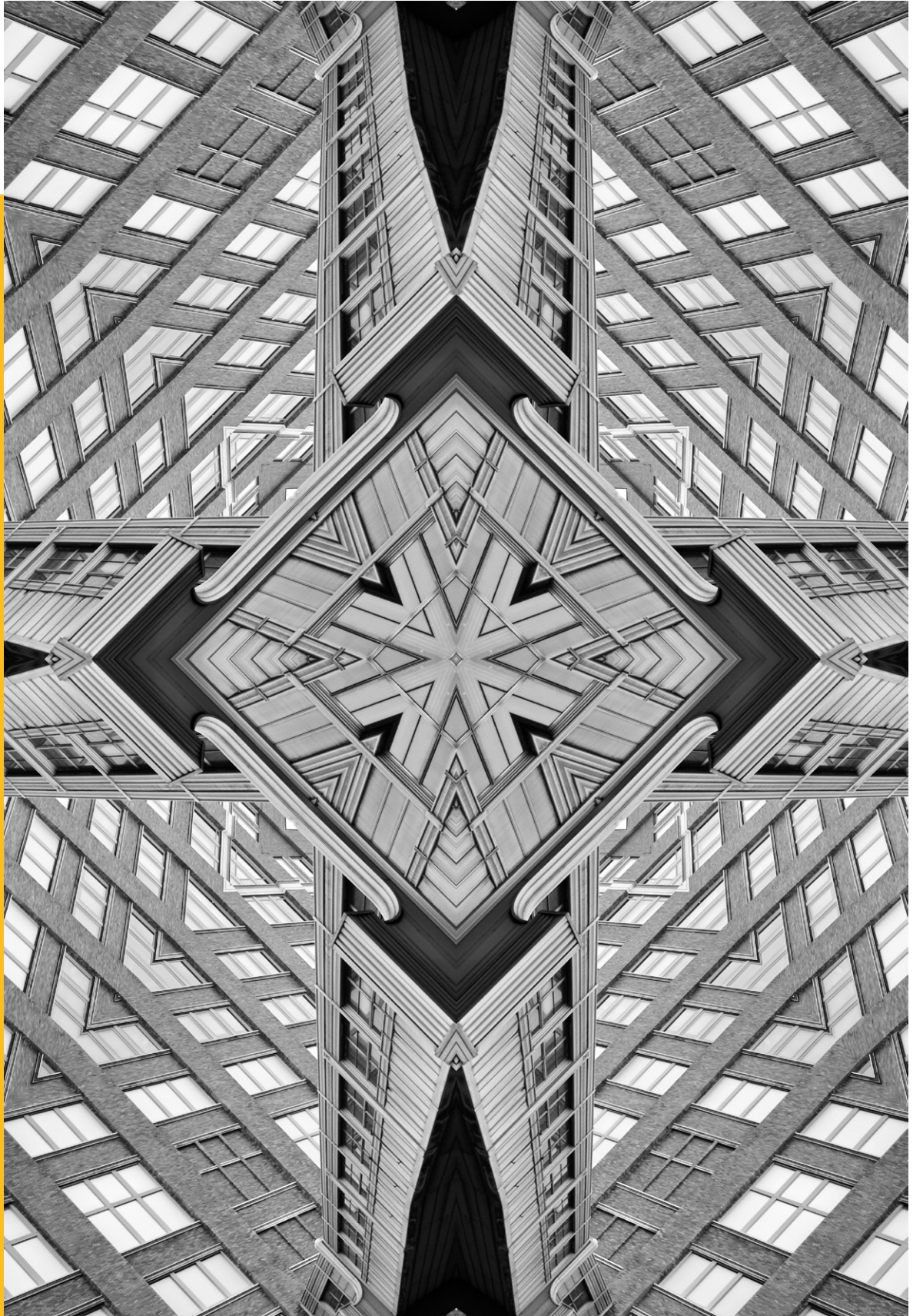


# Occasional Paper



**ISSUE NO. 445 AUGUST 2024**

© 2024 Observer Research Foundation. All rights reserved. No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from ORF.



# Securing the Critical Technology Supply Chain as a Function of National Intelligence

Archishman Goswami

## Abstract

This paper examines the role that national intelligence agencies may play in helping to secure critical technology supply chains. As the race for scientific advantage becomes increasingly characteristic of national security concerns amid growing multipolarity and interstate competition, national intelligence agencies are paying greater attention to the security of critical and emerging technologies. This paper analyses how intelligence agencies may work and adapt in relation to the specific challenges posed by this issue. The analysis is divided into sections on intelligence (examining the broadening of intelligence-gathering horizons and the likelihood of ally-on-ally espionage); counterintelligence (focused on insider threats from within the private sector); and covert action (assessing the potential for paramilitary action and offensive cyber to achieve kinetic effect vis-à-vis a competitor's supply chains).



## What unites Byzantium, Woodrow Wilson, and Beethoven?

**A**round 550 CE, Byzantine emperor Justinian I's efforts to produce silk—a highly valued luxury commodity—within the confines of his empire, and thus break the Chinese and Persian monopolies over its production and export, finally bore fruit when silkworms and secret methods of silk production were smuggled over from China by two travelling Indian monks.<sup>1</sup> In 1914, during the First World War, United States (US) President Woodrow Wilson, frustrated by his inability to prohibit US arms manufacturers from selling their wares to European powers, regretted that he “could do nothing else than leave the matter to settle itself”, as “the sales proceed from so many sources, and my lack of power is so evident.”<sup>2</sup> And in 2024, the Dutch government would launch a covert operation named after the classical composer, Ludwig van Beethoven, earmarking close to 3 billion euros to prevent semiconductor manufacturer ASML from moving its operations outside the Netherlands, where the possibility of compromise or trade theft is likelier.<sup>3</sup>

Defined by Mentzer et al. (2001) as “a set of three or more entities (organisations or individuals) directly involved in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer”, supply chain management has long dovetailed questions of strategic interest.<sup>4</sup> It has been the throughline connecting Byzantine trade theft, President Wilson's frustrations, and the Netherlands' domestic semiconductor manufacturing. Amid global power shifts in a world order that is as interconnected as it is competitive, the role of supply chains in undergirding domestic resilience, national power, and foreign policy is clearer than ever. As such, it must increasingly be treated as a domain of interest by global intelligence services, including in India.

Perhaps nowhere is this clearer than in the domain of critical and emerging technologies. Scientific advantage, underpinned by supply chain security, has long been seen as a determinant of strategic potential. It is therefore not unexpected that supply chains have come to be securitised in the current global geopolitical landscape, with both state and non-state actors seeking to gather intelligence on the capabilities of their adversaries, or even subvert or compromise them through kinetic or non-kinetic action. This is especially true in strategically sensitive areas like space technology, quantum computing, bioengineering, or artificial intelligence (AI). Examples abound, with Belgian intelligence agencies noting China's efforts to gather intelligence on supply chain systems at Liège cargo airport, and the arrest of a Russian spy in Germany in 2023 for collecting classified information on technologies and supply chains associated with the European Union's (EU) Ariane space programme.<sup>5,6</sup>

With their unique reach and skill sets, intelligence agencies, as custodians of national security, are equipped to secure supply chains against compromise even as they endeavour to maintain national advantage in this field. This paper is therefore trifurcated into sections examining the issue from the perspectives of intelligence (gathering sensitive and classified information on adversaries' and allies' supply chains); counterintelligence (securing one's own supply chains from the challenges posed by insider risks); and covert action (deploying kinetic effect to offensive effect against adversaries and their supply chains when faced with an active threat). The study will interrogate the positionality of national intelligence within supply chain security, examining how they may be used best to respond to challenges in this domain—while maintaining a focus on policy ramifications for the Indian government and strategic community.

“Amid global power shifts in a world order that is as interconnected as it is competitive, the role of supply chains in undergirding domestic resilience, national power, and foreign policy is clearer than ever.”

## A more global focus

**T**he geopolitics of supply chain management compels intelligence agencies to develop capabilities for information-gathering in increasingly unfamiliar geographies, given how supply chains are decentralised. This is a particular challenge for Indian intelligence agencies which, unlike their counterparts in advanced countries, lack the requisite economies of scale to enable unilateral collection of global intelligence.

Structurally dispersed across vendors, infrastructures, and logistical networks operating in a range of international jurisdictions, critical technology supply chains necessitate an expansion of intelligence-gathering capabilities across more diverse geographies. As security vulnerabilities across various points within a supply chain have far-reaching effects on national security, a purely regional focus for any intelligence service becomes insufficient. Cloud interdependencies operating across national jurisdictions and continents underpin the digital infrastructure sustaining global supply chains.<sup>7</sup> Factors such as these frame the various issues of supply chain security, even as producers of critical technology diversify lines of production and logistics to other countries to mitigate the risks.<sup>8</sup>

Moreover, a multiplicity of vendors, logistical networks, and infrastructures expands the risks for compromise via the ‘backdoor’—where an adversary’s security agency is able to embed its capabilities via a single ‘weak link’ within the technological components and networks comprising the supply chain.<sup>9</sup> Concerns exist, for instance, about the latitude this provides for revisionist powers such as China, a key producer of rare-earth minerals key to critical technology manufacture, in leveraging its position to exert pressure on adversaries.<sup>10</sup> Indeed, it is the logic carried by these changing dynamics that underpins new concepts in international relations thought such as ‘weaponised interdependence’, with scholars such as Henry Farrell and Abraham Newman taking note of the ‘chokepoints’ within a single supply chain that may serve as leverage by hegemon against adversaries.<sup>11</sup>

The changing circumstances must result in a new posture towards intelligence gathering in countries such as India. Given the characteristic dispersal of key critical technology supply chain nodes across diverse geographies, governments such as India’s may choose to coordinate the geographic focus of their intelligence collection efforts towards those countries and jurisdictions of importance within the supply chains of specific technologies. For example, one

may look at semiconductor devices required in critical national infrastructures and increasingly a determinant of geopolitical heft. A combination of liaison agreements and unilateral intelligence collection efforts, contingent on the state of diplomatic relations, the availability of time and resources, and political will, may help countries such as India to gather valuable intelligence to better secure semiconductor supply chains and ensure national resilience. Liaison agreements may be reached with intelligence services in Vietnam, Thailand, and Japan, for example, which share close strategic ties with New Delhi and who are India's fastest growing import sources for semiconductor devices.<sup>12</sup>

Yet this approach is subject to change, particularly when gathering intelligence about a country like China which, despite its belligerence towards India, is still nevertheless the source of over 50 percent of the latter's yearly semiconductor imports.<sup>13</sup> Intelligence on Chinese supply chain management and its corollary effects on semiconductor imports and their potential leverage may be accessed either through friendly third-country agencies willing to use their proximity to a certain part of the supply chain to gather intelligence for the R&AW, but where necessary, using the R&AW itself for this purpose. Allocating resources accordingly would provide a cost-effective means of gathering valuable intelligence on this critical area of national security.

It is in view of these changing dynamics, and their associated strategic implications for supply chain security, that all national intelligence services, including India's, must develop a wider array of intelligence-gathering assets, both human and technical, across less familiar geographies. Where this is not possible owing to the paucity of resources, national intelligence services should establish effective and reliable liaison agreements to expand reach in these regions, and identify both government bureaucracies and involved private sector actors to gain access to intelligence. Given their centrality to national security, supply chain management must increasingly come to determine trajectories of intelligence collection, and treated accordingly within the state's strategic agenda.

The globalised character of the supply chain has caused a wider reconsideration of partnerships and traditional alliances in geopolitics. As companies and governments seek to mitigate supply chain risks through processes of friendshoring or nearshoring,<sup>a</sup> questions remain about the extent to which these nodes are secure.<sup>14,15</sup> Neither of these strategies ensures complete separation of one's own supply chains from an opponent's influence, particularly in a multipolar world where the vast majority of states seek to 'hedge' between multiple strategic and economic partnerships as opposed to the formal alliances characterising the geopolitical order of the past century.<sup>16</sup> One economic power may leverage its existing relations with an ally of its adversary to undercut the latter's potential, compromise its functioning, or even drive a wedge between the two.

One may take, for instance, the US-led 'Chip 4' alliance, a loose coalition between the US and its East Asian allies, Japan, South Korea and Taiwan, established in 2021.<sup>17</sup> Concerns remain about what this four-way partnership may ultimately achieve, particularly given South Korea's membership. Despite its close strategic partnership with the US in view of regional security on the Korean peninsula, South Korean semiconductor supply chains are also closely tied in with China. Estimates suggest that Korean semiconductor companies SK-Hynix and Samsung Electronics manufacture, respectively, 40-50 percent and 40 percent of their chips in China.<sup>b,18</sup> There is therefore a clear convergence between the decentralised character of global supply chains, and the evolution of interstate relations in a multipolar world—patterns that are expected to make their way into the information-gathering priorities and agenda for national intelligence agencies.

There are two ways in which these intelligence efforts may materialise. The first is the establishment of closed-door mechanisms for intelligence sharing and communication around the field of critical and emerging technologies in the context of supply chain security. Greater transparency and trustful communication within these closed settings may help facilitate avenues for interoperability among partners in this field. Indeed, it is hoped that the establishment of the NSA-level US-India initiative on Critical and Emerging Technologies (iCET) in 2023, and regular communications between national

---

a 'Friendshoring' is the establishment of key supply chain nodes in ally or partner countries; 'nearshoring' is locating those nodes in neighbouring countries.

b These chips eventually make their way via the supply chain into critical infrastructures in the US.

security and intelligence officials on either side to this end, will allow a modicum of trust on either side in achieving supply chain security.<sup>19</sup> This was also observed in the Quad's establishment of the Critical and Emerging Technologies Working Group in 2021, which provides the mechanisms and infrastructure for Indian, US, Japanese and Australian security officials to parley on such issues as the proliferation of dual-use technologies, the presence of threat actors in one another's supply chains, and coordinated action to resolve common problems in this field.<sup>20</sup>

More controversially, though no less common, is ally-on-ally espionage (AAE)—spying on one's partners and allies to gain a better understanding of their vulnerabilities and intent to achieve strategic advantage. Although AAE is discouraged for the deleterious effects it has on longer-term trust and reputation, the globally dispersed configuration of modern critical technology supply chains and immediate real-world geopolitical circumstances may occasionally require such a line of action. This is true particularly when full intelligence about a competitor state's level of involvement in a partner's supply chain, and its strategic intent within this capacity, cannot be known through cooperation agreements alone.

Indeed, with China dominating around a quarter of the current global 300 mm chip market, it is inevitable that some of these chips become embedded within the supply chains of partner countries such as Bangladesh, Malaysia, or Vietnam; this has potential strategic implications for India.<sup>21,22,23</sup> While efforts to mitigate against the national security ramifications for India may ideally be pursued through agreements to exchange intelligence of strategic value with one another, where such intelligence is not forthcoming,<sup>c</sup> AAE may serve as a policy option. While it must still be seen as a measure of last resort owing to the longer-term consequences its exposure may have on trust and bilateral relations, AAE of such a kind would follow a pattern of action quietly pursued by great powers over history, and which has been publicly justified by global intelligence chiefs, including James Woolsey, Director of the CIA in the 1990s.<sup>24</sup>

Cases abound, from Soviet espionage during the Second World War on the Manhattan Project<sup>d</sup> being pursued at the time by its British and American allies<sup>25,26</sup> to, in more recent times, the revelations made about US spying against Germany and South Korea by the Snowden and Discord leaks in 2013 and

---

c This would be true, for instance, with Bangladesh, where political upheaval since August 2024 presents a possible reversal of diplomatic ties with India.

d The Manhattan Project refers to the joint efforts by the UK, US, and Canada, from 1942-1946, to develop atomic weapons amid the Second World War.



# Evolving Alliances?

2023,<sup>e</sup> respectively.<sup>27,28</sup> AAE would be inevitable, when conducted to gain a better understanding of the strategic risks to oneself due to the involvement of a malign actor like China within a partner's supply chains, and only after careful deliberation of the longer-term reputational costs of such action.

Ultimately, however, national intelligence agencies will likely employ a combination of the two methods to achieve their ends in pursuit of supply chain security. While existing mechanisms for intelligence sharing and coordination vis-à-vis critical technology supply chains will be actively used, as they are in India-US bilateral relations or multilateral fora like the Quad, AAE is likely to continue and even proliferate. As such, a greater proportion of intelligence resources are likely to be allocated towards estimating allied supply chain capabilities, and it is therefore recommended that more time and institutional assets are managed in accordance with common analytical problems of optimism biases, ethnocentrism, and sunk-cost fallacies accompanying these endeavours.<sup>29</sup>

“There is a clear convergence between the decentralised character of global supply chains and the evolution of interstate relations in a multipolar world.”

---

e Refers, respectively, to the disclosure of the United States' global surveillance programs by intelligence contractor Edward Snowden in 2013, and to the leaks of sensitive military intelligence documents on social media app Discord in 2023.

## Insider Threats

Supply chains today, especially in the critical technology and deep-tech sectors,<sup>f</sup> represent a complex of public and private sector interests. Yet with the unprecedented and growing scale of public-private cooperation in this sector and supply chain security comes the risks of insider threats targeting the private sector involved in such projects. From a national security standpoint, corporate/industrial espionage challenges such as these not only threaten the resilience of supply chains and wider strategic interests, but also necessitate a shift in how counterintelligence is perceived, structured, and implemented by the intelligence establishment.

Demonstrative of the convergence between corporate and state security, insider threats generally refer to the compromise of company secrets by an employee, which may occur either as a result of negligence, or malicious behaviour. The former is more common, with an estimated 56 percent of reported insider threat cases in the cyber sector occurring as a result of employee carelessness.<sup>30</sup> As governments worldwide, including India's, seek to secure critical technology supply chains through expanded cooperation with the private sector, intelligence services will need to increasingly account for the likelihood of insider risks caused by such atomised cases of negligence from within private sector partners and establish premeditated countermeasures in this regard.

Insider risks, however, can also emerge from the activities of a disgruntled, coerced or otherwise suborned employee within a private company working with the government in a critical part of the supply chain can always leverage their proximity to information of strategic value to compromise the supply chain.<sup>31</sup> Insider risks can be human, but more often than not, rely on an embedded individual to compromise a company's cybersecurity through viruses or ransomware deployed to steal secrets, or cause cyber systems to malfunction. Examples include a case in 2021 where an embittered employee of US healthcare company Stradis Healthcare deleted critical shipping data from the company's servers, delaying the delivery of important PPE kits to clients at the height of the Covid-19 pandemic.<sup>32</sup> In 2023, two former employees of Tesla were arrested for using their position to access the personal data of 75,000 employees at the company and attempting to sell it to German media outlets.<sup>33</sup>

---

<sup>f</sup> Sectors such as space and synthetic biology are some cases where these convergences are most visible, among others.

# Counterintelligence Activity

The wider malaise materialised by way of such examples is compounded by the broader cultural mismatch between the private sector, particularly those companies working in critical and emerging technologies like AI, and the state. The former remains generally wary that the state would deploy their technologies for military or strategic purposes.<sup>34</sup>

The detrimental effect posed to national security and strategic objectives on account of insider threats from within the private sector is not new. In the 1970s and 1980s, James Durward Harper, a Silicon Valley-based freelance engineer was arrested for using his proximity to a company working with the US government on its Minuteman-III ICBM systems to gather secrets for Polish intelligence.<sup>35</sup> What makes the current phase of insider threats particularly challenging for counterintelligence services, however, is the sheer scale of its proliferation. As governments cooperate more with the private sector in order to secure scientific and technological advantage in critical fields, the possibility of insider threats from within these private tech companies grows—and with it, ensuing challenges in terms of ensuring supply chain resilience in these domains.

The 2022 arrest of Chinese intelligence officer Xu Yanjun for the theft of trade secrets from GE Aerospace,<sup>36</sup> which has a number of manufacturing contracts with arms of the US government,<sup>37</sup> and the 2024 arrest of Linwei Ding, a Chinese engineer at Google, for stealing AI secrets for Beijing—portend a larger trend in counterespionage over this decade. It is one where insider threats grow within technological programmes and supply chains, and the lines between corporate and national intelligence blur to generate new challenges.<sup>38</sup> This, in turn, creates new challenges for and will shape the character of counterintelligence in the 2020s and beyond.

Although many of these examples may originate in the US, the counterintelligence challenge posed by insider threats is a global one, which countries such as India must begin preparing for. The establishment of indigenous technological manufacturing/innovation capabilities and supply chains to that end is a cornerstone of the government's vision of achieving a *Viksit Bharat* by 2047,<sup>39</sup> and is represented in the 2024 Union Budget's earmarking of INR100,000 crore (approx. US\$13.5 billion) for deep-tech research and development within the private sector.<sup>40</sup> One area where India has made strides in partnership with the private sector is space. Companies such as Pixxel, Skyroot, and Agnikul Cosmos have progressed in their field, including, like their older and better-established Western counterparts, working closely with the government in the defence and security spheres.<sup>41</sup> To this end, it becomes critical, from a counterintelligence perspective, to establish the requisite preventive and counter-measures to mitigate the risks posed to the resilience in their supply chains.



# Counterintelligence Activity

National security and intelligence agencies worldwide have increasingly taken cognisance of this challenge, with steps being taken by both governments and the private sector to prevent the compromise of key supply chains. In 2024, OpenAI began hiring an “insider risk investigator”, whose role includes liaising with the White House to combat insider threats to the theft or compromise of sensitive technologies and information within the supply chain by hostile state and non-state actors.<sup>42</sup> The year before, the UK announced the establishment of the National Protective Security Authority,<sup>43</sup> an agency placed under the authority of domestic and counterintelligence service MI5 to liaise with the private sector and protect critical national infrastructure and supply chains from compromise, with the new authority placing special focus on combatting insider threats.<sup>44</sup>

Likewise, the US Director of National Intelligence’s National Counterintelligence and Security Centre has published directives specially designed towards ensuring the security of supply chains and their resilience using a range of counterintelligence strategies and assets.<sup>45</sup> Policies such as these not only help arrest active, malign efforts by competitors and adversarial entities seeking to undermine the functioning of one’s supply chains, but also provide private sector partners with strategies and best practices to reduce insider risks. They provide a potential template for action for other governments, such as India’s, which seek to project power in the coming years as nodes of technological innovation and its associated supply chains.

“An estimated 56 percent of reported insider threat cases in the cyber sector occur as a result of employee carelessness.”

## Paramilitary Action

**A**s sub-threshold interstate conflict comes to define the language of international relations, supply chains, as infrastructural articulations of geopolitical intent, have come to serve as sites of strategic competition. Covert action—triangulated between paramilitary operations, the use of propaganda, and political action, among other strategies—is likely to be central to intelligence functions as espionage services are increasingly used by governments to undermine the integrity and resilience of competitors’ supply chains.

Kinetically-underpinned competition of such kind would be driven largely by reliance on paramilitary action. Depending on the availability of resources or intent meant to be signalled by such action, intelligence services may use proxy actors, or special forces units themselves, to disrupt a competitor’s logistical routes, or access to raw materials or processed components critical in the critical technology sector, such as rare-earth minerals or semiconductors. In either respect, such action would be informed by the principle of ‘strategic disruption’—a concept formulated by the RAND corporation in 2023.<sup>46</sup>

Examples proliferate, both within India’s neighbourhood and further afield, of the potential of both special forces and proxy paramilitary actors in demonstrating political muscle through the intended or united ‘strategic disruption’ of supply chains. In Myanmar, instability generated by conflict has given rise to an underground mining economy, of which paramilitary actors, including both pro-junta militias and rebel groups like the Kachin Independence Organisation, are a key part. The illicit mining of rare-earths as Dysprosium and Terbium key to the manufacturing of technological devices like electric vehicle batteries, has more than doubled between 2021 and 2023, from 19,500 to 42,000 tonnes.<sup>47</sup>

Farther afield, reports surrounding the involvement of US and Ukrainian intelligence/paramilitary organisations in covertly organising the explosion of the Nordstream pipeline in 2023 further indicates an appetite for ‘strategic disruption’ of supply chains within the mandate of special operations forces globally.<sup>48</sup> Either way, these cases demonstrate how paramilitary actors may be used in covert operations to undermine the functioning of competitors’ supply chains. Locally-embedded proxies or insurgent groups, as in Myanmar, may entrench themselves within resource extraction processes to undermine a competitors’ supply chains—a strategy that may be weaponised by adversary intelligence services to undercut subsequent economic gains and technological potential. Likewise, kinetic measures may be employed by intelligence services to damage the infrastructure sustaining these supply chains for the same strategic

# Covert Action and Supply Chains

ends, as seen in the underwater explosion of the Nordstream pipeline. In either of these cases, deniability is maintained by the culprit nation-state/strategic actor, and conflict occurs under the threshold of direct warfare. Yet the damage done is significant and is contingent on a strategic actor's willingness to employ force and unconventional tactics to compromise a competitor's objectives through the supply chain.

Governments such as India's may therefore seek to not only grow their covert action capabilities, but also establish countermeasures against such possible action. Clandestine diplomacy<sup>g</sup> must be pursued with local, militarised actors operating in regions (such as Myanmar and similar areas of strategic value with holding key resource deposits) where they hold the potential to determine outcomes for supply chains in terms of impacting logistics or access to resources.<sup>49</sup> Efforts may be taken to this end to identify intermediaries, establish channels of communication, but most importantly, to identify points of leverage over these actors which may enable negotiation and the process of clandestine diplomacy to move forward.

The Indian government may equally choose to take stock of the readiness of its tri-services special forces to adopt lessons relating to strategic disruption, and apply them in India's distinct context to use both defensive and offensive measures to secure critical technology supply chains. Established in 2019, the Armed Forces Special Operations Division (AFSOD) may organise military exercises, both alone and with trusted international partners, around situations requiring principles of strategic disruption to be employed either to secure one's own supply chains or undermine an adversary.<sup>50</sup> Lessons may be complemented by simultaneously establishing direct and covert lines of communication between AFSOD and the R&AW's autonomous paramilitary service, the Special Group, in developing strategies to deploy and defend against strategic disruption of supply chain infrastructures through kinetic action.

Ultimately, paramilitary action holds potential for both attackers and defenders of supply chains. Utilising the principle of 'strategic disruption', states may deploy both militarised proxies or special forces to undermine a competitor's supply chain logistics and infrastructure, diminishing the latter's ability to challenge one's own supply chain security. Politically unstable settings, or circumstances under which access to key raw materials is fraught by conflict dynamics—of which India's neighbourhood is replete (Myanmar being a key example)—provide the conditions under which such strategies may be employed.

---

<sup>g</sup> Some scholars see clandestine diplomacy as a form of covert action owing to its deniability and objective of achieving 'kinetic' effect by synthetically shaping the political aftermath.



## Offensive Cyber

Likening the most effective form of cyber-defence to “shooting the gun out of an outlaw’s hand before he can shoot it”, political theorist Joseph Nye argues that the character of cyber blurs the lines between defensive and offensive tactics, with the best defence requiring the constant pursuit of active offensive methods against threat actors, reliant on plausible deniability in order to maintain the element of surprise and therefore effectiveness.<sup>51</sup> Nowhere is this intertwined character clearer than in the use of cyber by intelligence services to secure their nation’s critical technology supply chains, and undermine competing ones, particularly as the success of supply chains come to be increasingly predicated upon the ability of computer technologies to support their functioning.

It is this symbiosis between software and critical technology supply chains that comes to the fore each time a cyberattack hampers or compromises the functioning of the supply chain. Threats like ransomware and data breaches and malware paralysing the functioning of key infrastructures pose a threat to the overall resilience of supply chains and diminish foreign investor and governmental confidence in the ability of a targeted state to secure their economic interests. This presents a geopolitical challenge that threat actors may seek to leverage for strategic gain.<sup>52</sup>

Given the overlaps between offence and defence in the use of cyber by intelligence and military agencies for strategic purposes, securing supply chains through a greater focus on covert action against threat actors in the cyber domain must become a critical area of focus for national intelligence agencies. The range of components and stakeholders within critical technology supply chains, from private financial institutions to tech companies and governments, allows hostile actors greater latitude in subverting the supply chain through any single stakeholder or node. The 2020 Solarwinds hack, for instance, was enabled by threat actors embedding themselves within cyber infrastructures upon which supply chains depend, causing insurers at least US\$90 million in losses as supply chains were affected globally.<sup>53,54</sup> Yet despite this impact, plausible deniability, facilitated by the amorphous character of cyberspace, has precluded any efforts to conclusively determine the responsibility of any primary strategic actor for the attack. US sources, though, have indicated the involvement of the Russian intelligence services<sup>55</sup> through its cyber-proxy APT29, also known as ‘Cozy Bear’.<sup>56</sup> If true, the incident is revelatory in highlighting two key dimensions of covert action in cyberspace and its overlap with supply chain security. First, it highlights the offensive targeting of adversaries’ supply chains as an increasingly

# Covert Action and Supply Chains

central function within the national intelligence mandate, allowing one nation to gain short- to medium-term strategic advantage vis-à-vis another. Second, the nature of cyberspace and the amorphous character of proxy actors in this domain not only makes attributability harder to achieve, but also incentivises offensive action by diminishing power differentials among strategic actors.


Aspects such as these underscore the need for the Indian government to develop and implement creative solutions towards the defence of supply chains by intelligence services in cyberspace. Some measures have been taken to this end. The Defence Cyber Agency (DCA), established in 2019, has organised wargames and simulations to increase supply chain and critical national infrastructure resilience against cyberattacks by hostile threat actors.<sup>57</sup> More remains to be done, however. It is recommended that the National Technical Research Organisation (NTRO), India's primary signals intelligence service, expand its mandate to focus on offensive tactics as a means of securing supply chains. An appetite for such a policy already exists, with NTRO chairman Arun Sinha underscoring the defence of supply chains using both passive and kinetic measures as a critical part of the agency's mandate.<sup>58</sup>

Another strategy would be the construction of a separate offensive cyber intelligence agency. While offensive action exists as part of the mandate of the DCA, ultimately, it operates under the command of the tri-services of the Indian armed forces. There is no other civilian intelligence agency, beyond the NTRO, which possesses the cyber capabilities required to secure supply chains through offensive action against threat actors. The establishment of such an agency would not only allow existing services such as the NTRO to avoid resource overstretch by instead focusing more on intelligence collection and security measures relating to counterintelligence, but also tie in better to India's current national security posture of 'defensive offence'—i.e., the principle that threat actors must be actively countered in order to best preserve national security and defence.<sup>59</sup> Given the centrality of this logic to cyber conflict, as underlined in Nye's abovementioned quote, such a strategy would help India achieve favourable outcomes in securing supply chains, particularly in critical technologies, from cyber threats, while managing resources more economically.

This paper has discussed some of the means by which national intelligence agencies may adapt and optimally respond to threats to supply chains and the associated national security implications. In the first section, it argued that the globally-dispersed character of the modern critical technology supply chain necessitates a similarly global focus within intelligence gathering and analysis today. Likewise, the globalised and dispersed character of the modern supply chain must also push intelligence agencies to better appreciate their allies' capabilities

From a counterintelligence perspective, the challenge posed by insider threats from within the private sector is noted, alongside potential countermeasures to enact in this regard. Public-private partnerships are not increasingly characteristic of today's deep-tech environment, but also crucial for breakthroughs and innovation in this field. However, with governments increasingly using corporate and industrial espionage within the private sector to gain greater access to state secrets, counterintelligence services must evolve and develop strategies to mitigate against these newer challenges. It is therefore incumbent that governments and the private sector establish mechanisms for information-sharing, best practices, and geostrategic circumstances.

Finally, covert action comes into focus, particularly the means by which these offensive measures may be used by intelligence services to secure their own supply chains and undermine their adversaries'. Expanding upon the principle of 'strategic disruption', the potential role played by paramilitary actors in compromising competitors' supply chains by compromising logistics and access to resources is highlighted with a focus on two such actors- proxy militarised actors, such as insurgent groups, or state-affiliated special operations forces themselves. Finally, the role of offensive cyber in this field is explored, stressing the intertwined features of defence and offence for an effective cyber policy aimed at ensuring supply chain resilience against hostile threat actors.

If the bipolar world order of the Cold War came to be shaped beginning in the 1960s by the space race between the Soviet Union and the US, today's multipolar avatar is underpinned by interstate competition for technological advantage in AI, quantum computing, synthetic biology, among others. As nations vie for strategic advantage in these fields, national intelligence agencies—as custodians of a nation's strategic interest—must adapt to new realities, and work to secure the supply chains upholding this scientific advantage. The extent to which they do so is a determinant of a nation's technological prowess, and ultimately, its place in a changing world. 

**Archishman Goswami** is an MPhil International Relations student at the University of Oxford.



- 1 Procopius: The Roman Silk Industry, c. 550, ed. Paul Halsall, Fordham University, <https://sourcebooks.fordham.edu/source/550byzsilk.asp>
- 2 Jami Miscik, Peter Orszag, and Theodore Bunzel, “Geopolitics in the C-Suite”, *Foreign Affairs*, March 11, 2024, <https://www.foreignaffairs.com/united-states/geopolitics-c-suite>
- 3 Aafke Eppinga, “Secret ‘Beethoven’ mission: cabinet wants to keep ASML in NL”, *Innovation Origins*, March 6, 2024, <https://innovationorigins.com/en/secret-beethoven-mission-cabinet-wants-to-keep-asml-in-nl/>
- 4 John Mentzer et al., “Defining Supply Chain Management”, *Journal of Business Logistics*, Vol 22 No 2 (2001), pp 4
- 5 Niamh Kennedy and Anna Cooban, “Belgium’s security services are monitoring Alibaba for possible spying”, *CNN*, October 5, 2023, <https://edition.cnn.com/2023/10/05/business/alibaba-belgium-spying-accusations/index.html>
- 6 “Germany puts Russian scientist on trial for space tech espionage”, *Al Jazeera*, January 27, 2022, <https://www.aljazeera.com/news/2022/1/27/germany-puts-russian-scientist-on-trial-for-space-tech-espionage>
- 7 Oceania Cyber Security Research Centre, “Critical Technology Supply Chain Principles- Submission”, November 2020, Melbourne, <https://ocsc.com.au/wp-content/uploads/2021/12/Critical-Technology-Supply-Chain-Principles.pdf>
- 8 Suhas AR, Joel Martin, and Niti Jhunjhunwala, “Semiconductors—the next frontier of geopolitics”, *HFS Research*, March 22, 2024, <https://www.hfsresearch.com/research/semiconductor-supply-chain-diversification/>
- 9 Littlefish, “Backdoor Vulnerability- What you need to know about supply chain attacks,” <https://www.littlefish.co.uk/insights/backdoor-vulnerability-supply-chain-attacks/>
- 10 Rajeswari Rajagopalan, “Critical Technologies Supply Chains”, *Observer Research Foundation*, December 23, 2023, <https://www.orfonline.org/research/critical-technologies-supply-chains>
- 11 Richard Byrne, “Panopticons and Chokepoints”, *The Wilson Quarterly*, Spring 2020, <https://www.wilsonquarterly.com/quarterly/who-writes-the-rules/panopticons-and-chokepoints>
- 12 “Semiconductor Devices in India”, *Observatory of Economic Complexity*, <https://oec.world/en/profile/bilateral-product/semiconductor-devices/reporter/ind>
- 13 “China, Hong Kong account for 56 pc of India ‘s total imports of electronics, telecom, electrical products: GTRI”, *The Economic Times*, May 2, 2024, <https://economictimes.indiatimes.com/news/economy/foreign-trade/china-hong-kong-account-for-56-pc-of-india-s-total-imports-of-electronics-telecom-electrical-products-gtri/articleshow/109787013.cms?from=mdr>

- 14 Niels Graham and Mondrita Rashid, “Is ‘friendshoring’ really working?”, *Atlantic Council*, July 23, 2023, <https://www.atlanticcouncil.org/blogs/new-atlanticist/is-friendshoring-really-working/>
- 15 Gary Drenik, “Why Nearshoring Is Closer Than Ever: How Mexico Is Becoming The Next Big Thing In Global Markets”, *Forbes*, March 23, 2023, <https://www.forbes.com/sites/garydrenik/2023/03/23/why-nearshoring-is-closer-than-ever-how-mexico-is-becoming-the-next-big-thing-in-global-markets/>
- 16 Emma Ashford and Evan Cooper, “Yes, The World is Multipolar”, *Foreign Policy*, October 5, 2023, <https://archive.ph/GmxnT>
- 17 Dashveenjit Kaur, “Chip 4 Alliance: Senior officials finally meet to discuss semiconductor supply chain”, *Techwire Asia*, February 28, 2023, <https://techwireasia.com/2023/02/chip-4-alliance-the-first-meeting-of-senior-officials-finally-transpired/>
- 18 Eric Jung, “The “Chip 4 Alliance” and Taiwan–South Korea Relations”, *Global Taiwan Institute*, September 20, 2023, <https://globaltaiwan.org/2023/09/the-chip-4-alliance-and-taiwansouth-korea-relations/>
- 19 Carnegie India, “India-U.S. Emerging Technologies Working Group,” <https://carnegieendowment.org/india/india-us-emerging-technologies-working-group?lang=en>
- 20 Samir Saran et al., “Two Decades of the Quad: Diplomacy and Cooperation in the Indo-Pacific”, *Observer Research Foundation*, June 14, 2024, <https://www.orfonline.org/research/two-decades-of-the-quad-diplomacy-and-cooperation-in-the-indo-pacific>
- 21 Jimmy Goodrich, “China’s Evolving Semiconductor Strategy”, *IGCC*, May 29, 2024, <https://ucigcc.org/blog/chinas-evolving-semiconductor-strategy/>
- 22 Semiconductor Devices in Bangladesh, *Observatory of Economic Complexity*, <https://oec.world/en/profile/bilateral-product/semiconductor-devices/reporter/bgd>
- 23 Miquel Vila Moreno, “The Association of Southeast Asian Nation’s Semiconductor Sector in a World of Bifurcated Supply Chains”, *Orion Policy Institute*, July 19, 2024, <https://www.orionpolicy.org/orionforum/288/the-association-of-southeast-asian-nation-s-semiconductor-sector-in-a-world-of-b>
- 24 James Woolsey, “Why We Spy on Our Allies”, *Wall Street Journal*, March 17, 2000, <https://www.wsj.com/articles/SB95326824311657269>
- 25 MI5, “Klaus Fuchs,” <https://www.mi5.gov.uk/history/the-cold-war/klaus-fuchs>
- 26 Spyscape, “The Cambridge Spy Scandal That Haunts Britain,” <https://spyscape.com/article/the-cambridge-spy-scandal-that-haunts-britain>
- 27 John Henley, “Denmark helped US spy on Angela Merkel and European allies – report”, *The Guardian*, May 31, 2021, <https://www.theguardian.com/world/2021/may/31/denmark-helped-us-spy-on-angela-merkel-and-european-allies-report>

- 28 Chad de Guzman, “Leaked Pentagon Documents Appear to Show U.S. Spying on Ally South Korea”, *Time*, April 10, 2023, <https://time.com/6269905/us-pentagon-leaked-documents-south-korea/>
- 29 Itai Shapira, “The Unique Challenge of Assessing Partners and Allies”, *RUSI*, April 27, 2022, <https://rusi.org/explore-our-research/publications/commentary/unique-challenge-assessing-partners-and-allies>
- 30 Samantha Schwartz, “Careless employees behind the majority of insider threat incidents: report”, *Cybersecurity Dive*, January 25, 2022, <https://www.cybersecuritydive.com/news/insider-threat-malicious-negligent-employee/617656/>
- 31 Mimecast, “Insider Threat” <https://www.mimecast.com/content/insider-threat/>
- 32 Becky Bracken, “Fired Healthcare Exec Stalls Critical PPE Shipment for Months”, *Threatpost*, January 7, 2021, <https://threatpost.com/healthcare-exec-stalls-critical-ppe-shipment/162855/>
- 33 Carly Page, “Tesla says data breach impacting 75,000 employees was an insider job”, *TechCrunch*, August 21, 2023, <https://techcrunch.com/2023/08/21/tesla-breach-employee-insider/>
- 34 Patrick Tucker, “Google DeepMind Researchers Join Pledge Not to Work in Lethal AI”, *DefenceOne*, July 18, 2018, <https://www.defenseone.com/technology/2018/07/google-deepmind-researchers-pledge-lethal-ai/149819/>
- 35 Brazen, “Spy Valley: An Engineer’s Nuclear Betrayal” (podcast, Spotify, 2023), <https://open.spotify.com/show/2DUz7SWBE44AdgFytwNCNZ?si=adb0d239ee544bfa>
- 36 “US court sentences Chinese spy to 20 years for stealing trade secrets”, *The Guardian*, November 16, 2022, <https://www.theguardian.com/us-news/2022/nov/16/us-court-sentences-chinese-spy-for-stealing-trade-secrets>
- 37 GE Aerospace, “Talkin’ ‘bout next gen: GE Aviation awarded \$1B contract for future military propulsion”, *GE Aerospace*, June 30, 2016, <https://www.geaerospace.com/news/articles/technology/talkin-bout-next-gen-ge-aviation-awarded-1b-contract-future-military-propulsion>
- 38 Kathryn Armstrong, “Ex-Google engineer charged with stealing AI secrets”, *BBC*, March 7, 2024, <https://www.bbc.com/news/world-us-canada-68497508>
- 39 Rahul Chhabra, “Innovation key to Viksit Bharat by 2047: Dharmendra Pradhan”, *The Sunday Guardian*, January 28, 2024, <https://sundayguardianlive.com/news/innovation-key-to-viksit-bharat-by-2047-dharmendra-pradhan>
- 40 Harichandran Arakali, “Budget 2024: FM Sitharaman announces large fund to support R&D, deep tech”, *Forbes India*, February 1, 2024, <https://www.forbesindia.com/article/news/budget-2024-fm-sitharaman-announces-large-fund-to-support-rd-deep-tech/91177/1>



- 41 Manufacturing Today, “Pixxel secures 350th iDEX contract to develop advanced miniaturised satellites for Indian Air Force”, June 29, 2024, <https://www.manufacturingtodayindia.com/pixxel-secures-350th-idex-contract-to-develop-advanced-miniaturised-satellites-for-indian-air-force/>
- 42 James Morales, “OpenAI Introduces New Position to Combat Insider Threats, Enhancing Collaboration with White House”, *CCN*, March 26, 2024, <https://www.ccn.com/news/technology/openai-hiring-insider-risk-investigator-collaborating-white-house/>
- 43 MI5, “New body will help the UK combat national security threats”, March 13, 2023, <https://www.mi5.gov.uk/news/new-body-will-help-the-uk-combat-national-security-threats>
- 44 National Protective Security Authority, “Insider Risk: What it is and why it matters”, January 4, 2024, <https://www.npsa.gov.uk/insider-risk>
- 45 The National Counterintelligence and Security Center, “Supply Chain Risk Management,” <https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats#content>
- 46 RAND Corporation, “Strategic Disruption by Special Operations Forces”, December 2023, Washington D.C., [https://www.rand.org/pubs/research\\_reports/RRA1794-1.html](https://www.rand.org/pubs/research_reports/RRA1794-1.html)
- 47 Perrine Mouterde, “Rare-earth mining in Myanmar: ‘An extreme example of widespread destruction’”, *Le Monde*, May 23, 2024, [https://www.lemonde.fr/en-environment/article/2024/05/23/rare-earth-mining-in-myanmar-an-extreme-example-of-widespread-destruction\\_6672433\\_114.html](https://www.lemonde.fr/en-environment/article/2024/05/23/rare-earth-mining-in-myanmar-an-extreme-example-of-widespread-destruction_6672433_114.html)
- 48 “Ukrainian Military Officer Accused of Attack on Nord Stream Gas Pipeline”, *Voice of America*, November 13, 2023, <https://www.voanews.com/a/ukrainian-military-officer-accused-of-attack-on-nord-stream-gas-pipeline/7352410.html>
- 49 Len Scott, “Secret Intelligence, Covert Action and Clandestine Diplomacy”, *Intelligence and National Security*, Vol 19 No 2 (2004), pp 331
- 50 Yuvraj Tyagi, “Analysing India’s Elite Special Forces under AFSOD: MARCOS, Garud, and Para SF in the line of duty”, *Republicworld*, December 10, 2023, <https://www.republicworld.com/defence/war-games/analyzing-india-s-elite-special-forces-under-afsod-marcos-garud-and-para-sf-in-the-line-of-duty>
- 51 Joseph Nye, “Power and national Security in Cyberspace”, in *America’s Cyber Future: Security and Prosperity in the Information Age* (Washington DC: Centre for a New American Security), pp 17, [https://www.files.ethz.ch/isn/129907/CNAS\\_Cyber\\_Volume%20II\\_2.pdf](https://www.files.ethz.ch/isn/129907/CNAS_Cyber_Volume%20II_2.pdf)
- 52 “Top 5 Supply Chain Cyber Risks”, *Avetta Blog*, <https://www.avetta.com/blog/top-5-supply-chain-cyber-risks>
- 53 Samit Shah, “The Financial Impact of SolarWinds Breach”, *BitSight*, January 12,

- 2021, <https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided>
- 54 Kate Kuehn, “The Lasting Effects of SolarWinds: The Winds that Never Stop Blowing”, *vArmour*, December 23, 2020, <https://www.varmour.com/blog/the-lasting-effects-of-solarwinds-the-winds-that-never-stop-blowing/>
- 55 Dina Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story Of The SolarWinds Hack”, *NPR*, April 16, 2021, <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>
- 56 Jessica Lyons, “Russia’s Cozy Bear dives into cloud environments with a new bag of tricks”, *The Register*, February 27, 2024, [https://www.theregister.com/2024/02/27/russia\\_cozy\\_bear\\_new\\_ttps/](https://www.theregister.com/2024/02/27/russia_cozy_bear_new_ttps/)
- 57 Govind Choudhary, “India conducts national cyber defence exercise to safeguard critical infrastructure amid escalating threats”, *Livemint*, May 28, 2023, <https://www.livemint.com/news/india-conducts-national-cyber-defence-exercise-to-safeguard-critical-infrastructure-amid-escalating-threats-11685248974907.html>
- 58 Shashank Shekhar, “India’s Digital Revolution Faces Growing Cyber Threats, Need Robust Mitigation Strategies: NTRO Chief Arun Sinha at c0c0n 2023”, *the420*, October 9, 2023, <https://www.the420.in/india-cybersecurity-threats-ntro-arun-sinha-warning-cocon-keral-police/>
- 59 Shailaja Neelakantan, “When NSA Ajit Doval outlined India’s new Pak strategy- defensive offence- perfectly”, *The Times of India*, October 4, 2016, <https://timesofindia.indiatimes.com/india/when-nsa-ajit-doval-outlined-indias-new-pakistan-strategy-defensive-offense-perfectly/articleshow/54670600.cms>

*Images used in this paper are from Getty Images/Busà Photography.*





**Ideas . Forums . Leadership . Impact**

20, Rouse Avenue Institutional Area,  
New Delhi - 110 002, INDIA  
Ph. : +91-11-35332000. Fax : +91-11-35332005  
E-mail: [contactus@orfonline.org](mailto:contactus@orfonline.org)  
Website: [www.orfonline.org](http://www.orfonline.org)