' capabilities, platforms, networks, and systems. The DCYA is complemented by a civilian cyber capability provided by the NTRO, which is part of the Prime Minister's Office. The DCYA therefore contributes to India's cyber deterrence and enables it to use cyber capabilities as a tool of statecraft, actively pursuing national strategic objectives. It was estimated in 2018 to comprise 1000 personnel—but with no further detail about the different roles and skill levels within this complement.[65]

Strategic cyber operations—including espionage, disruptive and destructive operations, and online information operations—are the purview of two agencies under the direction of the prime minister: the NTRO and the external intelligence agency, Research and Analysis Wing. These are, understandably, the least publicly visible aspects of India's cyber statecraft. Strategic cyber operations are similarly obscured in all states, although there are some interesting exercises in strategic communication about the use of cyber operations to further national strategic objectives, such as the 2023 Responsible Cyber Power in Practice publication by the UK's National Cyber Force.[66] It is an open question whether, at an appropriate point of maturity in offensive cyber capability development and employment, India might find it strategically useful (for signaling purposes, to reduce the risk of misperception) to make a similar departure from its traditional secrecy about operational matters.

Given the somewhat busy inter-institutional context outlined above, in which several agencies and departments retain operational equities, India's MEA must coordinate between the institutions to shape the objectives that India's diplomats bring to international forums of debate about cyber norms. Like in other states, while diplomats pursue India's cyber diplomacy objectives, they do not own the operational equities that are at stake in the establishing of national red lines.[67] It is clear from public statements over the past decade by a range of India's senior diplomats and securocrats that a plurality of views exists within the Modi government over the desirability of multilateral negotiations that might bring more binding constraints on states' freedom of action in cyberspace.[68] In the absence of clear public doctrine regarding Indian cyber operations, it is an interpretive challenge to understand how India's cyber diplomacy relates to the more operational aspects of India's cyber statecraft.

India's Cyber Threats

Over the past twenty years, and particularly over the past decade, India has undergone a rapid digital transformation—driving South Asia to become one of the world's fastest growing regions for internet connectivity.[69] In 2015, India already had 120 million users of the internet, making it the world's third-largest user base, but with considerable room to grow considering its population.[70] By 2023, internet penetration had reached over 50 percent of the country's 1.4 billion population.[71] Digital technologies are being adopted across sectors and in both urban and rural areas, transforming the sale and consumption of goods and services and reducing the developmentally damaging digital divide.

In the past decade, the digital economy has contributed significantly to growth in India. In 2015, it was estimated that the internet contributed 1.6 percent of India's GDP. As of 2025, the Indian IT industry alone employs 5.4 million people, estimated to contribute 10 percent of its GDP, and more than half of its services exports.[72] Technology is also at the heart of flagship government initiatives designed to widen access to public and essential services. Aadhar, the digital biometric identity system, is providing Indians with a ubiquitous digital identity and access to government services, while the Unified Payments Interface is democratizing cashless transactions. Both systems have high levels of adoption, but they represent attractive targets for attackers as critical digital infrastructures.[73]

Digital connectivity and innovation are important factors in the Modi government's economic strategy. But, as the United States itself has found, the more digitized a country becomes, the more targets it presents for cyber criminals and malevolent state actors to exploit.[74] One recent estimate places India's private sector as the second-most cyber-attacked in the Asia-Pacific region, with over 3000 such attacks per week, behind only Taiwan.[75] As in many other countries, during the coronavirus pandemic, cyber attacks targeting individuals, businesses, and government agencies increased substantially. This trend was particularly evident in India, highlighting its systemic cyber vulnerabilities.[76] Despite considerable administrative reforms over the last decade, India remains a prime target for cyber attacks, with ransomware payments estimated at $1.54 billion over ten months in 2023.[77] Again, it is important to distinguish the global picture—in which international efforts to counter ransomware crime are yet to have a significant discernible impact on the incidence of this crime—and the specifically Indian context, in which government and other stakeholders use the levers available to them to mitigate existing threats and build resilience.

The following section focuses on four main cyber threats facing India: state-sponsored attacks, espionage operations, cyber crime, and information operations from state and non-state actors.

State-sponsored attacks and espionage

State-affiliated cyber threats are most notable in the form of espionage and infrastructure-targeting. Adversarial nations, particularly China and Pakistan, have been alleged to be implicated (sometimes jointly) in numerous cyber incidents aimed at undermining India's strategic and economic interests.[78] Conversely, cyber espionage threat actors involved in targeting China have been alleged to have an India nexus.[79]

Chinese (reportedly state-affiliated) groups have been linked to cyber espionage campaigns targeting sensitive sectors such as defense, telecommunications, and government networks. The i-Soon leaks early in 2024 and the insight they provided into China's hacking industry highlighted this potential link.[80] These espionage campaigns have targeted government, the military, and the private sector in India.

In addition to cyber espionage, India has also been the target of cyber attacks against critical infrastructures such as power plants. Some of these incidents are believed to originate in China.[81] In October 2020, against a backdrop of bilateral tensions between China and India over a disputed border, the city of Mumbai experienced a significant power outage. Subsequent reporting suggested that the outage was due to a suspected cyber attack.[82] The incident disrupted daily life and raised concerns about the vulnerability of critical infrastructure to cyber threats. According to a report by Recorded Future, malware connected with the threat actor known as RedEcho—an actor believed to be associated with the Chinese state—had been present on India's electricity network at the time of the outage.[83] The group's activities included deploying malware in systems belonging to Indian power generation and transmission organizations. The report was, however, unable to examine the claim that the Mumbai outage was directly attributable to a cyber attack.[84] And a subsequent Indian government inquiry called into doubt the cyber attack scenario, suggesting that equipment failure was the cause.[85]

Whatever the ultimate provenance of the Mumbai outage, the wider malware campaign against Indian infrastructure highlights the strategic context in which cyber operations target India's critical infrastructure. India is obviously not the only state in which Chinese threat activity on infrastructure is suspected. There are several factors that shape a state's response to being the victim of a cyber operation.[86] The United States government, for example, has formally attributed both digital espionage and infrastructure pre-positioning operations to Chinese threat actors, such as Flax Typhoon, Salt Typhoon, and Volt Typhoon.[87] Three notable differences in the India-China case are that: (1) there is suspicion that a disruptive cyber operation has actually been conducted against infrastructure targets, rather than a pre-positioning phase; (2) the cyber interactions between India and China take place in the context of a bilateral relationship that includes a disputed border; and relatedly, (3) the Indian government has been much more circumspect than the U.S. government in its public handling of these issues.

One pertinent observation is that, given the claims and counter-claims made by India and China about one another as cyber threats, it might well be difficult for these two countries—either bilaterally or collaboratively within a grouping such as BRICS—to develop shared proposals to advance the global agenda of cyber diplomacy. They might find common cause on a range of less controversial issues in the bilateral relationship, such as the importance of sovereignty and the role of states in internet governance, or exhortative rather than prohibitive global cyber norms. Unless the recent rapprochement between Modi and Chinese President Xi Jinping fundamentally transforms the bilateral relationship, there is much that divides India and China despite their cooperation on certain issues. Cyberspace appears to be a domain in which these complexities and tensions are given heightened operational expression. A bilateral cyber risk-reduction dialogue might at some point be desirable to both sides, but, somewhat akin to the agreement in 2015 between Xi and then U.S. president Barack Obama, the outcomes of such an agreement would be contested and fragile, and the momentum to negotiate it would likely only arise when both sides perceived it as advantageous.[88]

Cyber crime

Cyber crime by nonstate actors is another rapidly growing concern for India, with attacks becoming more frequent and sophisticated. Sometimes these criminals are based within India itself,[89] but there is also considerable foreign-origin cyber crime targeting India, particularly regarding ransomware crimes.[90] None of this is surprising: as the world's fifth largest economy, with a thriving digital sector, it should be expected that India would experience the global trend of rising cyber crime. And as the global effort to counter ransomware cyber crime has demonstrated, no single state has the power to solve this problem, and it is proving difficult for existing multi-state and multi-stakeholder efforts to counter.

According to the Oxford Cybercrime Index, which ranks countries most affected by cyber crime, India ranks tenth, below the UK and Brazil, but above Iran and Belarus.[91] According to India's National Cybersecurity Coordinator, Lieutenant General M.U. Nair, ransomware payments doubled between 2022 and 2023, and India experiences nearly double the global average of cyber incidents.[92] Cyber criminals target individuals, businesses, and government entities. Cyber crime includes ransomware, data breaches, and fraud. Ransomware has affected numerous Indian businesses, causing operational disruptions and financial losses. Similarly, data breaches targeting financial institutions and e-commerce platforms have compromised the personal and financial information of millions of Indians. This vector has recently expanded to targeting election systems and databases.[93]

In August 2018, Cosmos Bank, one of India's oldest cooperative banks, suffered a massive breach by cyber criminals, resulting in a loss of approximately $13.5 million (94 crore rupees). Cyber criminals infiltrated the bank's systems and manipulated the ATM switch server, enabling them to authorize fraudulent transactions across twenty-eight countries. The attackers withdrew cash from ATMs and conducted unauthorized SWIFT transactions, exploiting vulnerabilities in the bank's network security. This crime was attributed to North Korean threat actor the Lazarus Group.[94] The same year, another major data breach was reported involving India's Aadhaar system, managed by the Unique Identification Authority of India (UIDAI). Investigations revealed that unauthorized access to Aadhaar data was being sold on the black market.[95] For as little as 500 rupees (approximately $7), individuals could obtain access to the personal information of over a billion Indian citizens, including biometric data. This breach raised significant concerns about data privacy and the security of the Aadhaar system.[96] In March 2021, digital wallet and payment service provider MobiKwik faced allegations of a massive data breach affecting 3.5 million users. Hackers reportedly accessed and posted sensitive user data, including names, email addresses, phone numbers, and payment information, on the dark web.[97] The breach exposed vulnerabilities in MobiKwik's security infrastructure and highlighted the growing threat of cyber crime targeting financial technology companies in India.

It is notable that while the state-sponsored threats facing India in cyberspace mirror its principal non-cyber threats (for example, from China and Pakistan), when it comes to cyber crime, India faces similar attacks to those on many other states. For example, despite India's strategic ties to Russia, Russian ransomware criminals have victimized Indian targets as readily as targets in states with worse bilateral relations.[98] The issue is not that the Russian state is directing cyber criminals to victimize India. It is that the Russian state is either unable or unwilling to dissuade them from doing so. There is, however, as yet no evidence that this situation is adversely affecting that wider bilateral relationship.

Terrorist propaganda

Another category of non-state threats facing India in cyberspace is terrorism. Organizations such as the Islamic State (IS) and al-Qaeda have used online platforms both for recruitment, indoctrination, and spreading propaganda in India. In 2014, al-Qaeda announced in a widely shared online video the formation of its Indian subcontinent branch, al-Qaeda in the Indian Subcontinent. The video called for attacks against Indian targets and aimed to incite violence among Indian Muslims.[99] Such propaganda efforts are part of broader strategies of radicalization and regional destabilization. In 2014, the arrest of Mehdi Masroor Biswas, an Indian engineer from Bangalore who ran a prominent pro-IS Twitter account, highlighted the group's digital reach in India. Biswas's account, which had tens of thousands of followers, was used to glorify IS activities and attract new recruits.[100]

Hacktivism

Hacktivist groups such as Anonymous India have conducted cyber protests and data leaks to promote a variety of campaigns. These activities, while often nonviolent, can cause significant reputational damage and some operational disruption. For example, hacktivists have defaced Indian government websites and released sensitive information to facilitate protests against government policies. Most prominently, Anonymous India launched a series of cyber attacks in 2012 dubbed "Operation India" in protest against the Indian government's stance on internet censorship and corruption. The group targeted several government websites, including the websites of the Indian National Congress party, the Bharatiya Janata Party, and the Supreme Court of India.[101] These attacks involved defacing websites and leaking sensitive data to draw public attention to issues of transparency and freedom of speech.

More recently, Indonesian hacktivist groups have hacked and defaced Indian government websites in response to the Indian position in the conflict between Israel and Hamas.[102] This hacktivism aims to amplify dissent and to disrupt governmental operations as a form of digital protest. None of this implies that India is uniquely a victim of hacktivism. The Canadian government's Center for Cyber Security, for example, recently stated that, during the on-going bilateral dispute between Canada and India, a "pro-Indian hacktivist group" had claimed responsibility for disrupting and defacing websites, including that of the Canadian Armed Forces.[103]

India's ongoing digital transformation, marked by increasingly widespread internet penetration and digital technology adoption across various sectors, has made the country an increasingly attractive target in cyberspace. The threat landscape encompasses both state and non-state actors. India is not unique in this respect, given the recent global rise in cyber threats. Nonetheless, as an increasingly large and increasingly digitized economy, India is a bigger target than many. The next section explores how Indian policy and strategy is used to counter these cyber threats.

Cybersecurity Strategy

The past decade has been a period of intensifying effort by states to develop effective, well-coordinated cybersecurity strategies. This effort includes improvements in domestic governmental cybersecurity apparatus and legislation, as well as improving relationships between government and domestic stakeholders, and between the state and its international partners. As outlined above, India's experience over the past twenty years mirrors these wider global trends.

Most recently, in April 2023, CERT-In published a series of new directives for reporting cybersecurity incidents, which was followed later that year by the publication of a National Cyber Security Reference Framework (NCRF).[104] The NCRF was produced by the NCIIPC and funded by the NSC. It superseded the NCSP from 2013, providing a structured framework for identifying the cybersecurity responsibilities of different institutions and stakeholders. The NCRF focuses particularly on seven sectors of critical infrastructure—banking and financial services, energy, government enterprises, healthcare, strategic enterprises, telecommunications, and transportation—that have seen the sharpest rise in cybersecurity threats. The NCRF improves guidance on governance, management, and the architecture of both information technology and operational technology systems.[105]

Like other countries over the last decade, India has recognized that the pace and intensity of cyber threats requires a revised national response at the strategic level. The NCRF's focus on areas of critical infrastructure highlights the priority of threats to infrastructure from cyber criminals and hostile state actors. While the publication of a new framework a decade after the NCSP is a slow response, the more important question is how effectively the government will coordinate national cybersecurity policy implementation and operations in practice. The NCRF is still comparatively new, but the government will need to monitor feedback and continuously review its effectiveness in countering cyber threats.

Cyber Capabilities

India is not regarded as a global top-tier cyber power.[106] It has even been described as a "muddling cyber-power."[107] But assessment of India's cyber power is made difficult by the lack of open-source information about its capabilities and operations, or of publicly available cyber doctrine explaining the principles behind their use.[108] Nonetheless, it is clear that cyber threat actors engaged in intelligence collection, and assessed as having a possible Indian connection—without any evidence of a governmental affiliation—have become more numerous, more capable, and more diverse in their targeting over the past decade.[109] There is very little public visibility regarding India's capabilities in cyberspace—but absence of evidence is not necessarily evidence of absence.

Recognizing the importance of cyber resilience and defense, India has focused on developing cyber capabilities for intelligence collection, defensive, and offensive operations. The NCCC, established in 2015, aims to streamline cyber-related intelligence collection.[110] Resource constraints and skills shortages reportedly undermine its effectiveness—a globally ubiquitous theme for governmental cybersecurity. India's cybersecurity workforce requirement is estimated to be around 1.5 million professionals by 2025. Its cyber workforce gap—currently estimated at 30 percent —is expected to widen even further as demand grows faster than the available supply.[111]

From a military perspective, the Indian Armed Forces have invested in both defensive and offensive cyber capabilities; their capacity is likely equal or superior to that of Pakistan, but inferior to that of China.[112] This is partly due to the lack of institutional prioritization of emerging technologies for military purposes.[113] India's offensive cyber capabilities are developing, and the MOD has recently operationalized its command cyber operations and support wings.[114] Yet they are characterized by regional focus and notable limitations.[115] In the past, India's offensive cyber operations have reportedly primarily targeted Pakistan.[116] While firm evidence is elusive, it seems plausible to speculate that, over the past five years, India's offensive cyber program has been affected by the same shift in strategic thinking that has influenced non-cyber activities in India's statecraft: affording a higher priority to development and employment of capabilities to address China.

India has the wider foundational infrastructure needed for offensive cyber strategies, including a robust information technology sector, intelligence, surveillance, and reconnaissance capabilities, and relevant institutions like the DCYA. As mentioned above, the DCYA, established in 2018, is designed to conduct offensive and defensive cyber operations, functioning similarly to a cyber command structure. In addition to the DCYA, the civilian NTRO also retains a cyber operations mission (in addition to its digital espionage mission), but there is little public clarity about how effectively the two complement each other—or whether deconfliction is even necessary.[117] There is little public information about the NTRO, the budget and operations of which are classified, although recent reporting suggests the intra-government view is that the agency requires reinvigoration under new leadership.[118] Similarly, public information suggests that the DCYA is an inchoate agency, whose development is proceeding more slowly and with fewer resources than the armed forces had desired.[119] In both cases, information is scarce, but the tentative conclusion regarding India's national cyber operations institutions is that they are not yet where India needs them to be.

Despite ongoing investment in capability development, India's offensive cyber efforts could be undermined by the absence of a comprehensive and cohesive cyber strategy, as well as by the resource constraints reportedly noted above.[120] These gaps could inhibit the full operationalization and strategic use of offensive cyber capabilities. Without a unified strategy, resource allocation and capability integration will remain inconsistent, limiting the overall effectiveness of India's cyber operations.[121] But without insight into the inter-institutional status quo, it is difficult to appraise the current state of offensive cyber maturity and coordination. Perhaps the most obvious question from the outside is where India's government prioritizes investment in military cyber (both cyber defense and cyber operations in support of the armed forces) in comparison to investment in cyber capabilities to deter, or if necessary respond to, hostile actors' disruptive or destructive operations against India's critical infrastructure. This debate is wholly opaque to outsiders, but it is likely that the bilateral tensions with China after 2020 have intensified efforts to improve the maturity and strategic utility of the latter capabilities.

Beyond low-level degradation and website defacement activity—often associated with moments of tension—between India and Pakistan, there have also been reports of similarly low-level activity against Canadian government targets in 2023, during a period of bilateral tension with India (see below).[122] This activity was reportedly claimed by a hacker group known as the Indian Cyber Force.[123] This group is reportedly reactive, for example conducting similar low-level disruptive attacks in subsequent months against Qatari and Hamas-related websites.[124] While the activities of this group appear to be aligned with a certain conception of India's interests, it is not publicly known whether or to what extent this group is associated with Indian governmental or political actors.

There is significant ambiguity about India's cyber doctrine.[125] This ranges from questions about potential use of proxies to specific questions about how the DCYA and NTRO might operate. Whether this ambiguity is a bug (a simple absence of clear doctrine) or a feature (a deliberate effort to increase uncertainty) is less apparent. Of course, there could be elements of both. Notwithstanding, India's growing cyber capabilities are supported by a dynamic private sector and foundational cyber institutions. It would be prudent for India to continue to improve its cyber capabilities—the public statements of senior Indian officials (see below) suggest they recognize this and that political will perseveres, despite a few dissonant notes about the institutions responsible for cyber operations.

For India to benefit fully from its cyber capabilities as tools of national statecraft, the government will need strategic patience and an integrated, whole-of-nation approach to cyber statecraft.[126] It will also need to be clear about the effects it wants to achieve and how these serve specific national objectives.[127] The DCYA must, for example, coherently prioritize between different objectives, integrate cyber effects in support of each service in the armed forces, and (if it conducts cyber operations below the threshold of armed conflict) deconflict clearly with NTRO and the Research and Analysis Wing (India's external intelligence service).

India's Cyber Strategy and Foreign Policy

Modi's Foreign Policy Agenda

To understand how cyber policies and equities contribute to India's national strategy, it is important to situate cyber-related issues within the context of Indian foreign policy, particularly as it has been pursued under Modi since 2014. India's approach to cyber diplomacy, like India's other foreign policy, is influenced by a combination of historical legacies, regional dynamics, and evolving debates about global governance. It is important to understand how India's cyber diplomacy is situated in this context, rather than seeing Indian cyber diplomacy through a distorting prism of standing between two camps of like-minded states and authoritarian states.

Whilst significant executive power has always been vested in the prime minister and his office, Modi has reportedly centralized foreign policy decisionmaking to a considerable extent, driving key initiatives and setting the strategic direction.[128] Under Modi, the Prime Minister's Office has become the pivotal player in foreign policy, overseeing critical decisions and ensuring alignment with the broader political agenda.[129]

The MEA also remains a crucial actor in formulating and implementing foreign policy. It provides expert advice, conducts diplomatic negotiations, and manages India's international relations on a day-to-day basis. On the other hand, the Indian defense establishment, including the MOD, the armed forces, and the intelligence agencies, significantly influences the more securitized aspects of foreign policy. The long-serving National Security Adviser Ajit Doval plays a key role in coordinating between different branches of the government and directly advising Modi.[130] From the perspective of cyber statecraft, it is clear that securocrats are likely to have most influence in calibrating the development of India's tacit doctrine and decisions about the employment of capabilities. This establishes the context and boundaries within which India's diplomatic positions can be crafted regarding the agreement of norms of responsible state behavior in cyberspace.

When Modi entered office in 2014, commentary speculated that his foreign policy would be steeped in nationalism but also reflect pragmatic prioritization of relationships—including with China—that would promote India's economic growth.[131] Furthermore, alongside its deprecation of the Nehruvian concept of nonalignment, Modi's administration has made much of the importance to India of pursuing a diplomacy of "multi-alignment.[132] A key element of this approach—mindful of the threat posed by China—has been maintaining India's relationships with both the United States and Russia. This has become an even more delicate balancing act since Russia's full-scale invasion of Ukraine in 2022, which left it more reliant on China. Some commentators concerned that India can no longer rely on Russia vis-à-vis the China threat.[133] Others doubt whether Western states should pursue close relations with India, given Modi's domestic policies and his willingness to maintain such close ties to Russia.[134]

Modi's foreign policy has emphasized the principle of strategic autonomy, echoing a wider priority of his governing agenda: the need for *atmanirbhar bharat* (self-reliance).[135] An important motivation for the cultivation of strategic autonomy is the perceived need to decouple from China and "derisk" that bilateral relationship. While India would prefer to regard China simply as a major trade partner, the recent turn in China's foreign policy—and specifically the issue of border tensions—has forced Modi to adopt a different approach, particularly from his second term (starting in 2019) onward.[136] Tensions with China, given China's rising military power and India's relational weakness, have worried both India's political elite and its population as a whole.[137] One consequence of this perception shift—which is likely to endure despite the apparent diplomatic progress made in late October 2024 in reducing risk and building confidence over the bilateral border issue[138]—is that India is increasingly careful to separate economic and security-related issues in the bilateral relationship. This is a step that will be familiar to readers in North America and Europe.[139]

Lacking the military power to rely solely on itself to balance China, India has needed to pursue a range of closer ties to the United States and other states interested in balancing against China.[140] This can be seen most clearly in the rejuvenated Quad partnership. Over the past three years, the Quad has been developing an initiative to improve the cybersecurity of critical infrastructure, supply chains, and the software development process; to facilitate coordination and knowledge-sharing between the Quad's members; and to enhance cybersecurity across the Indo-Pacific region.[141]

Beyond China, the Modi administration has pursued regional cooperation as the cornerstone of its foreign policy. The South Asian "neighborhood" is, understandably, India's first priority.[142] Precisely because of its relative size in the region, India's diplomacy toward its neighbors needs to reassure and at times placate them—what one scholar has referred to as managing the effects of "small neighbor syndrome"[143]—and there are limits to what India can achieve.[144] The Modi government has pursued this priority through initiatives such as the "Act East" policy since 2014, with a focus on Pakistan and Bangladesh.[145] The extent to which India's immediate region demands executive bandwidth fluctuates over time; the recent political crisis in Bangladesh, for example, necessitated more urgent prioritization.[146]

Modi's geopolitical ambitions for India certainly extend beyond its immediate neighborhood, toward a more influential global role. India also engages in multilateral forums such as the BRICS and the G20. BRICS is important as a platform for signaling and for enabling India to amplify the voice of the Global South in international debates. BRICS has, however, achieved relatively modest outcomes in policy terms as yet, primarily in efforts to diversify international financial arrangements and institutions.[147]

For all Modi's ambition, it is clear that there are limits to what India can achieve globally. Karthik Nachiappan, for example, suggests that India should be seen more as a "premature power" than a "rising power," reflecting the sharp constraints on wider diplomatic action implicit in India's immediate need to pursue economic growth and secure its periphery.[148] This sense of limits—and indeed of relational weakness—is also discernible in relations with China, where, although India has sought to foster balancing partnerships with other states, "New Delhi's relative weakness compels it to avoid provoking Beijing."[149] How India juggles the extent and intensity of these balancing commitments alongside direct management of its bilateral relationship with China will shape its wider statecraft, in which cyber diplomacy and cyber operations both play a part.[150]

One issue that has appeared to complicate India's closer partnerships with Western states is the ongoing controversy over alleged Indian involvement in extraterritorial killings. Under Modi, there has reportedly been an increase in external operations against individuals and groups deemed to be a threat to India's national security.[151] In 2024, for example, India's defense minister appeared to confirm the existence of a targeted killing policy against individuals based in Pakistan and associated with Islamist movements.[152]

Canadian Prime Minister Justin Trudeau publicly raised serious allegations in 2023 of India's involvement in the assassination in Canada of a Sikh separatist, Canadian national Hardeep Singh Nijjar.[153] Since then, Canadian authorities have charged three Indian nationals.[154] Whilst the Indian government denied involvement, the incident has certainly had deleterious consequences for the bilateral relationship, with India expelling forty-one Canadian diplomats and suspending the processing of visas in response to these accusations.[155] There have also been (see above) reported Indian hacktivist disruptions of Canadian government websites following these statements.

This issue has also strained India's relations with the United States.[156] Last year, American prosecutors charged an Indian national suspected of planning another assassination, this time in the United States. The indictment revealed the existence of a large-scale assassination plot targeting numerous Khalistani activists across the United States and Canada.[157] This has already had specific repercussions for Indo-U.S. security relations, with the U.S. Congress delaying an arms sale.[158] The bigger issue is the possibility that this episode will ultimately undermine the trust and slow the momentum behind India's closer ties with the United States and other states keen to balance against China. External Affairs Minister S. Jaishankar's books, published over the last decade, articulate a vision of foreign policy that combines both an active pursuit of multiple vectors of diplomacy with a focus on developing and, where necessary, using hard power to pursue India's goals.[159] Perhaps the most plausible interpretation of the targeted killing issue—notwithstanding the Indian government's denial—would be that, if such a policy exists, it reflects an exploratory dimension of India's statecraft, willing to calibrate and re-calibrate actions according to their impact. A number of recent articles by Western commentators have explored a similar theme, namely how to manage a relationship with India that is premised on an alignment of interests that are shared only up to a point.[160]

For Jaishankar, India's contemporary foreign policy embraces the imperative of "engaging in multiple directions and constantly balancing competitive relationships."[161] The priority of maintaining a "multipolar Asia" and balancing against security risks from China explains India's continued pragmatic relationship with Russia, despite the dismay of India's Western partners.[162] Whether or not Russia ultimately proves itself an unreliable partner for India vis-à-vis China, this should not be the focus of Western diplomacy with India. Instead, Western diplomats should focus on building from the starting point of initiatives such as those pursued under the umbrella of the Quad. The agenda should be one of pragmatic, incremental, and mutually beneficial projects that are unencumbered by high-flown rhetoric about alliances and shared values.[163] Jaishankar applies this approach to foreign policy generally and to engaging India as part of global cyber diplomacy specifically.

Indian Cyber Diplomacy

Cyber diplomacy plays a growing role in India's foreign policy agenda.[164] For example, the MEA created a dedicated Cyber Diplomacy Division (CDD) in 2017, the year it hosted the Global Conference on Cyberspace, to complement the existing division of Disarmament and

International Security Affairs. CDD covers both bilateral cyber dialogues and multilateral cyber negotiations, including the UN cyber norms process, internet governance, and international negotiations about data protection.[165] This was an unsurprising development, given the increasing importance of cyberspace in national security, economic development, and international relations. India's cyber diplomacy is characterized by a mix of confidence- and capacity-building measures, diplomatic engagement, and efforts to shape global cyber governance norms. Its highest cyber priorities are consistent with Jaishankar's philosophy that there is a general need for states to pursue a "securitizing of the routine" to guard against foreign subversion and threats to critical infrastructure.[166]

There is some disagreement in scholarly and policy-focused literature about how best to interpret India's record in cyber diplomacy. Some scholars emphasize that India has been actively engaged for two decades in United Nations processes from the Group of Governmental Experts (GGE) onward and has a track record of explicit support for multilateral processes shaping norms of responsible state behavior in cyberspace.[167] They cite, for example, India's successful advocacy of the Open-ended Working Group (OEWG) as a more globally representative forum for cyber norms discussion than the GGE.[168] Yet other scholars have been underwhelmed by India's substantive achievements in cyber diplomacy.[169] Moreover, some are skeptical of how carefully coordinated India's diplomatic positions have been, both within government and between governmental and other stakeholders. They argue, quite plausibly and reasonably, that India most keenly engages only on those issues it prioritizes as strategically important.[170]

In a 2016 speech, India's then deputy national security adviser Arvind Gupta clarified India's globally mainstream view that "there is now a growing recognition that international law, particularly the UN charter, applies as much as to cyberspace as to other domains." He further observed, somewhat elusively, that debate was "inconclusive" on whether "intervention through cyber means in other countries' networks…is justified or not."[171] Gupta commented in that speech that there might be a say-do gap between what states claim while participating in cyber norms diplomacy and their actual conduct in cyber operations: "It is quite possible that states may be clandestinely developing arsenal of tools of cyber-attack even as they discuss the need for accepted norms in cyberspace."[172] This comment perhaps indicates one source of India's reluctance to become more proactive in the cyber norms debate. Through the lens of Jaishankar's pragmatism, it is possible to speculate about the nuanced relationship between diplomacy and action in India's cyber statecraft.

Notwithstanding the more operational aspects of India's cyber statecraft,[173] India advocates for a rules-based international order in cyberspace, emphasizing principles such as the peaceful use of cyberspace, respect for sovereignty, and non-interference in the internal affairs of states.[174] India's cyber diplomacy appears therefore to be situated in the mainstream of global efforts to promote responsible state behavior and prevent the militarization of cyberspace. One former senior Indian diplomat, Ambassador Asoke Mukerji, who played a significant part in coordinating India's cyber diplomacy dialogues, has even advocated for a more binding international cyber agreement.[175] This opinion is an outlier: it is more common for India's cyber-diplomatic positions to reflect specific national interests. For example, India has emphasized the importance of trusted supply chains in cyber diplomacy forums, indicating the high national security priority of this issue in light of bilateral tensions with China.[176] Similarly, in its cyber-related activities under the auspices of the Quad, India is pursuing enhancements of its domestic cyber security capacity and not engaging with other Quad members on more controversial issues of potential diplomatic disagreement.

Arindrajit Basu has argued that there is relatively little disagreement between domestic stakeholders about India's role in global cyber diplomacy. He suggests that the reason for this is that none of these stakeholders have been able to precisely articulate a clear view about what India actually wants to get out of the global process, apart from instrumental improvements in its domestic cybersecurity capacity and resilience.[177] Basu's argument reflects wider recognition that public debate about cybersecurity should be broader and deeper than it presently is.[178] The result in India, argues Basu, is somewhat "passive" stakeholder engagement in India's cyber diplomacy, complemented by a governmental position that neither opposes nor proactively embraces the multistakeholder nature of cyber diplomacy.[179] Official Indian cyber delegations, for example, rarely include a multistakeholder component. India does, however, conduct ad hoc stakeholder engagement and supports a variety of conferences, including hosting the fifth Global Conference on Cyberspace in 2017.[180]

In the absence of a prominent contribution from civil society stakeholders, Indian cyber diplomacy is shaped principally by national interest and the institutional capacity.[181] Scholars have highlighted prominent themes in India's cyber diplomacy statements in multilateral forums, including concern for sovereignty, autonomy, multilateralism, capacity-building, cyber terrorism, and supply-chain security.[182] These situate India somewhere between the liberal and sovereigntist camps in global cyber diplomacy and some observers wonder how long India will be able to modulate its position between these two camps.

India's cyber diplomacy, therefore, exhibits the same flexibility and pragmatism as its wider foreign policy, supporting, in turn, the GGE, the OEWG, and the ad hoc committee to negotiate a global cyber crime treaty.[183] This tension should be familiar from the survey of India's wider foreign policy dilemmas regarding China and Russia. But there is a further, cyber-specific question that bears on the coherence of India's cyber statecraft: how to resolve any implicit tension between India's choices about cyber diplomacy and its priorities regarding cyber operations.

India actively participates in a wide variety of international forums and initiatives aimed at shaping global cyber governance norms. This includes engagement via organizations like the United Nations and the International Telecommunication Union, and partnerships such as the Shanghai Cooperation Organisation (SCO) and BRICS. However, bilateral tensions between India and other member states (China in BRICS, and both China and Pakistan in the SCO) render these organizations implausible as vehicles for substantive cybersecurity cooperation.

The U.S.-India cybersecurity partnership is one of the deepest and most enduring collaborations India has in the cyber domain. Initiated nearly twenty years ago, this partnership formally began with the establishment of the U.S.-India Cyber Security Forum, which was first convened in 2002.[184] There is now a long-established track record of collaboration between the two governments, but also more widely through academia, the private sector, and joint research and development initiatives in science and technology, including cybersecurity.[185]

Bilateral cyber cooperation between India and the United States is now complemented by the wider initiatives emerging under the auspices of the Quad.[186] Cybersecurity has emerged as a significant pillar of activity for the Quad both because it is a shared national security priority amongst Quad member states and because it is amenable to a wide range of relatively soft coordination, capacity-building, and educational initiatives.[187] These initiatives are desirable in themselves—building cybersecurity and resilience—but are also helpful in providing opportunities to elaborate and intensify the Quad as a strategic tool. However, the progress being made on cybersecurity issues within the Quad should not raise hope of a convergence between India and like-minded states on other issues where they are not obviously aligned with India's national interest, such as commercial spyware.

India's cyber diplomacy thus provokes a surprisingly wide range of different views, from plaudits for its active engagement and broadening of global representation in cyber diplomacy to criticism of its past administrative disorganization and "largely non-committal" relationship with the norms of cyber diplomacy.[188] One reason for this seeming inconsistency is probably the fact that cyber diplomacy is but one tool of a wider cyber statecraft. It is genuinely difficult to appraise the effectiveness of any single tool when the contours of the full agenda are (potentially by design) somewhat blurry. As Basu and Nachiappan have argued, it would be entirely in keeping with the Modi administration's wider preference toward diplomatic flexibility for India's cyber diplomacy to leave itself plenty of room to maneuver.[189] It is also consistent with Jaishankar's analysis of contemporary international relations, namely that norms are being eroded and states are responding by developing a wide array of capabilities and demonstrating an appetite to use them assertively to pursue national strategic objectives.[190]

Conclusion

India's cyber statecraft is a set of tools to facilitate India's wider national strategy and foreign policy agenda. Its different elements reflect Modi's prioritization of national security and commitment to India's strategic autonomy, including in diplomatic debates about re-balancing global governance. As cyberspace continues to evolve as a domain of international competition and cooperation, India's approach to cyber diplomacy under Modi will likely remain pragmatic. It will adapt to emerging challenges and opportunities, and will continue to prioritize the safeguarding of India's sovereign freedom of action.

Western cyber engagement that goes with, rather than against, the grain of this orientation is likely to be the most effective. Overtures from the United States and other like-minded states that focus on contributing to India's security and developmental priorities will be more constructively received by Modi than those that focus on those areas of India's domestic cyber policies—such as surveillance and spyware legislation—that touch on more sensitive issues of sovereignty and autonomy. But the United States and like-minded countries have a range of options, levers, and forums at their disposal to pursue influence on those areas where it is likely to be most effective.

There is some debate about precisely how to interpret India's embrace of the global cyber normative process and what the future might bring for India's cyber statecraft. It is particularly difficult, for example, to assess the existence or extent of the say-do gap between India's normative statements and its discreet development and employment of cyber capabilities. Reportedly Indian threat actors appear to be more focused on espionage than pre-positioning for offensive cyber operations. But this apparent prioritization of espionage begs the question of how to interpret the available evidence, both in terms of its accuracy and completeness in conveying present reality (is our visibility consequentially limited?[191]), and in its reliability as a predictor of future developments in India's cyber doctrine—that is, as India becomes more operationally potent, might its government be tempted to assert itself more in cyberspace?

Notwithstanding India's security competition with Pakistan, it is the bilateral relationship with China which will be the most significant outside factor in shaping India's wider cyber statecraft. Tensions with China reduce the extent to which India perceives BRICS and the SCO as forums for cybersecurity cooperation. This makes less difference in the field of norms and capacity-building, but even here cooperation will be carefully bounded to reduce risk.

Given the strength of its digital economy and innovation, and its potential for further growth in connectivity, digital inclusion, and workforce development, India has considerable latent cyber power. There are, however, significant obstacles to converting latent into actual power—and indeed in orchestrating its effective use. Future developments should focus principally on investment in and improved coordination of domestic cybersecurity, resilience, and cyber defense.[192]

India's next steps in cyber strategy are also likely to include continued pursuit of offensive capabilities and an appetite to use (and signal the potential use of) these capabilities more assertively against India's adversaries. This would need to be handled carefully, learning lessons from elsewhere about how to calibrate such operations and achieve effects in and through cyberspace. These are difficult, sensitive discussions for India's strategic partners to cultivate with its relevant national security institutions. Such efforts could usefully be complemented by sponsoring Track II dialogues on these issues, thus improving the nuance of think tank and other deliberations about the operational aspects of India's cyber statecraft.

Most importantly, India needs to clarify what effects it means to generate through the use of cyber capabilities and what contribution it intends to make to wider statecraft, and work backward from there to address outstanding issues of resources, organization, and execution. India would then benefit, in due course, from pursuing more transparency about its cyber doctrine, not least as a confidence-building measure to reduce the risk of misunderstanding and to improve regional cyber stability. There are interesting lessons to learn here from observing such efforts elsewhere, such as those of the UK's National Cyber Force. Despite alternative views of what could be achieved by more coherent or assiduous cyber norms diplomacy,[193] it will be India's success in developing the other aspects of its cyber statecraft that will shape the requirements of its cyber diplomacy, as will the reciprocal efforts of its adversaries across all elements of statecraft.

About the Authors

Joe Devanny is a senior lecturer in national security studies at the Department of War Studies at King's College London. He is a 2023–25 Project Fellow of the Research Institute for Sociotechnical Cyber Security (RISCS), working on "middle ground" cyber statecraft. He was a 2022–23 British Academy Innovation Fellow at the UK Foreign, Commonwealth, and Development Office, conducting research on cyber diplomacy.

Arthur P.B. Laudrain is a research associate in cyber diplomacy at the Department of War Studies and holds a doctorate in cybersecurity from the University of Oxford. Arthur is part of the Cyber Statecraft in an Age of Systemic Competition project, jointly funded by Engineering & Physical Sciences Research Council and the Defence Science and Technology Laboratory. He has been involved with the European Initiative for Security Studies since 2017, and is part of the British Academy Early Career Researcher Network.

Acknowledgments

The authors would like to thank the Defence Science and Technology Laboratory (Dstl) for funding this research through the Engineering and Physical Sciences Research Council (EPSRC) as part of the project on Cyber Statecraft in an Era of Systemic Competition. We are also very grateful to the Carnegie Endowment's Technology and International Affairs Program, including the editorial team and very helpful reviewers. The paper does not, however, reflect the views of the Dstl, the EPSRC, the Carnegie Endowment for International Peace, or King's College London. The authors benefited greatly from a range of conversations with other researchers and experts, including in a December 2024 roundtable discussion at King's College London. All errors and omissions are, however, the sole responsibility of the authors.

Notes

[1] For more on this series, see https://carnegieendowment.org/programs/technology-and-international-affairs/cyber-diplomacy-in-the-middle-ground?lang=en.

[2] P.S. Raghavan, "The Making of India›s Foreign Policy: From Non-Alignment to Multi-Alignment," *Indian Foreign Affairs Journal* 12, no. 4 (2017): 328.

[3] In the words of India's foreign minister: "For all the talk of globalisation and common good, nations still calculate unsentimentally what is to their particular advantage." S. Jaishankar, *Why Bharat Matters* (Rupa Publications, 2024), 46.

[4] Daniel Markey, "India as It Is: Washington and New Delhi Share Interests, Not Values," *Foreign Affairs*, June 16, 2023, https://www.foreignaffairs.com/india/markey-modi-biden-united-states.

[5] Madhu Bhalla, "The China Factor in India's Economic Diplomacy," *Observer Research Foundation* (blog), April 26, 2021, https://www.orfonline.org/expert-speak/china-factor-india-economic-diplomacy.

[6] Marcus Willett, *Cyber Operations and their Responsible Use* (Routledge for IISS, 2024), 36. Willett narrows the definition of cyber operations by omitting digital espionage. From our perspective, digital espionage is clearly a tool of cyber statecraft, as is domestic cybersecurity. Willett's definition also includes not only disruptive and destructive cyber operations, but also online information operations. For the purposes of assessing a state's cyber statecraft, it is necessary to consider in scope each of these operational activities: espionage, cybersecurity and resilience, disruptive and destructive ("offensive cyber") operations, and online information operations. Nor is statecraft the sole preserve of state entities; various proxy relationships can magnify or dilute the totality of a state's intended statecraft activities. See, for example, Tim Maurer, *Cyber Mercenaries: The State, Hackers and Power* (Cambridge University Press, 2018).

[7] S. Jaishankar, *The India Way: Strategies for an Uncertain World* (Harper Collins India, 2020).

[8] Harsh V. Pant and Julie Super, "Non-Alignment and Beyond," in Harsh Pant (ed.), *New Directions in India's Foreign Policy: Theory and Praxis* (Cambridge University Press, 2019), 127–148; and P.S. Raghavan, "The Making of India's Foreign Policy: From Non-Alignment to Multi-Alignment," *Indian Foreign Affairs Journal* 12, no. 4 (2017): 326–341.

[9] Kate Fazzini, "In India-Pakistan Conflict, There's a Long-Simmering Online War, and Some Very Good Hackers on Both Sides," CNBC, February 27, 2019, https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html.

[10] Tanvi Madan, “China Has Lost India: How Beijing’s Aggression Pushed New Delhi to the West,” *Foreign Affairs,* October 4, 2022, https://www.foreignaffairs.com/china/china-has-lost-india.

[11] Sreeram Chaulia, “BJP, India’s Foreign Policy and the ‘Realist Alternative’ to the Nehruvian Tradition,” *International Politics* 39, no. 2 (June 2002): 215–234; Sumit Ganguly, “India After Nonalignment: Why Modi Skipped the Summit,” *Foreign Affairs,* September 19, 2016, https://www.foreignaffairs.com/india/india-after-nonalignment; Ashley J. Tellis, “America’s Bad Bet on India: New Delhi Won’t Side With Washington Against Beijing,” *Foreign Affairs,* May 1, 2023, https://www.foreignaffairs.com/india/americas-bad-bet-india-modi; and Susan L. Shirk, *Overreach: How China Derailed Its Peaceful Rise* (Oxford University Press 2023).

[12] Chris Kay and John Reed, “Can India’s Economy Thrive Without China’s Help?,” *Financial Times,* August 7, 2024, https://www.ft.com/content/5a2b4491-5687-4b11-872d-a4f51121bbb2.

[13] Jonathan Greig, “Suspected China-Backed Hackers Target 7 Indian Electricity Grid Centers,” The Record, April 8, 2022, https://therecord.media/suspected-china-backed-hackers-target-7-indian-electricity-grid-centers.

[14] Hannes Ebert, “Hacked IT Superpower: How India Secures its Cyberspace as a Rising Digital Democracy.” *India Review* 19, no. 4 (October 2020): 376–413; and Tim Stevens, “India’s Cybersecurity Challenges,” *Sovereign Data* 2, no. 4 (2016): 1–4.

[15] Arindrajit Basu and Karthik Nachiappan, “Will India Negotiate in Cyberspace?,” in Fabio Cristiano and Bibi van den Berg (eds). *Hybridity, Conflict and the Global Politics of Cybersecurity* (Rowman and Littlefield, 2023) 189–210; and Arvind Gupta, “Securing Cyberspace: Asian and International Perspectives,” 18th Asian Security Conference, February 10, 2016, archived July 19, 2024, https://web.archive.org/web/20240719094254/https://idsa.in/keyspeeches/18asc-securing-cyberspace-asian-and-international-perspectives_deputy-nsa.

[16] Arindrajit Basu, “India’s International Cyber Operations: Tracing National Doctrine and Capabilities,” UN Institute for Disarmament Research, 2022, https://unidir.org/wp-content/uploads/2023/05/UNIDIR_India_International_Cyber_Operations.pdf; Caleb de Boer, “To Protect and Project: India’s Underdeveloped Cyberspace Operations Programme,” *Canadian Forces College,* 2020, https://www.cfc.forces.gc.ca/259/290/22/305/DeBoer.pdf; and Thangjam K. Singh and Sanjay K. Jha, “From Code to Command: Unveiling India’s Cyberpower Strategy,” *Comparative Strategy* 43, no. 3 (2024): 223–236, https://doi.org/10.1080/01495933.2024.2340951.

[17] For a good summary of the emergence of the contemporary cyber policy landscape and government interaction with both the private sector and civil society, see Shuchita Thapar, *Mapping the Cyber Policy Landscape: India,* Global Partners Digital, February 2016, https://www.gp-digital.org/wp-content/uploads/2017/05/India_mapping-report_final_2-1.pdf.

[18] Ebert, “Hacked IT Superpower,” 376–413; and Karthik Nachiappan and Nishant Rajeev, “India as a Muddling Cyber-Power,” National University of Singapore Institute of South Asian Studies, July 22, 2021, https://www.isas.nus.edu.sg/papers/india-as-a-muddling-cyber-power/.

[19] This was most obviously true of the foundational impact on India’s foreign policy exerted by its first prime minister, Jawaharlal Nehru. Much of India’s subsequent foreign policy debates are consciously framed around participants’ views of the pros and cons of the Nehruvian approach. But even more recently, a considerable literature has developed around understanding Modi’s foreign policy. See, for example: Niranjan Sahoo, “Decoding Modi’s Foreign Policy,” Carnegie Endowment for International Peace, September 23, 2014, https://carnegieendowment.org/research/2014/09/decoding-modis-foreign-policy?lang=en; Sreeram Chaulia, Modi Doctrine: The Foreign Policy of India’s Prime Minister (New Delhi: Bloomsbury, 2016); Manjari Chatterjee Miller and Kate Sullivan de Estrada, “Pragmatism in Indian Foreign Policy: How Ideas Constrain Modi,” *International Affairs* 93, no. 1 (2017): 27–49; and Jaishankar, *Why Bharat Matters.*

[20] Harsh V. Pant and Avinash Paliwal, “Foreign Policy Analysis and Indian Foreign Policy,” in Harsh Pant (ed.), *New Directions in India’s Foreign Policy: Theory and Praxis* (Cambridge University Press, 2019), 120.

21 Anil Anand, "Indian Non-Alignment 2.0: Defensible Duplicity," Australian Institute of International Affairs, October 5, 2023, https://www.internationalaffairs.org.au/australianoutlook/indian-non-alignment-2-0-defensible-duplicity/; Sushant Singh, "Why Modi Can't Make India a Great Power: Government-Backed Intolerance Is Tearing the Country Apart," *Foreign Affairs,* September 4, 2023, https://www.foreignaffairs.com/india/why-modi-cant-make-india-great-power; and Rohan Mukherjee, "A Hindu Nationalist Foreign Policy: Under Modi, India Is Becoming More Assertive," *Foreign Affairs,* April 4, 2024, https://www.foreignaffairs.com/india/hindu-nationalist-foreign-policy. For digital surveillance in India, see: Amnesty International, "India: Amnesty International Letter to the Technical Committee Appointed by the Supreme Court of India," February 15, 2022, https://www.amnesty.org/en/documents/asa20/5930/2022/en/; and "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists," Amnesty International, December 28, 2023, https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/. For reporting regarding a reportedly burgeoning cyber surveillance export market, see: David D. Kirkpatrick, "A Confession Exposes India's Secret Hacking Industry," *New Yorker,* June 1, 2023, https://www.newyorker.com/news/annals-of-crime/a-confession-exposes-indias-secret-hacking-industry. And for reports of alleged assassinations/extrajudicial killings, see: "Indian Nationals Charged in Murder of Canadian Sikh Activist," *Japan Times,* May 4, 2024, https://www.japantimes.co.jp/news/2024/05/04/asia-pacific/politics/india-canada-arrests-killing/; and Hannah Ellis-Petersen, "India Appears to Confirm Extrajudicial Killings in Pakistan," *Guardian,* April 5, 2024, https://www.theguardian.com/world/2024/apr/05/india-appears-to-confirm-extrajudicial-killings-in-pakistan.

22 Abhijnan Rej and Rahul Sagar, "The BJP and Indian Grand Strategy," in Milan Vaishnav (ed.), *The BJP in Power: Indian Democracy and Religious Nationalism* (Carnegie Endowment for International Peace, 2019), 79, https://carnegieendowment.org/research/2019/04/the-bjp-in-power-indian-democracy-and-religious-nationalism?lang=en.

23 George Perkovich, *India's Nuclear Bomb: The Impact on Global Proliferation* (University of California Press, 1999).

24 Kartik Bommakanti, ed., "A Decade of Defence Reforms under Modi," Observer Research Foundation Special Report No. 230, July 15, 2024, https://www.orfonline.org/research/a-decade-of-defence-reforms-under-modi; and Joaquin Matamis, "India's Military Modernization Efforts Under Prime Minister Modi," Stimson Center, May 22, 2024, https://www.stimson.org/2024/indias-military-modernization-efforts-under-prime-minister-modi/.

25 Suchet Vir Singh, "Indian Militaries Theatre Command Plans: Where Does the Proposed Overhaul Stand?," Observer Research Foundation, July 20, 2023, https://www.orfonline.org/expert-speak/indian-militaries-theatre-command-plans-where-does-the-proposed-overhaul-stand.

26 International Institute for Strategic Studies, *The Military Balance 2024* (International Institute for Strategic Studies, 2024), 224, 265, https://www.iiss.org/publications/the-military-balance/2024/the-military-balance-2024/.

27 Rajoli Siddharth Jayaprakash, "The State of India-Russia Relations in Light of PM Modi's Visit to Moscow," Observer Research Foundation, July 15, 2024, https://www.orfonline.org/expert-speak/the-state-of-india-russia-relations-in-light-of-pm-modi-s-visit-to-moscow; Madan, "China Has Lost India"; and Tellis, "America's Bad Bet on India."

28 Manoj Kumar, "India, France Agree on Joint Defence Production," Reuters, January 27, 2024, https://www.reuters.com/world/india-france-agree-joint-defence-production-statement-2024-01-27/.

29 For a good recent overview of India's position in global cyber diplomacy, see: "Sameer Patil, India's Cyber Diplomacy Shapes Its Rule-Maker Aspirations," in Andrea Salvi, Heli Tiirmaa-Klaar, James Andrew Lewis (eds.), *A Handbook for the Practice of Cyber Diplomacy (EU Cyber Direct, 2025), 112–115,* https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/APafQ4IV/a-handbook-for-the-practice-of-cyber-diplomacy.pdf.

30 Laiqh A. Khan, "Failure to Counter BJP's Politicisation of Pulwama Attack a Reason for Congress Setback in Karnataka," *The Hindu*, August 15, 2019, https://www.thehindu.com/news/national/karnataka/failure-to-counter-bjps-politicisation-of-pulwama-attack-a-reason-for-cong-setback/article29103390.ece; and Pallab Bhattacharya, "Pulwama, Balakot Dominate India's Pre-Poll Political Discourse," *Daily Star*, March 5, 2019, https://www.thedailystar.net/opinion/global-affairs/news/pulwama-balakot-dominate-indias-pre-poll-political-discourse-1710580.

[31] Anshul Trivedi, “Narendra Modi’s Post-Pulwama Doctrine: Securitise Politics, Politicise Security,” The Wire, February 14, 2020, https://thewire.in/politics/modi-doctrine-pulwama-security.

[32] Rej and Sagar, “The BJP and Indian Grand Strategy,” 82; Ashley J. Tellis, “Troubles Aplenty: Foreign Policy Challenges for the Next Indian Government,” Carnegie Endowment for International Peace, May 20, 2019, https://carnegieendowment.org/research/2019/05/troubles-aplenty-foreign-policy-challenges-for-the-next-indian-government?lang=en.

[33] Manjari Chatterjee Miller and Kate Sullivan de Estrada, “Pragmatism in Indian Foreign Policy: How Ideas Constrain Modi,” *International Affairs* 93, no. 1 (2017), 27–49; Pant and Super, “Non-Alignment and Beyond,” 127–148.

[34] “Unabashed and Unabated: India Leads the World Shutdown Count for Sixth Year,” Access Now, May 15, 2024, https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en/; Kris Ruijgrok, “The Authoritarian Practice of Issuing Internet Shutdowns in India: The Bharatiya Janata Party’s Direct and Indirect Responsibility,” *Democratization* 29, no. 4 (May 19, 2022), 611–633, https://doi.org/10.1080/13510347.2021.1993826.

[35] “Longest Internet Shutdown in 2023 Took Place in Manipur Amidst Human Rights Violations: Report,” *The Hindu,* January 11, 2024, https://www.thehindu.com/sci-tech/technology/longest-internet-shutdown-2023-took-place-manipur-amidst-human-rights-violations-report/article67726259.ece.

[36] “National Cyber Threat Assessment 2025-26,” Canadian Centre for Cyber Security, October 30, 2024, 35, https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026.

[37] Kushagra Singh, Gurshabad Grover, and Varun Bansal, “How India Censors the Web,” in *Proceedings of the 12th ACM Conference on Web Science*, WebSci ’20 (Association for Computing Machinery, 2020), 21–28, https://doi.org/10.1145/3394231.3397891.

[38] Lata Rajagopalan Kumar, “Muscle or Muzzle? A Critical Analysis of Media, Power and Censorship in Democratic India,” *International Journal of Media & Cultural Politics* 13, no. 1–2 (March 2017), 75-89, https://doi.org/10.1386/macp.13.1-2.75_1.

[39] Gatra Priyandita and Arindrajit Basu, “Why Haven’t India and Indonesia Signed Up for Anti-Spyware Dialogue?,” Royal United Services Institution, April 10, 2024, https://www.rusi.org/explore-our-research/publications/commentary/why-havent-india-and-indonesia-signed-anti-spyware-dialogue.

[40] Kirkpatrick, “A Confession Exposes India’s Secret Hacking Industry.”.

[41] Amnesty International, “India: Amnesty International Letter to the Technical Committee”; Amnesty International, “India: Damning New Forensic Investigation.”

[42] Rohan Venkataramakrishnan, “Across Official Denials and BJP Responses, One Phrase Missing: ‘India Did Not Use Pegasus Spyware,’” Scroll.in, July 21, 2021, https://scroll.in/article/1000605/across-official-denials-and-bjp-responses-one-phrase-missing-india-did-not-use-pegasus-spyware.

[43] “Pegasus: Centre Pleads National Security; SC Says Won’t Force It,” *Indian Express*, August 17, 2021, https://indianexpress.com/article/india/pegasus-row-supreme-court-centre-7457708/.

[44] Dhananjay Mahapatra, “Supreme Court-Picked Panel Finds No Proof of Pegasus on 29 phones It Got,” *Times of India,* August 26, 2022, https://timesofindia.indiatimes.com/india/supreme-court-picked-panel-finds-no-proof-of-pegasus-on-29-phones-it-got/articleshow/93786248.cms.

[45] Andrea Peterson, “Report Links Indian Company to Spyware That Targeted Togolese Activist,” The Record, October 7, 2021, https://therecord.media/report-links-indian-company-to-spyware-that-targeted-togolese-activist.

[46] “ESET Research Investigates Donot Team: Cyberespionage Targeting Military & Governments in South Asia,” ESET, January 18, 2022, https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-investigates-donot-team-cyberespionage-targeting-military-governments-in-south-asia/.

47 BlackBerry, "Mobile Malware and APT Espionage: Prolific, Pervasive, and Cross-Platform," *BlackBerry Blog,* October 23, 2019, https://blogs.blackberry.com/en/2019/10/mobile-malware-and-apt-espionage-prolific-pervasive-and-cross-platform; "Togo: Prominent Activist Targeted with Indian-Made Spyware Linked to Notorious Hacker Group," Amnesty International, October 7, 2021, https://www.amnesty.org/en/latest/news/2021/10/togo-activist-targeted-with-spyware-by-notorious-hacker-group/; and BlackBerry, "SideWinder Utilizes New Infrastructure to Target Ports and Maritime Facilities in the Mediterranean Sea," *BlackBerry Blog,* July 25, 2024, https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-mediterranean-sea.

48 Gatra Priyandita and Arindrajit Basu, "Why Haven't India and Indonesia Signed Up For Anti-Spyware Dialogue?," *RUSI* (blog), April 10, 2024, https://www.rusi.org/explore-our-research/publications/commentary/why-havent-india-and-indonesia-signed-anti-spyware-dialogue.

49 This is visible, for example, in India's perception of the nuclear nonproliferation regime. See George Perkovich, *India's Nuclear Bomb: The Impact on Global Proliferation* (University of California Press, 1999), 7.

50 Both IBSA and BRICS are flexible forums that could theoretically provide the nucleus for such an initiative, if the necessary political will existed—although it is difficult to imagine, for example, China and India pursuing and agreeing to such an initiative to constrain their respective espionage activities. For the organizational development of BRICS in particular, see: Oliver Stuenkel, *The BRICS and the Future of Global Order,* 2nd ed. (Rowman & Littlefield, 2020).

51 The authors are grateful to the practitioners and academics we have spoken to about the institutional dynamics of India's cyber statecraft for helping us clarify the competing interests that shape it, particularly the primacy of the security and intelligence apparatus on operational matters, on which it is believed the MEA (the institutional lead for cyber diplomacy) has relatively little influence.

52 Colin S. Gray, *Making Sense of Cyber Power: Why the Sky Is Not Falling,* Strategic Studies Institute, U.S. Army War College, 2013.

53 Shashank Joshi, "India's National Security Advisor: What Advice Will Modi Receive?," *RUSI* (blog), June 29, 2014, https://rusi.org/explore-our-research/publications/commentary/indias-national-security-advisor-what-advice-will-modi-receive.

54 "How NSA Ajit Doval Prepared the Ground for PM Modi's Landmark US Visit," *Economic Times*, June 16, 2023, https://economictimes.indiatimes.com/news/india/how-nsa-ajit-doval-prepared-the-ground-for-modis-landmark-us-visit/articleshow/101019072.cms?from=mdr.

55 Matamis, "India's Military Modernization Efforts Under Prime Minister Modi."

56 Frank O'Donnell and Harsh V. Pant, "The Evolution in India's National Security Apparatus: Persisting Structural Deficiencies," in *Handbook of Indian Defence Policy* (Routledge, 2016), 283–293.

57 Sanja Kelly, Sarah Cook, and Mai Truong (eds.), *Freedom on the Net: A Global Assessment of Internet and Digital Media,* Freedom House, September 24, 2012, 236, https://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report_0.pdf; and Pankaj Phanase, "Kargil After 25 Years: Assessing Technological Impact on India's Armed Forces," Vivekananda International Foundation, August 22, 2024, https://www.vifindia.org/2024/august/22/Kargil-After-25-Years-Assessing-Technological-Impact-on-India-s-Armed-Forces.

58 International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment* (International Institute for Strategic Studies, 2021), 135.

59 "India's National Cyber Security Policy (NCSP)," Indian Ministry of Electronics and Information Technology, 2013, https://www.meity.gov.in/content/national-cyber-security-policy-2013-0.

60 Namrata Biji Ahuja, "Doval's Supporting Hands Are Seasoned Spymasters—Rajinder Khanna, Pankaj Singh and Ravichandran," The Week, July 4, 2024, https://www.theweek.in/news/india/2024/07/04/dovals-supporting-hands-are-seasoned-spymasters-rajinder-khanna-pankaj-singh-and-ravichandran.html.

61 "Cyberspace Integral Part of Country's Security: NCSC Lt Gen M U Nair," *Business Standard,* April 5, 2024, https://www.business-standard.com/india-news/cyberspace-integral-part-of-country-s-security-ncsc-lt-gen-m-u-nair-124040500008_1.html.

62 "Five Botnet and Malware Cleaning Tools Offered by Government," *Times of India,* February 24, 2024, https://timesofindia.indiatimes.com/gadgets-news/five-government-provided-botnet-and-malware-cleaning-tools/articleshow/107951686.cms.

63 “Functions of Ministry of Electronics and Information Technology | Ministry of Electronics and Information Technology, Government of India,” Indian Ministry of Electronics and Information Technology, accessed May 29, 2024, https://www.meity.gov.in/about-meity/functions-of-meity.

64 CXOtoday News Desk, “Indian Government Doubles Cybersecurity Funding from Rs 400 Cr to Rs 750 Cr in 2024 Interim Budget: Industry Leaders Strongly Advocate,” CXOToday.com, February 7, 2024, https://cxotoday.com/specials/indian-government-doubles-cybersecurity-funding-from-rs-400-cr-to-rs-750-cr-in-2024-interim-budget-industry-leaders-strongly-advocate/.

65 “New Players Join Race for Offensive Cyber Abilities,” Oxford Analytica Daily Brief, August 20, 2018, https://css.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.

66 National Cyber Force, “The National Cyber Force: Responsible Cyber Power in Practice,” UK Government, 2023, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice. For a reflection on the value of such transparency initiatives and strategic narratives, see Joe Devanny and Andrew Dwyer, “From Cyber Security to Cyber Power: Appraising the Emergence of ‘Responsible, Democratic Cyber Power’ in UK Strategy,” in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (NATO Collaborative Cyber Defence Centre of Excellence, 2023), 381–397.

67 The mechanics of this intra-governmental coordination in India are opaque, but for an analysis of how this process has developed over the last decade in the UK, see Devanny and Dwyer, “From Cyber Security to Cyber Power: Appraising the Emergence of ‘Responsible, Democratic Cyber Power’ in UK Strategy.” While the UK’s foreign ministry—the Foreign, Commonwealth and Development Office (FCDO)—plays a more active role in national cyber strategy than it did a decade ago, it is still understandably constrained by the operational equities of agencies such as the cyber, intelligence, and security agency Government Communications Headquarters and the other institutional components of the UK’s National Cyber Force. Extrapolating to India, there are two relevant differences: the External Affairs Ministry has a smaller capacity to engage in cyber diplomacy than does the FCDO and the cyber operational equities are both less mature and more narrowly targeted than is the case in the UK. See (forthcoming): Joe Devanny, “The United Kingdom,” in George Christou, Wilhem Vosse, Joe Burton and Joachim Koops (eds.), *The Palgrave Handbook on Cyber Diplomacy* (Palgrave Macmillan, 2025).

68 See, for example, Arvind Gupta, “Securing Cyberspace: A National Security Perspective,” in Cherian Samuel and Munish Sharma (eds.), *Securing Cyberspace: Asian and International Perspectives* (18th Asian Security Conference, February 10, 2016), https://idsa.in/system/files/book/book_securing-cyberspace_0.pdf; and Asoke Mukerji, “The Need for an International Convention on Cyberspace,” *Horizons* 16 (Spring 2020), https://www.cirsd.org/en/horizons/horizons-spring-2020-issue-no-16/the-need-for-an-international-convention-on-cyberspace.

69 Carmen Ang, “These Are the Countries Where Internet Access Is Lowest,” World Economic Forum, August 17, 2020, https://www.weforum.org/agenda/2020/08/internet-users-usage-countries-change-demographics/.

70 Chandra Gnanasambandam et al., “Online and Upcoming: The Internet’s Impact on India,” McKinsey & Company, December 2012, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/India/Online%20and%20upcoming%20The%20Internets%20impact%20on%20India/Online_and_Upcoming_The_internets_impact_on_India.pdf.

71 Sameer Patil and Aneesh Parnerkar, “The Untapped Potential of India-Estonia Cyber Cooperation,” Observer Research Foundation, July 31, 2024, https://www.orfonline.org/expert-speak/the-untapped-potential-of-india-estonia-cyber-cooperation.

72 “IT-BPM Industry in India - Market Size, Opportunities, FDI,” Invest India, accessed March 19, 2025, https://www.investindia.gov.in/sector/it-bpm.

73 For recent foreign threats to India’s digital infrastructure, see: Jonathan Greig, “Suspected China-Backed Hackers Target 7 Indian Electricity Grid Centers,” The Record, April 8, 2022, https://therecord.media/suspected-china-backed-hackers-target-7-indian-electricity-grid-centers; and Jonathan Greig, “Suspected Chinese Gov’t Hackers Used Ransomware as Cover in Attacks on Brazil Presidency, Indian Health Org,” The Record, June 27, 2024, https://therecord.media/chamelgang-china-apt-ransomware-distraction.

74 Monica Kamiska, "Risk Aversion Is at the Heart of the Cyber Response Dilemma," Council on Foreign Relations, March 31, 2021, https://www.cfr.org/blog/risk-aversion-heart-cyber-response-dilemma; and Frank Rose, "NNSA Principal Deputy Administrator Frank Rose›s remarks for the Department of Energy Cyber Security Conference," U.S. Department of Energy, May 10, 2023, https://www.energy.gov/nnsa/articles/nnsa-principal-deputy-administrator-frank-roses-remarks-department-energy-cyber.

75 "India Businesses Face over 3,000 Cyberattacks per Week, Second Only to Taiwan Firms," *The Hindu,* July 18, 2024, https://www.thehindu.com/sci-tech/technology/internet/india-businesses-face-over-3000-cyberattacks-per-week-second-only-to-taiwan-firms/article68417640.ece.

76 Neeraj Chauhan, "Almost 300% Rise in Cyber Attacks in India in 2020, Govt Tells Parliament," *Hindustan Times*, March 23, 2021, https://www.hindustantimes.com/india-news/almost-300-rise-in-cyber-attacks-in-india-in-2020-govt-tells-parliament-101616496416988.html.

77 "Indian Cyberspace Seeing Incidents at Higher Rate than Global Average: National Cybersecurity Coordinator," *Economic Times*, November 19, 2023, https://economictimes.indiatimes.com/tech/technology/indian-cyberspace-seeing-incidents-at-higher-rate-than-global-average-national-cybersecurity-coordinator/articleshow/105330185.cms.

78 Sameer Patil, "Cyber Attacks: Pakistan Emerges as China's Proxy Against India," *Observer Research Foundation,* February 15, 2022, https://www.orfonline.org/research/pakistan-emerges-as-chinas-proxy-against-india.

79 Zhang Tong, "India Has Become a Major Source of Cybersecurity Threats in China: Security Expert," *South China Morning Post,* February 16, 2024, https://www.scmp.com/news/china/science/article/3251536/india-has-become-major-source-cybersecurity-threats-china-security-expert. It is worth noting the degree of circumspection in attribution statements regarding an "India nexus" in threat activity that appears in both Western cyber threat intelligence reporting and reporting from Chinese information and communications companies. Consider, for example, the recent Knownsec report on apparent espionage targeting of Pakistan by Mysterious Elephant, an actor Knownsec cautiously describes as originating in "South Asia." See Daryna Antoniuk, "South Asian Hackers Target Pakistani Entities in New Espionage Campaign," The Record, November 25, 2024, https://therecord.media/south-asian-hackers-target-pakistan-entities-in-espionage-campaign.

80 Paul Mozur, Keith Bradsher, John Liu, and Aaron Krolik, "Leaked Files Show the Secret World of China's Hackers for Hire," *New York Times,* February 22, 2024, https://www.nytimes.com/2024/02/22/business/china-leaked-files.html.

81 P. J. George, "Explained | Red Echo, ShadowPad, and the Targeting of India's Power Grid," *The Hindu*, March 6, 2021, https://www.thehindu.com/sci-tech/technology/red-echo-over-india/article34008299.ece.

82 Sahil Joshi and Divyesh Singh, "Mega Mumbai Power Outage May Be Result of Cyber Attack, Final Report Awaited," *India Today,* November 20, 2020, https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20.

83 Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, February 28, 2021, https://www.recordedfuture.com/blog/redecho-targeting-indian-power-sector.

84 David Sanger and Emily Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *New York Times,* February 28, 2021, https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

85 "'It Was Human Error': Cyberattacks Took Place but Didn't Cause Mumbai Power Outage, Says Govt," *Times of India*, March 2, 2021, https://timesofindia.indiatimes.com/india/2020-mumbai-power-outage-caused-by-human-error-not-cyber-attack-union-power-minister/articleshow/81292545.cms.

86 Joe Devanny, Ciaran Martin, and Tim Stevens, "On the Strategic Consequences of Digital Espionage," *Journal of Cyber Policy* 6, no. 3 (2021), 429–450.

87 Jessica Lyons, "China's Volt Typhoon Crew and Its Botnet Surge Back with a Vengeance," The Register, November 13, 2024, https://www.theregister.com/2024/11/13/china_volt_typhoon_back/; "What You Need to Know About the Salt Typhoon Hack," Axios, October 15, 2024, https://www.axios.com/2024/10/15/salt-typhoon-hack-china-verizon-att; and Joe Warminsky, "FBI Says It Recently Dismantled a Second Major China-Linked Botnet," The Record, September 18, 2024, https://therecord.media/fbi-dismantles-flax-typhoon-china-linked-botnet-wray-aspen.

88 See the analysis of the Obama-Xi agreement in Devanny, Martin and Stevens, "On the Strategic Consequences of Digital Espionage," 437–438.

89 Dwaipayan Ghosh, "Jamtara & Beyond: Cyber Fraud Hubs Sprout in North India Towns," *Times of India*, March 13, 2024, https://timesofindia.indiatimes.com/city/kolkata/jamtara-beyond-cyber-fraud-hubs-sprout-in-north-india-towns/articleshow/108448284.cms.

90 "India Rescuing Citizens Forced into Cyber Fraud Schemes in Cambodia," Reuters, April 1, 2024, https://www.reuters.com/world/india/india-rescuing-citizens-forced-into-cyber-fraud-schemes-cambodia-2024-03-31/.

91 Miranda Bruce et al., "Mapping the Global Geography of Cybercrime with the World Cybercrime Index," *PLOS ONE* 19, no. 4 (April 10, 2024): e0297312, https://doi.org/10.1371/journal.pone.0297312.

92 "Indian Cyberspace Seeing Incidents at Higher Rate than Global Average: National Cybersecurity Coordinator," *The Hindu,* November 19, 2023, https://www.thehindu.com/sci-tech/technology/indian-cyberspace-seeing-incidents-at-higher-rate-than-global-average-national-cybersecurity-coordinator/article67550840.ece.

93 "Cybercriminals Are Targeting Elections in India with Influence Campaigns," *Resecurity* (blog), accessed May 29, 2024, https://www.resecurity.com/blog/article/cybercriminals-are-targeting-elections-in-india-with-influence-campaigns.

94 Oleg Kolesnikov, "Securonix Threat Research: Cosmos Bank SWIFT/ATM US$13.5 Million Cyber Attack Detection Using Security Analytics," Securonix, accessed May 29, 2024, https://www.securonix.com/blog/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/.

95 "PII Belonging to Indian Citizens, Including Their Aadhaar IDs, Offered for Sale on the Dark Web," *Resecurity* (blog), accessed May 29, 2024, https://www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web.

96 Mardav Jain, "The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment," Henry M. Jackson School of International Studies, May 9, 2019, https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/.

97 "Data of 10 Crore Mobikwik Users for Sale on Dark Web, Say Cybersecurity Experts," *Economic Times*, March 30, 2021, https://economictimes.indiatimes.com/tech/startups/mobikwik-data-breach-personal-data-of-over-10-crore-users-allegedly-available-on-sale/articleshow/81756544.cms?from=mdr.

98 "Ransomware Trends 2024: Insights for Global Cybersecurity Readiness," Cyber Peace Institute, December 31, 2024, https://www.cyberpeace.org/resources/blogs/ransomware-trends-2024-insights-for-global-cybersecurity-readiness.

99 "Al-Qa'ida in the Indian Subcontinent (AQIS) - Statement of Reasons," Australian National Security, accessed May 29, 2024, https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/al-qaida-in-the-indian-subcontinent-aqis.

100 The Hindu Bureau, "NIA Court Convicts IS Propagandist Mehdi Masroor Biswas; Sentencing Likely Today," *The Hindu*, January 19, 2024, https://www.thehindu.com/news/cities/bangalore/nia-court-convicts-is-propagandist-mehdi-masroor-biswas-sentencing-likely-today/article67756737.ece. Countering terrorists' instrumental use of communications technologies such as social media platforms to propagandize, radicalize, and recruit is a global priority, not just for India's government. The different experiences of governments engaging with or regulating social media companies to address the problems of violence and extremism is a salient issue of global public policy debate.

101 "Anonymous Attacks Indian Government Websites," BBC News, May 18, 2012, https://www.bbc.com/news/technology-18114984.

102 Dia Rekhi, "Alarm Bells Go off as Indonesian Hacktivists Breach Government Websites," *Economic Times*, January 30, 2024, https://economictimes.indiatimes.com/tech/technology/indonesian-hackers-behind-breach-of-indian-websites-this-month-experts/articleshow/107239316.cms?from=mdr.

103 "National Cyber Threat Assessment 2025-26," Canadian Centre for Cyber Security, October 30, 2024, 35, https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026.

[104] Neeraj Soni, "National Cyber Security Reference Framework – Need of the Hour," Cyber Peace Foundation, June 20, 2023, https://www.cyberpeace.org/resources/blogs/national-cyber-security-reference-framework-need-of-the-hour.

[105] "Indian Blueprint for Cyber Security Finalised: Pant," *Indian Express,* June 14, 2023, https://indianexpress.com/article/cities/pune/indian-blueprint-for-cyber-security-finalised-pant-8659660/.

[106] De Boer, "To Protect and Project"; "Cyber Power – Tier Three," International Institute for Strategic Studies, June 28, 2021, https://www.iiss.org/en/research-paper/2021/06/cyber-power---tier-three/.

[107] Karthik Nachiappan and Nishant Rajeev, "India as a Muddling Cyber-Power," National University of Singapore Institute of South Asian Studies, July 22, 2021, https://www.isas.nus.edu.sg/papers/india-as-a-muddling-cyber-power/.

[108] Basu, "India's International Cyber Operations."

[109] There is much uncertainty about the present state of India's sovereign cyber capabilities, the coherence of its inter-institutional coordination of cyber operations, and its operational activity in cyberspace. Similarly, the private sector cyber threat intelligence community reports instances of threat activity that appear to align with India's strategic interests, but which may have been perpetrated by actors from outside of the Indian government. These overlapping uncertainties are the biggest lacuna in contemporary understanding of India's cyber statecraft. See, for example: Antoniuk, "India-Linked Hackers Target Pakistan with Spyware"; Basu, "India's International Cyber Operations"; BlackBerry, "SideWinder Utilizes New Infrastructure"; de Boer, "To Protect and Project"; Kate Fazzini, "In India-Pakistan Conflict, There's a Long-Simmering Online War"; Karthik Bommakanti et al., "Cyber Operations in India's Military Strategy," in *Emerging Technologies and India's Defence Preparedness,* Observer Research Foundation Special Report No. 209, April 2023, 24–27, https://www.orfonline.org/public/uploads/posts/pdf/20240510151332.pdf; and M.K. Narayan, "The Best Among Limited Options," *The Hindu,* September 21, 2016, https://www.thehindu.com/opinion/lead/M.-K.-Narayanan-on-India-Pakistan-diplomacy-and-terrorism/article55940567.ece.

[110] Saikat Datta, "Cyber Protection Body Pushes Ahead - Hindustan Times," January 20, 2014, archived January 19, 2014, https://web.archive.org/web/20140119201552/http://www.hindustantimes.com/india-news/cyber-protection-body-pushes-ahead/article1-1174753.aspx.

[111] Annapurna Roy, "Skill Gap in Workforce, AI Advancements Make Cyber Attacks More Threatening in India," *Economic Times*, April 14, 2024, https://economictimes.indiatimes.com/tech/technology/skill-gap-in-workforce-ai-advancements-make-cyber-attacks-more-threatening-in-india/articleshow/109267290.cms?from=mdr#.

[112] B. Poornima, "Cyber Preparedness of the Indian Armed Forces," *Journal of Asian Security and International Affairs* 10, no. 3 (December 1, 2023): 301–324, https://doi.org/10.1177/23477970231207250; "NCSI : Ranking," National Cyber Security Index, accessed April 19, 2024, https://ncsi.ega.ee/ncsi-index/.

[113] Bommakanti et al., "Cyber Operations in India's Military Strategy."

[114] Rahul Singh, "Army to Set Up Specialised Units to Strengthen Cybersecurity," *Hindustan Times*, April 27, 2023, https://www.hindustantimes.com/india-news/indian-army-to-create-specialised-units-for-cybersecurity-and-net-centricity-as-adversaries-expand-cyber-warfare-capabilities-101682602122696.html.

[115] International Institute for Strategic Studies, "Cyber Power – Tier Three."

[116] Narayanan, "The Best Among Limited Options."

[117] Basu, "India's International Cyber Operations"3.

[118] Meetu Jain, "Amit Shah and Ajit Doval in Tussle Over Control of NTRO," The Wire, November 2, 2024, https://thewire.in/government/amit-shah-and-ajit-doval-in-tussle-over-control-of-ntro.

[119] Rajat Pandit, "Armed Forces Formulate New Doctrine for Cyberspace Operations," *Times of India, June 18, 2024,* https://timesofindia.indiatimes.com/india/armed-forces-formulate-new-doctrine-for-cyberspace-operations/articleshow/111094158.cms.

[120] Poornima, "Cyber Preparedness of the Indian Armed Forces."

[121] Karthik Nachiappan, "Going On The Offensive: India's Cyber Capabilities – Analysis," Eurasia Review, December 30, 2022, https://www.eurasiareview.com/31122022-going-on-the-offensive-indias-cyber-capabilities-analysis/.

122 Fazzini, "In India-Pakistan Conflict, There's a Long-Simmering Online War"; and Summar Iqbal Babar, Muhammad Nadeem Mirza, and Irfan Hasnain Qaisrani, "Evaluating the Nature of Cyber Warfare between Pakistan and India," *Webology* 18, no. 6 (2021): 6973–6985.

123 Dylan Robertson, "Cyberattacks Hit Military, Parliament Websites as India-Based Group Targets Canada," Canadian Broadcasting Corporation, September 28, 2023, https://www.cbc.ca/news/politics/cyberattacks-parliament-india-1.6981399.

124 "After Canada and Palestine, Indian Hackers Launch Cyber Attacks on Qatar to Avenge Death Penalty of Former Navy Officers," Mint, November 8, 2023, https://www.livemint.com/news/world/indian-hackers-launch-cyber-attacks-on-qatar-to-avenge-the-death-penalty-of-indian-navy-officers-report-11699454790456.html; and Akinobu Iwasawa, "Israel-Hamas War Draws Russian, Indian ‹Hacktivists› into Shadow Conflict," *Nikkei Asia,* October 27, 2023, https://asia.nikkei.com/Politics/Middle-East-crisis/Israel-Hamas-war-draws-Russian-Indian-hacktivists-into-shadow-conflict.

125 Basu, "India's International Cyber Operations," 4, 8.

126 Nachiappan, "Going On The Offensive: India's Cyber Capabilities,"; and Singh and Jha, "From Code to Command," 232.

127 Arun Sukumar, "The Missing Option: India, Pakistan and Armed Conflict in Cyberspace," *ORF Digital Debates* 3 (2016): 1–6, https://scholarlypublications.universiteitleiden.nl/access/item%3A3618298/view.

128 Pratul Sharma, "From Nehru to Modi, PMs Have Always Taken Independent Foreign Policy Decisions," The Week, December 17, 2022, https://www.theweek.in/theweek/cover/2022/12/17/independent-foreign-policy-decisions-of-indian-prime-ministers.html.

129 Siddharthya Roy, "Indian Foreign Policy Under Narendra Modi: A Decade of Transformation," *Diplomat*, July 1, 2024, https://thediplomat.com/2024/06/indian-foreign-policy-under-narendra-modi-a-decade-of-transformation/.

130 "Who Is Ajit Doval, India's Longest-Serving NSA, Now in His Third Term under Modi 3.0," *Economic Times*, June 14, 2024, https://economictimes.indiatimes.com/news/defence/who-is-ajit-doval-indias-longest-serving-nsa-now-in-his-third-term-under-modi-3-0/articleshow/110971725.cms?from=mdr.

131 Niranjan Sahoo, "Decoding Modi's Foreign Policy," Carnegie Endowment for International Peace, September 23, 2014, https://carnegieendowment.org/research/2014/09/decoding-modis-foreign-policy?lang=en; Ashley J. Tellis, "Between the Times: India's Predicaments and its Grand Strategy," Carnegie Endowment for International Peace, December 3, 2012, https://carnegieendowment.org/posts/2012/12/between-the-times-indias-predicaments-and-its-grand-strategy?lang=en; and P.S. Raghavan, "The Making of India›s Foreign Policy: From Non-Alignment to Multi-Alignment," *Indian Foreign Affairs Journal* 12, no. 4 (326–341).

132 Ganguly, "India After Nonalignment."

133 Sumit Ganguly and Dinsha Mistree, "The Folly of India's Neutrality: In the Face of Chinese Aggression, New Delhi Must Align with Washington," *Foreign Affairs,* June 20, 2023, https://www.foreignaffairs.com/india/folly-indias-neutrality.

134 Anand, "Indian Non-Alignment 2.0"; and Singh, "Why Modi Can't Make India a Great Power."

135 Sumana Nandy, "PM Modi's Push for Atmanirbhar Bharat with Reference to Russia-Ukraine War in Victory Speech," *India Today*, March 10, 2022, https://www.indiatoday.in/india/story/pm-modi-push-for-atmanirbhar-bharat-with-reference-to-russia-ukraine-war-in-victory-speech-1923951-2022-03-10.

136 Rej and Sagar, "The BJP and Indian Grand Strategy," 82; and Sophie Landrin, "In the Himalayas, India Remains under Increasing Threat from China," *Le Monde*, February 2, 2023, https://www.lemonde.fr/en/opinion/article/2023/02/02/in-the-himalayas-india-remains-under-increasing-threat-from-china_6014076_23.html.

137 Michael Kugelman, "China Has Become India's Greatest Threat," *Foreign Policy*, April 18, 2024, https://foreignpolicy.com/2023/01/19/india-china-military-threat-security-pakistan/.

138 Anupreeta Das, Hari Kumar, and Vivian Wang, "India and China Reach Border Deal That Could Ease Hostilities," *New York Times,* October 22, 2024, https://www.nytimes.com/2024/10/22/world/asia/india-china-border.html.

139 Valbona Zaneli, “The Trends Driving Transatlantic Convergence on China,” *Diplomat,* November 30, 2023, https://thediplomat.com/2023/11/the-trends-driving-transatlantic-convergence-on-china/.

140 Robert D. Blackwill and Ashley J. Tellis, “The India Dividend: New Delhi Remains Washington’s Best Hope in Asia,” *Foreign Affairs,* August 12, 2019, https://www.foreignaffairs.com/articles/india/2019-08-12/india-dividend; Madan, “China Has Lost India”; Ganguly and Mistree, “The Folly of India’s Neutrality” and Deepak Upadhyay, “India Signs Deal with US for 31 Predator Drones to Boost Military’s Combat Prowess,” Mint, October 14, 2024, https://www.livemint.com/news/india/india-signs-deal-with-us-for-31-predator-drones-to-boost-militarys-combat-prowess-11728982615017.html.

141 The latest phase in the Quad’s life is relatively new, dating from 2021 onward. Its cybersecurity partnership is still emerging, so assessing its progress is difficult. As a relatively loose, informal “plurilateral” grouping, the Quad is essentially what its members choose to make of it. See Ravi Nayyar, “The Quad: Tackling the Spider, Not Cobwebs, in Cyberspace,” *The Interpreter (blog), Lowy Institute,* July 20, 2023, https://www.lowyinstitute.org/the-interpreter/quad-tackling-spider-not-cobwebs-cyberspace; Rajeswari Pillai Rajagopalan, “Fixing Cyber Vulnerabilities: An Agenda for the Quad,” Observer Research Foundation, February 16, 2024, https://www.orfonline.org/research/fixing-cyber-vulnerabilities-an-agenda-for-the-quad; Tobias Scholz, “Quad Vadis? A Risk Assessment of the Quad’s Emerging Cybersecurity Partnership,” Observer Research Foundation, August 17, 2023, https://www.orfonline.org/research/quad-vadis-a-risk-assessment-of-the-quad-s-emerging-cybersecurity-partnership; Mari Yamaguchi, “Japan, US, Australia, India at Tokyo Talks on Maritime and Cyber Security amid China Concerns,” *Independent,* July 29, 2024, https://www.independent.co.uk/news/china-ap-antony-blinken-tokyo-japan-b2587427.html.

142 Jaishankar, *Why Bharat Matters,* xvii.

143 Raghavan, “The Making of India›s Foreign Policy,” 328–329.

144 Tellis, “Troubles Aplenty.”

145 Amitendu Palit, “India’s Act East Policy and Implications for Southeast Asia,” *Southeast Asian Affairs* (2016): 81–92, https://www.jstor.org/stable/26466920.

146 Abul Kashem and Shariful Islam, “Narendra Modi’s Bangladesh Policy and India–Bangladesh Relations: Challenges and Possible Policy Responses,” *India Quarterly 72,* no. 3 (2016), 250–267; “Explained: How Sheikh Hasina’s Resignation Will Impact India-Bangladesh Ties,” *Economic Times,* August 5, 2024, https://economictimes.indiatimes.com/news/india/explained-how-sheikh-hasinas-resignation-will-impacts-india-bangladesh-ties/articleshow/112296686.cms; and Salil Tripathi, “Bangladesh Has a Difficult Road Ahead,” *Foreign Policy,* August 5, 2024, https://foreignpolicy.com/2024/08/05/bangladesh-sheikh-hasina-flees-protests.

147 Harsh V. Pant and Tobias Scholz, “BRICS: Expiring Political Relevance and Inspiring New Coalitions,” in *Handbook on Global Governance and Regionalism* (Edward Elgar Publishing, 2022), 148–159. See also Stuenkel, *The BRICS and the Future of Global Order.*

148 Karthik Nachiappan, *Does India Negotiate? (Oxford University Press, 2019), 197.*

149 Tellis, “America’s Bad Bet on India.”

150 Pant and Super, “Non-Alignment and Beyond,” 128.

151 Hannah Ellis-Petersen, Aakash Hassan, and Shah Meer Baloch, “Indian Government Ordered Killings in Pakistan, Intelligence Officials Claim,” *Guardian*, April 4, 2024, https://www.theguardian.com/world/2024/apr/04/indian-government-assassination-allegations-pakistan-intelligence-officials.

152 Hannah Ellis-Petersen, “India Appears to Confirm Extrajudicial Killings in Pakistan,” *Guardian*, April 5, 2024, https://www.theguardian.com/world/2024/apr/05/india-appears-to-confirm-extrajudicial-killings-in-pakistan.

153 “Debates (Hansard) No. 219 - September 18, 2023 (44-1) - House of Commons of Canada,” Parliament of Canada, archived October 15, 2023, https://perma.cc/N6D2-KUXY.

154 “Indian Nationals Charged in Murder of Canadian Sikh Activist,” *Japan Times*, May 4, 2024, https://www.japantimes.co.jp/news/2024/05/04/asia-pacific/politics/india-canada-arrests-killing/.

155 Hannah Ellis-Petersen and Leyland Cecco, “India Orders Canada to Remove 41 Diplomats from Delhi Embassy,” *Guardian*, October 3, 2023, https://www.theguardian.com/world/2023/oct/03/india-orders-canada-to-remove-41-diplomats-from-delhi-embassy-reports.

156 Saira Bano, "The Fallout of India's Extrajudicial Killings," Georgetown Journal of International Affairs, April 9, 2024, https://gjia.georgetown.edu/2024/04/09/the-fallout-of-indias-extrajudicial-killings/.

157 "Justice Department Announces Charges in Connection with Foiled Plot to Assassinate U.S. Citizen in New York City," U.S. Department of Justice, November 29, 2023, https://www.justice.gov/opa/pr/justice-department-announces-charges-connection-foiled-plot-assassinate-us-citizen-new-york.

158 Ajai Shukla, "US Blocks $3-Billion Drone Sale to India Until 'Meaningful Investigation' of Pannun Assassination Conspiracy," The Wire, January 31, 2024, https://thewire.in/security/us-drone-sale-sky-guardian-pannu-killing-investigation.

159 Consider just two of several such passages: "In the final analysis, hard power will always score over soft power. Ideally, the two should be in lock-step, so that capabilities and influence grow side by side." And from the same publication: "What characterises our times is a willingness to be far more muscular and unabashed in using the toolbox of influence and capability." Jaishankar, *Why Bharat Matters,* 196 and 168.

160 Anand, "Indian Non-Alignment 2.0"; Blackwill and Tellis, "The India Dividend"; Markey, "India as It Is"; Rohan Mukherjee, "A Hindu Nationalist Foreign Policy: Under Modi, India Is Becoming More Assertive," *Foreign Affairs,* April 4, 2024, https://www.foreignaffairs.com/india/hindu-nationalist-foreign-policy; Tellis, "America's Bad Bet on India."

161 Jaishankar, *Why Bharat Matters, 3.*

162 Shishir Gupta, "Why Was PM Modi's Visit to Russia Strategically Important?," *Hindustan Times*, July 11, 2024, https://www.hindustantimes.com/india-news/why-was-pm-modis-visit-to-russia-strategically-important-101720681226190.html; and Jayaprakash, "The State of India-Russia Relations."

163 Markey, "India as It Is."

164 Basu and Nachiappan, "Will India Negotiate in Cyberspace?," 189–210.

165 "Annual Report 2019-20," Indian Ministry of External Affairs, accessed March 17, 2025, 31–32, https://www.mea.gov.in/Uploads/PublicationDocs/32489_AR_Spread_2020_new.pdf.

166 Jaishankar, *Why Bharat Matters,* 164.

167 Singh and Jha, "From Code to Command," 230.

168 Mukerji, "The Need for an International Convention on Cyberspace," 202–205.

169 Trisha Ray and Akhil Deo, "Priorities for a Technology Foreign Policy for India," ORF Issue Brief 403, September 2020, 7, https://www.orfonline.org/wp-content/uploads/2020/09/ORF_IssueBrief_403_TechForeignPolicy.pdf.

170 Arindrajit Basu, "India's 'passive' Multistakeholder Cyber Diplomacy" in Ian Johnstone, Arun Sukumar, and Joel Trachtman (eds.), *Building an International Cybersecurity Regime: Multistakeholder Diplomacy* (Edward Elgar Publishing, 2023), 201–219; Basu and Nachiappan, "Will India negotiate in cyberspace?," 189–210.

171 Gupta, "Securing Cyberspace."

172 Gupta, "Securing Cyberspace."

173 In the absence of a published national cyber strategy that incorporates all elements of cyber statecraft, it is still possible to conceive of a strategic approach, defined by principles and observed behavior. See Nina Silove, "Beyond the Buzzword: The Three Meanings of 'Grand Strategy,'" *Security Studies 27,* no. 1 (2017): 27–57.

174 "'Delhi Declaration' for Responsible State Behaviour in Cyberspace for G20 Countries," *The Hindu,* June 5, 2023, https://www.thehindu.com/news/national/delhi-declaration-for-responsible-state-behaviour-in-cyberspace-for-g20-countries/article66933354.ece; "Joint Statement on the Inaugural India-Australia Foreign Ministers' Cyber Framework," Indian Ministry of External Affairs, February 12, 2022, https://www.mea.gov.in/bilateral-documents.htm?dtl/34860/Joint+Statement+on+the+Inaugural+IndiaAustralia+Foreign+Ministers+Cyber+Framework+Dialogue; "India-UK Cyber Statement, April 2022," UK Prime Minister's Office, April 22, 2022, https://www.gov.uk/government/publications/prime-minister-boris-johnsons-visit-to-india-april-2022-uk-india-joint-statements/india-uk-cyber-statement-april-2022.

175 Mukerji, “The Need for an International Convention on Cyberspace.”

176 Basu, “India’s ‘Passive’ Multistakeholder Cyber Diplomacy,” 214.

177 Basu, “India’s ‘Passive’ Multistakeholder Cyber Diplomacy,” 201.

178 Syed Akbaruddin, “A Quest for Order Amid Cyber Insecurity,” *The Hindu,* July 30, 2020, https://www.thehindu.com/opinion/lead/a-quest-for-order-amid-cyber -insecurity/article32225383.ece.

179 Basu, “India’s ‘Passive’ Multistakeholder Cyber Diplomacy,” 203.

180 Basu, “India’s ‘Passive’ Multistakeholder Cyber Diplomacy,” 204.

181 Basu and Nachiappan, “Will India Negotiate in Cyberspace?,” 191.

182 André Barrinha and Rebecca Turner, “Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia, and India,” *Contemporary Security Policy* 45, no. 1 (2024): 72–109, https://www.tandfonline.com/doi/full/10.1080/13523260.2023.2266906.

183 Basu and Nachiappan, “Will India Negotiate in Cyberspace?,” 195.

184 Rahul Prakash, “India-US Cyber Relations,” Observer Research Foundation, January 14, 2014, https://www.orfonline.org/research/india-us-cyber-relations; “U.S.-India Cyber Security Forum: Enhanced Cooperation to Safeguard Shared Information Infrastructures,” U.S. Department of State, March 3, 2006, https://2001-2009.state.gov/p/sca/rls/fs/2006/62530.htm.

185 Norman P. Neureiter and Michael Cheetham, “The Indo-U.S. Science and Technology Forum as a Model for Bilateral Cooperation,” *Science & Diplomacy* 2, no. 4 (December 2013): https://www.sciencediplomacy.org/sites/default/files/the_indo-u.s._science_and_technology_forum_science__diplomacy_0.pdf.

186 “Remarks on India and the United States: A Vision for the 21st Century,” U.S. Department of State, July 20, 2011, https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/07/168840.htm.

187 Rajagopalan, “Fixing Cyber Vulnerabilities”; “Fact Sheet: 2024 Quad Leaders’ Summit,” Indian Prime Minister’s Office, September 22, 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2057460; “Joint Statement on the 2024 Quad Cyber Challenge,” Ministry of External Affairs, October 22, 2024, https://www.mea.gov.in/bilateral-documents.htm?dtl/38448/Joint+Statement+on+the+2024+Quad+Cyber+Challenge.

188 Basu and Nachiappan, “Will India Negotiate in Cyberspace?,” 194.

189 Basu and Nachiappan, “Will India Negotiate in Cyberspace?,” 195.

190 Jaishankar, *Why Bharat Matters,* 163–168.

191 Basu and Nachiappan, “Will India Negotiate in Cyberspace?,” 196.

192 Basu, “India’s ‘Passive’ Multistakeholder Cyber Diplomacy,” 215–216.

193 Basu, “India’s ‘Passive’ Multistakeholder Cyber Diplomacy,” 218–219; and Basu and Nachiappan, “Will India Negotiate in Cyberspace?,” 203.

Carnegie Endowment for International Peace

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 170 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

Technology and International Affairs

The Technology and International Affairs Program develops insights to address the governance challenges and large-scale risks of new technologies. Our experts identify actionable best practices and incentives for industry and government leaders on artificial intelligence, cyber threats, cloud security, countering influence operations, reducing the risk of biotechnologies, and ensuring global digital inclusion.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org