Exploring the Knowledge Nexus

India's Path in Terrorism-Driven Institutional Growth

Chris C. Demchak
Eric Werner

Introduction

The search for knowledge and certainty drives the evolution of large-scale institutions in modern societies.[1] These organizations, in turn, alter and solidify the structural and political landscape of society through their search for effectiveness by expanding or competing for control of their environments. In stable democracies, this accumulated organizational landscape evolves either to manage acceptably enough or to ignore society-wide problems. Occasionally, challenges—like terrorism—emerge that defy traditional processes to cause significant uncertainties for large organizations. To reestablish preferred certainty levels, organizations reach beyond established boundaries and procedures to acquire more knowledge or control.[2]

For established institutions, threats must be considered dire indeed to stimulate a search for new knowledge. If undertaken, the search beyond normal institutional boundaries moves them into the *knowledge nexus*—the information-sharing terrain between communities that may or may not be in use. Generally, sharing information is not seen as beneficial, or needed information is fragmented beyond recognition or visibility across agencies. As information societies continue to evolve, much needed information has simply never been collected officially. This leaves a largely un-

---

On the faculty of the University of Arizona's School of Public Administration and Policy, Dr. Chris C. Demchak received her PhD from Berkeley in political science with a focus on organizational theory and complex technical systems, as well as two master's degrees in economic development (Princeton) and energy engineering (Berkeley). She has published numerous articles on societal information warfare (theory of action, BIK behavior-based privacy), security institutions (counterterrorism "knowledge nexus"), and new military models ("Atrium" model for joint forces), as well as the book *Military Organizations, Complex Machines* in the Cornell Security Studies series.

Currently a graduate student in international affairs at American University, Eric Werner graduated from the University of Arizona in December 2006. An honors student in political science and Near Eastern studies and a recipient of the Department of Political Science's "Most Outstanding Student Award" as well as the University of Arizona's Murray DeArmond Mind, Body, and Spirit Award, he has participated in several research projects involving homeland security analysis, governance security, and responses to terrorism.

explored arena beyond normal institutional boundaries where potentially vital information may reside.

For security organizations the counterterrorism (CT) knowledge nexus has been largely vacant up to now. War, or an equivalent national-level threat, is usually necessary to motivate national-level institutions to share internal knowledge with each other or with their domestic colleagues. Military preparations for war have often involved reaching out to create new institutions and infrastructure just to reduce uncertainties in foreseeable conflicts.[3] Even in war and within the same military community, however, such developments are not easy or automatic. Battle histories resonate with stories of military units refusing to cooperate with others, especially if cooperation seems to confer advantages on competing services.[4] This impetus for turf protection is as true for police departments[5] and national agencies[6] as it is for militaries.[7]

Until 2001, domestic terrorism was not widely viewed as a national-level problem requiring military or national foreign intelligence assistance. Most Western nations characterized terrorism on homeland soil as a criminal activity and thus assigned responsibility for countering terrorism to domestic police services.[8] In recent decades, terrorism has waxed and waned in stressing police capabilities, only solidly becoming of national security concern in the United States after the attacks in 2001.[9] With little political pressure to do otherwise, national-level military and intelligence agencies did not seek to be involved, other than peripherally, in police matters. Similarly, insurgencies in Westernized nations have been rare as well and given to the military to handle.[10] States have not institutionally viewed threats from insurgencies as comparable to those posed by domestic terrorism. Police or intelligence agency involvement has generally occurred under temporary, ad hoc arrangements rather than being integrated to the extent necessary to begin forming a CT knowledge nexus.[11]

Since 2001, however, CT has unexpectedly developed the political potential to challenge established organizational boundary paradigms. Modern democracies have become intolerant of arbitrary or preventable death. Citizens have developed unprecedented expectations that public agencies will ensure their safety. These societies tend to be complex, interdependent, nonautarchic, dynamic, networked sociotechnical systems with members who are impatient with dangers perceived as avoidable. In particular, citizens increasingly have a strong sense of entitlement to be protected against the potential of an arbitrary mass casualty attack.[12]

Especially after the 2001 New York attack, the US government and global Westernized media vigorously and internationally framed foreigner-instigated domestic terrorism as a major national and domestic threat aimed at Westernized democracies. As a result of this framing, it has become widely accepted that the institutional solution requires relatively holistic cooperation across traditionally separate domains of national security services.[13]

Under political pressure to be seen as prepared and to obtain or retain international status with peer professional groups, police, military, and intelligence agencies across Western nations are now, at a minimum, discussing information acquisition, sharing, analysis, and distribution. This new "not quite national security but more than routine criminality" framing of terrorism challenges established operational distinctions between levels of police, domestic intelligence, and military contributions to homeland defense, eroding institutional boundaries across Westernized liberal democracies.[14] In the process, these widely scattered efforts are beginning to fill the void with organizational and technical elements aimed at sharing information.

Such fervor in peacetime is highly unusual, and the process has gone largely unnoticed and uncharted externally. Consequently, we know very little about how the institutionalization of this knowledge nexus proceeds. Institutionalization of the CT knowledge nexus can provide enormous benefits, but a need for information and certainty among institutions often links them into large-scale technical systems (LTS) with unintended consequences.[15] For example, in nations not yet experiencing terrorism, large institutions may simply have monthly meetings. Others, such as the United States, may create new organizations such as the Department of Homeland Security (DHS).

Effective CT in liberal democracies with strong civil control of security forces is taken to require public actions that are preemptive, rapid, and accurate. Inevitably, such actions involve the necessary and deliberate interruption of social activities and, potentially, the compromise of civil liberties for security purposes. Whatever those actions are, public law and expectations across democracies require that knowledge-driven operations be—or at least appear to be—narrowly targeted and popularly viewed as unbiased and legitimate. These exceptional demands on civil, intelligence, and military structures require extra care to understand the circumstances under which the knowledge nexus forms and the longer term nature and directions of its emergent structures.

This study is a first step in a longer range, wider focused, cross-national research agenda on the extent to which the search for knowledge across civilian, intelligence, and military counterterrorism organizations may be developing an unprecedented CT knowledge nexus. Using a grounded theory approach across a large number of media and other secondary sources, this essay documents the institutional beginnings of a CT-induced knowledge nexus in a natural experiment occurring in the large-scale federal democracy of India. It is a nation dealing with a considerable terrorism challenge and security institutions with exceptionally strong traditions of defending domain boundaries. The evidence accumulated from an exhaustive search of published reports suggests that redefining terrorism as a national problem has indeed weakened turf boundaries across these traditionally insular security communities in India.

To our surprise, however, the institutional kernel of this nexus did not emerge from the higher status national-level agencies in the military or intelligence communities, but rather from the more pedestrian state police forces. To an unexpected extent, the national-level communities—intelligence and military—have concretely supported the growth of state-level antiterrorism squads (ATS), even when the actual experience with terrorism is on the decline. We hypothesize that in India, prompted first by experience and then by internationally reinforced urgency, these ATSs have begun institutionalizing the CT knowledge nexus. In 2001, with institutionalization well underway, numbers of terrorism incidents began to decline across India, but the number of ATSs continued to increase for the next four years. The CT knowledge nexus is changing the topology of the Indian state by forging relatively resilient links across the organizational boundaries of local and national levels.

The idea of using small, formally organized squads of military or police forces to disrupt enemy organizations first emerged in Europe long before its arrival in India. In 1941, the United Kingdom created the Special Air Service (SAS) with the objective of going behind enemy lines to attack German troops and infrastructure in Africa. In the 1950s, the SAS was transformed from a special forces unit to a counterinsurgency (COIN) institution protecting British interests around the world. With this change in mission emphasis from conventional state military threats to those from nonstate organizations, the concept of an *antiterrorism squad* was born. The SAS ran COIN operations in Oman, Malaysia, Borneo, and Aden.[16]

In the 1970s, the experience of terrorism as more than a criminal or crazed activity prompted the creation of specialized response institutions and the evolution of others across several nations. The Israeli deep reconnaissance and intelligence teams of Sayeret Matkal were created in 1957 but evolved into counterterrorism in the 1970s based on the model of the British SAS. After the 1972 Munich massacre of Israeli Olympic athletes, the surprised and poorly prepared German police formally created GSG-9, Germany's first antiterrorism squad.[17] It drew conceptually on the examples of the British SAS and Israeli Sayeret Matkal.[18] Having a team specialized in CT became more internationally desirable after the 1976 successful Israeli Operation Thunderbolt that rescued 106 passengers at the Entebbe International Airport in Uganda.[19] During the 1970s, Belgium, Italy, Australia, and the United States established ATSs in military units.[20]

As an institutional adaptation to surprise in large-scale systems, the ATS evolutionary development in India falls upon a midpoint of a formalized CT knowledge nexus continuum marked by announcements of more or new joint discussions, exercises, or regularized briefings on the low end and full-scale, formal creation of new organizational structures across cities, states, and national agencies on the high end. As such, the Indian experience may provide more nuanced lessons about structuring responses to CT knowledge requirements under differing circumstances of frequency and consequence than the example of, say, the DHS in the United States. Thus, this work seeks to uncover the large-scale technical structures emerging in a wide variety of national contexts. The need for terrorism-related knowledge is beginning to ripple through government cyber operations with unknown consequences for institutional effectiveness, civil liberties, and civil-military relations.

Defining the Knowledge Nexus

A knowledge nexus evolves when organizational walls are breached to facilitate mutually beneficial information sharing among institutions. The definition of *knowledge* here is broad; it encompasses anything that reduces the unknowns associated with a contingency and that helps the recipient counter an uncertainty. Knowledge can be found in a spare part, a supplemental external training course, access to new databases, or seconded experts.[21] The emergence of knowledge societies has led to an increasing emphasis on cyber methods of knowledge formation, stor-

age, transmission, and retrieval. However, unless organizations perceive a need to augment existing knowledge by developing external knowledge delivery networks, the nexus between institutions remains essentially unclaimed domain space. In principle, a nexus should only begin to take shape when an identifiable large-scale problem emerges and is widely recognized to impose knowledge demands beyond the existing capabilities of any single institution. To meet individual obligations, each institution will have to reach beyond its own strongly maintained boundaries to link with the other organizations in some process of knowledge exchange. Figure 1 models this process of institutional development.

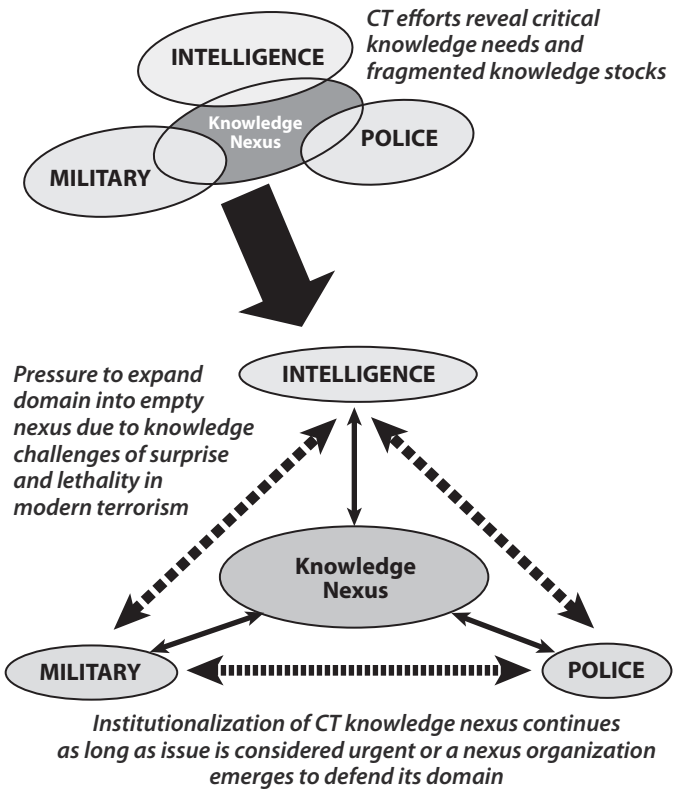

Figure 1. Knowledge nexus model of interinstitutional domain formalization. (Adapted from Chris C. Demchak and Eric Werner, "'Knowledge Nexus': Learning Security in the Information and Terrorism Age" (paper presentation, International Security Studies Section annual meeting, International Security Association, Tucson, AZ, 26–28 October 2006).

As data exchanges intensify and become more frequent over time, institutions change structures, dependency perceptions, and relationships. In the commercial world, it has been said that two large organizations

cannot sustain a joint venture unless everything is perceived to be shared evenly. If not, then one will absorb the other, or either the shared subsidiary or the joint venture will disband.[22] In public institutions, however, the process is more gradual, with a slow formalization of routine interactions. One result may be an enlargement of one organization to absorb the resources associated with the problem—just as in the commercial world. A second consequence could be disengagement if the originating problem is resolved or decreases in importance. A third possibility is the development of a slowly institutionalizing shadow organization sustained by the shared practices and knowledge moving between two otherwise distinct agencies. This not-quite-formally-recognized knowledge nexus could function for years as organization members maintain personal and professional relationships even after the original problem dissipates. The knowledge nexus could conceivably become the source of entirely new institutions formed from the parent organizations by political leaders. A fourth possibility is the complete joining of the two organizations with the shadow organization serving as the intervening glue for the merger.

The knowledge nexus varies in its level of institutionalization according to the level of criticality by which the stimulating problem is socially constructed. War or its imminence is particularly powerful in forcing interconnections across organizations and communities. Historically the pursuit of war by political leaders has developed the institutions of the society. France under Louis XIV and Napoléon could be viewed as classic examples of the massive development of society's infrastructure and institutions as a function of the need during war for resources and logistics transcending the traditional bounds of the military's internal capabilities.[23] Figure 2 depicts the progression of institutionalization levels of the knowledge nexus. Furthermore, the more intrusive the threat and the more long-standing the uncertainty, the more likely the formerly temporary arrangements across organizations will formalize and remain over time.[24]

Given the uniqueness of this issue for increasingly complex societies, it is unclear how institutionalization of the knowledge nexus might develop in any nation's CT effort, but the process is open for informed speculation and empirical discovery. When CT is taken so seriously that the turf walls around institutional data begin to buckle, the organizational and wider nexus development clearly become of interest to scholars and practitioners.[25] Over time, as Philip Selznick observed, if informal information-sharing relations become accepted, they begin to become part of the formal structures among those elements involved.[26]

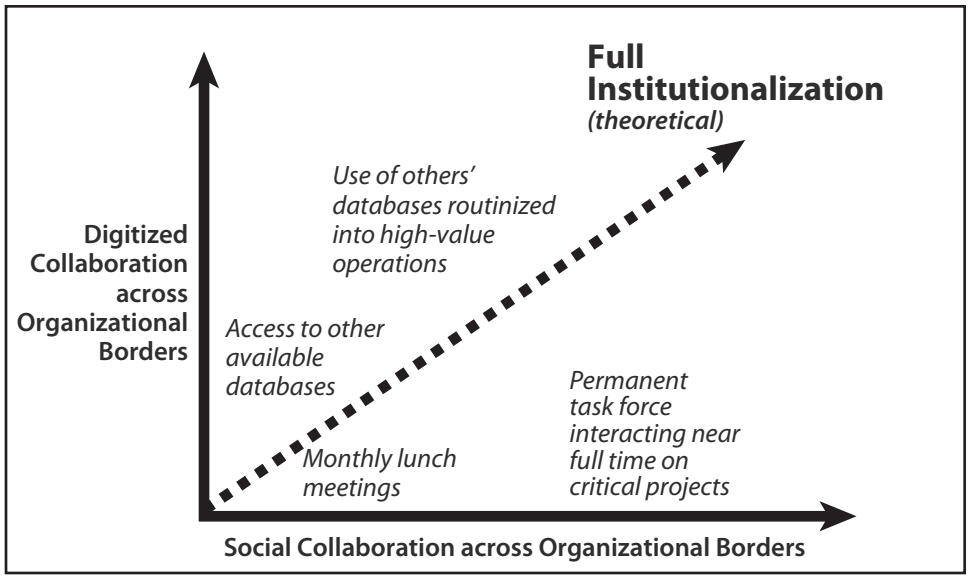

Figure 2. Range of social and digital institutionalization in the nexus. (Adapted from Demchak and Werner, "'Knowledge Nexus.'")

The more compelling the fear of terrorism, the more one expects to find institutions mobilizing to find certainty-enhancing knowledge for future safety. This, in turn, formalizes reliance on the knowledge nexus. It is, however, critical to this larger societal process that terrorist events be framed as possibly recurring and national in implication for the nexus to coalesce into a large-scale cyber system with society-wide effects.

There is plenty of international discourse—some quite emotional—about the imminent threat of foreign-based terrorism since 2001. That year was really only a watershed for the United States, and yet the Bush administration's framing of the "global war on terror" seems to have imprinted security discourses far beyond the US experience. Therefore, if a state shows either trivial terrorist experience or declining experience, and yet increases its institutionalization of a CT knowledge nexus, we infer that urgency has supplanted experience as a motivator for such development. The decline of concrete events suggests the US characterization of the global terrorist threat has resonated with a wide range of nations—even when those nations have not experienced a comparable threat from terrorism and yet are institutionalizing a knowledge nexus between police, military, and intelligence organizations. That police forces in particular—traditionally strongly locally focused—might respond to an international message of urgency underscores the potential power of the post-9/11 framing of CT and of the

unprecedented growth of communications infrastructure linking nations.[27] The process of emulating other professional developments is historically not common in most public service domains, especially across national borders. Most public agencies do not look to their colleagues in other nations, or even other provinces and states, for guidance on how to structure or operate themselves. This process, formally called *mimetic isomorphism*, is particularly unlikely when organizations have few competitive or policy connections already in place.[28] Such copying is more common in militaries, which often seek to mirror each other in hopes of averting operational or technological surprise.[29] The convergence of ideas leading to institutional change can also be normative in the sense that it becomes associated with minimum standards for acceptance into professional ranks.[30]

In testing these hypotheses quantitatively and qualitatively, we relied on evidence in public media along the continuum of interaction events. Public announcements, especially in the wake of terrorist events, constituted the bulk of our data under the presumption that formalization heading towards a true CT knowledge nexus could not be held in secret across three large institutions. In short, so many actors would be involved that the normal way large organizations communicate—by public actions—would inevitably be used in the process.

In 2003, the United States moved toward the end of the continuum in knowledge nexus institutionalization with the creation of the new DHS. However effective it may prove, this response was exceptionally rapid, occurring within two years of the watershed event. The "new agency" response, however, is consistent with the historical effects of divided governance on US public agencies. Congressional partisan disagreements have often led to creation of new independent agencies rather than the overhaul of existing agencies.[31] The US case is also distinct in scope because of the creation of an enormous agency consisting of 180,000 members. The establishment of this massive new agency involved the direct transfer of nearly 20 organizational elements from other agencies to the new department. Elements deemed related to CT were simply coerced, including several politically weak, formerly relatively independent, and culturally distinct agencies such as the US Coast Guard.[32] Long-established organizational boundaries were unusually disregarded in this process, indicating extraordinary perceptions of urgency among political leaders despite the lack of direct long-term experience with terrorism.[33] In this work, the US counterterrorism knowledge nexus example is taken as a defining end of spectrum, unlikely to be the pattern of institutionalization in other democracies but informing in its efforts

to force knowledge sharing from the top down, onto and across distinct domains of the three security communities.

India as a Compelling Natural Experiment

A more likely pattern in CT knowledge nexus development is occurring in India. This large Westernized and federal democracy provides an exceptional natural experiment. Several advanced democracies such as the United Kingdom, Spain, and Israel have confronted international and domestic terrorism for years.[34] Only India's circumstances, however, pit exceptional experience with terrorism and a national bureaucratic culture recognized to be extraordinarily rigid and hierarchical.[35] It is a large, fractious democracy relying on extensive, independent, highly bureaucratized agencies with a history of very strong turf distinctions and a generalist, patriarchal civil service zealously guarding power distinctions in their organizations.[36]

In India, strongly stovepiped and defensive security agencies pose particularly tough obstacles to forming an interinstitutional knowledge nexus of any sort.[37] Like most Westernized states, the Indian military, police, and intelligence agencies have entrenched and organizationally distinct cultures, policy preferences, legal status, domains, tools, competencies, and knowledge filters.[38] Similar to many nations, Indian security institutions do not seek to interact routinely. Even after crises that require cooperation, they usually minimize innovations or adaptations that would force continuing interorganizational boundary crossing.[39] Indian bureaucratic path dependence combines the complexities of the structures of British colonial administration with those of the underlying native Indian caste and ethnic divisions.[40] Information sharing faces some of the greatest bureaucratic challenges under these circumstances.[41]

Finally, long before the United States had its major attack, Indian forces were frequently experiencing terrorist incidents across states. Over the past 20 years, experience with homegrown terrorism across India ballooned, and with it, the interest of state police organizations in a visible response. As of 2006, the South Asia Terrorism (Web) Portal listed approximately 179 religious, ideological, and ethno-nationalist groups operating across India. Larger states like Manipur face 39 active terrorist groups, while even tiny Nagaland deals with at least three active organizations. Through 2001, the average civilian and security forces' casualty result was the equivalent of one 9/11 per year, or about 2,500 people. The number of annual incidents

is sometimes three times the death rate, leaving the police chasing duds, attempted bombings, and real events throughout the year.[42]

Thus, India provides a particularly rich case for discerning evidence of institutionalization at the CT knowledge nexus owing to the cross-agency, comprehensive information requirements of CT campaigns. We used secondary sources in as comprehensive a review as possible of 10 years of published news reports, committee findings, and academic analysis on terrorist events from 1996 to 2005. We also charted the public evidence of increased interagency integration along social and technical axes in India in response to terrorism. Our goal was to see if a CT knowledge nexus could develop in India in any externally discernible way. Given the Indian institutional circumstances, if a CT knowledge nexus appears to be emerging here, then CT may be fairly construed as an institutional concept that approaches the power of war to force bureaucratic adaptation.

Indian Security Bureaucracies and Information Sharing

With its independence in 1947, India inherited the large public institutions, organizational structures, and class-imbued culture of British colonial administration.[43] For a variety of reasons, including scale and heterogeneity, many of these hierarchical organizations remain essentially unchanged internally[44] with strong patriarchal control mechanisms sustained from the Nehru era to the present.[45] The roots of preferences for rigid social divisions lie in Indian history of hierarchies among humans, animals, and deities. Sustained to a large extent by Hindu views of humans as stratified by caste and prior life decisions, unabashed elitism allocates power in many spheres of social activity in India.[46] Most government agency managers come overwhelmingly from upper and rising middle castes.[47] The pervasive tendency to observe distinctions in position and strong risk avoidance of Indian management culture is consistent with this history.[48] Unsurprisingly, decisions made in Indian bureaucracies tend to rationalize and perpetuate long-standing institutional power distribution, access, and information relationships.[49]

In particular, the traditions encourage inaction. Independent decisions that operate outside of established procedures are bureaucratically dangerous, especially for decisions involving uncertain wider political ripple effects or whose known effects are strongly opposed by powerful external political forces. For

any given official, passing onerous and highly selective national exams is the prerequisite for lifelong employment, but beyond that gate, survival depends on having the right family, caste, and network of high-level contacts. Within federal and state bureaucracies, officials are frequently moved for trivial reasons. This churn has reinforced tendencies to avoid decisions that might cause an unhappy superior to suddenly move offending subordinates. Fewer than 50 percent of the federal bureaucrats stay in any given position for more than a year; most do not stay in place long enough to acquire specialized competence. The majority become corrupted as a consequence of developing defenses required to avoid the political costs of making decisions that powerful outside stakeholders may view unfavorably.[50]

The number of civil service jobs and legislative positions reserved for "untouchables"[51] and women complicates the social conventions separating castes and gender. Male members of the elite caste resent these equalizing rules, thus increasing the disinclination to respond positively to interaction requests within and across agencies. Positive discrimination in reserved positions has indeed recruited some of the most advanced members into the circle of the Indian elite. But it has also tended to help restrict cooperation to even smaller groups of friends among caste or ethnically homogeneous bureaucrats rather than encouraging synergy among a heterogeneous pool of government personnel. The normal rule-driven rigidity of the enormous civil service has been made even more sluggish for otherwise desirable purposes.[52] The resulting ossification of internal procedures, in turn, further encourages the widespread use of "speed money"—bribes to ensure that some official action actually occurs.[53] Senior officials are disillusioned with the political system and their positions in it to a greater extent than are junior bureaucrats; however, they also tend to regard corruption and its inefficiencies as inevitable.[54]

These distortions in willingness of public agencies to cooperate internally extend throughout all levels of federal and state government.[55] Parliament and reformers have made little headway despite many commissions and efforts to reform the densely turf-bound structures.[56] Changes to the standard operating legal codes nominally governing official practices are often simply ignored.[57] Recently, the Indian Supreme Court ruled that officials were to be left in place at least two years in what was widely seen as an anticorruption ruling.[58] This ruling was based upon recommendations first made in 1977; its chances of implementation are extremely unclear.[59] In Indian security organizations, the

major players have distinctive histories in their establishment and evolution; the resulting insularity is remarkably resilient.[60]

CT information-sharing efforts in India face a daunting task in this massively fragmented, well-entrenched bureaucracy. In principle, the authorization for routine or in-depth interagency information sharing and acquisition will have to move upward through a number of higher levels of management before reaching a final decision-making authority.[61] Normally, the highest-level managers make most of the decisions; procedures that force empowerment onto lower organizational levels are considered uncomfortable at best.[62] While some sectors of the bureaucracy require and eventually obtain information from other sectors, role and procedural expectations, low competency levels among constantly rotated officials, and the deeply ingrained suspicions borne of class, gender, or ethnic distinctions prolong the process.

The Military in the Nexus

The Indian Army is first and foremost a direct descendent of the colonial administrative structures of the British Empire expressed in the British army up to World War II. As the oldest and most prestigious armed force in the nation, the Indian Army has retained a distinctively nineteenth-century British underpinning to its structures and enduring procedures. Serving under the Ministry of Defence (MOD), the army's million-odd soldiers are spread across six operational commands, or field armies. The organization controls the regular army, army reserve, homeland defense Territorial Army, and National Cadet Corps (aka ROTC).[63]

In recent years, the army's focus has widened from engaging in high-intensity conflict to include low-intensity, internal security operations. Since independence, the Indian military has fought in three major wars, one minor conflict with Pakistan, and one border war with China. In the 1990s, however, in addition to its responsibility for external threats, the army began COIN operations against Sikh separatists in the state of Punjab. With the consent of the MOD, the army established new—or reoriented existing—paramilitary units for duties in Kashmir, Assam, and the northeast states. Today, the Indian Army's counterinsurgency-trained units such as the National Security Guards (NSG) are also expected to mount CT operations. Other services have specialized units or tools applicable to CT, but the army is considered the lead service for this mission.[64]

Beginning in the late 1980s, military interaction with police units began to expand as COIN operations began to overlap the internal security obligations of local police forces.[65] Paramilitary forces now serve across military and police domains; however, they generally perform as military auxiliaries to the police to minimize army involvement in domestic law enforcement.[66] For example, the MOD established the 35,000-strong Rashtriya Rifles in the 1990s for COIN-acquired internal security duties in areas considered relatively pacified over the course of the decade.[67] The Assam Rifles, similarly, were initially formed by the British in 1917 to battle insurgency in the northeast but have evolved to participate in internal security operations in the northwest areas of Jammu and Kashmir.[68] Created under the military, these paramilitaries are legally under the broader jurisdiction and strategic control of the Home Ministry, along with clearly domestic security units such as the Home Guard, Border Security Force, Indo-Tibetan Border Police, Central Reserve Police Force, Special Security Bureau, Central Industrial Security Force, Civil Defence, Railway Protection Force, State Armed Police, and Defence Security Corps. However, since the MOD retains operational control of these forces, they are not considered, and do not consider themselves to be, police assets.[69]

According to published accounts, interactions by the military with the national-level Indian intelligence services are limited to routine and high-level refined intelligence reports; dynamic, in-depth cooperation is rare at best. Since 1947, military intelligence organizations have been given the lead in intelligence collection in border areas.[70] In 2002, under considerable opposition by both national-level intelligence agencies and the services, the Indian Defense Intelligence Agency (IDIA) was created to integrate the separate and insular intelligence networks of the army, navy, and air force into a single organization similar to that of the US Defense Intelligence Agency. Designed to coordinate and share information across the military services and with the federal intelligence agencies, the largely civilian IDIA tracks troop movements in neighboring countries, monitors terrorist groups, and assesses internal security threats.[71]

Like other Indian bureaucracies, the military is noted for its lack of timeliness, accuracy, or comprehensiveness in exchanging internal information—even in conflict situations.[72] The same applies to its ability to provide intelligence to or obtain it from external institutions, notably among the national intelligence agencies.[73] Any given military unit's ac-

cess to external intelligence data depends on a network of personalities in power, the urgency of events, and the character of the knowledge needed. Among military services, turf battles have long been considered debilitating and, until recently, accepted as endemic.[74]

Indeed, information sharing across the Indian military or with the national-level intelligence services has not seemed to improve despite the recognition of a need for integrated knowledge in COIN or CT. The IDIA fell afoul of the bitter interservice and international agency rivalry over control of knowledge assets. Up to the late 1990s, intelligence cooperation between border COIN forces and the Research and Analysis Wing (RAW) in particular was infrequent at best. In spring of 1999, a surprised Indian Army found Pakistani paramilitary forces in place across the Kashmiri line of control between India and Pakistan; they had infiltrated earlier than security forces' estimates anticipated. The resulting conflict at the Kargil Pass reinstated the status quo. This time, however, the usual post-conflict struggle to assign blame for the intelligence failure concentrated attention on integrating military and national intelligence capabilities—the result was the IDIA. The military, citing risk to internal efficiencies, has subsequently proven reluctant to share information. Integrated staffs within each military branch have administratively undermined the transfer of existing operations to IDIA divisions or subordinate organizations.[75] The military's refusal to share knowledge with the IDIA replicates enduring turf battles and has, thus far, channeled IDIA and its liaisons between different agencies into accepting the service's traditional, archaic, and inefficient system of reporting and analysis.[76]

At higher levels of civilian agencies, such as the Intelligence Bureau (IB) and the RAW, officials tend to view the IDIA as a competing intelligence agency.[77] At lower levels, the IB and RAW, with the IDIA in attendance, will occasionally conduct joint meetings with coordinated analysis for use by army commanders in areas governed by the Armed Forces Special Powers Act.[78] These field meetings are designed to encourage interaction among field personnel of all the organizations, but they are not technical and are too uncommon to be considered evidence of institutionalization.[79] There is little data so far to indicate that the establishment of the IDIA is altering either the basic landscape of information sharing between agencies or the distorting effects of loyalty to specific service branches. Figure 3 presents the military institutions associated with the development of the CT nexus in detail.

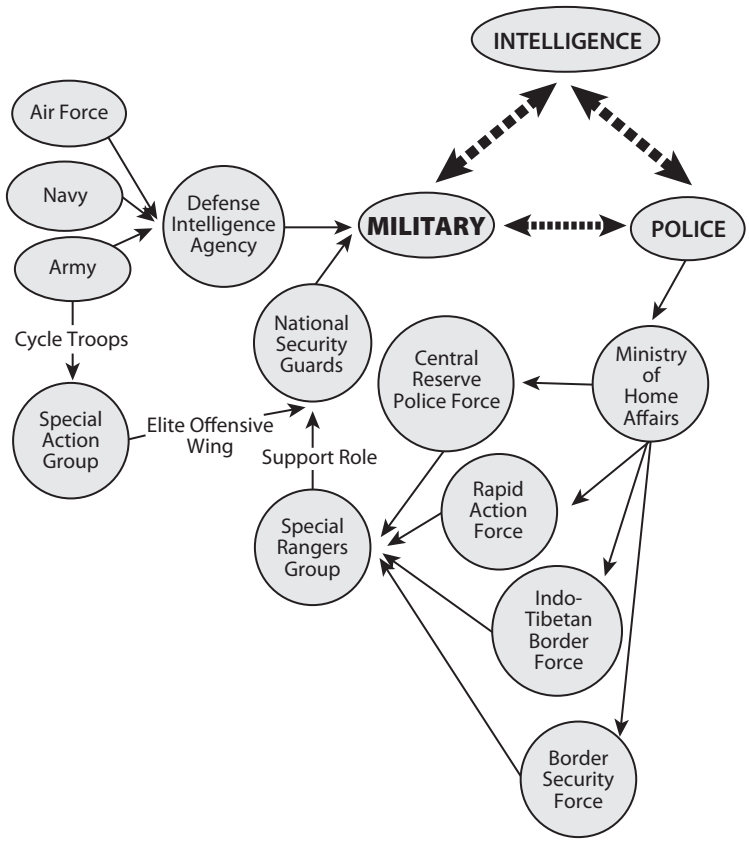

Figure 3. Military organizations in the Indian CT knowledge nexus. (Adapted from Demchak and Werner, " 'Knowledge Nexus.' ")

Intelligence Institutions in the Nexus

The two main agencies that constitute India's national-level intelligence community are younger and more prestigious than either the army or the police services. Established in 1920, the IB is subordinate to the Ministry of Home Affairs, with responsibility for domestic counterintelligence and CT. The RAW was established in 1968 as a subordinate component of the Ministry of External Affairs. It provides direct intelligence on foreign security threats to the prime minister's cabinet. Since these organizations are not subject to public oversight, little is publicly confirmed about their internal operations.[80] There are several smaller, less prominent agencies with intelligence responsibilities, but these generally support the larger bureaucracies.[81] The IB director portfolio expanded to include intelligence collection in border areas and to some other external intelligence

responsibilities after the first Indo-Pakistani War of 1947–49. Recently, the IB's influence in national security decisions rose dramatically with the growing recognition of the importance of accurate and timely intelligence collection in border states and beyond.[82]

The RAW emerged in the early 1970s from the remnant of the Indian Air Force's small aerial reconnaissance center as a wing to a larger IB. The RAW subsequently became a separate agency when its founder, Rameshwar Nath Kao, persuaded Prime Minister Indira Gandhi to designate the head of the organization as a secretary in 1976. Elevating the organization to the prime minister's cabinet greatly increased its influence on domestic and foreign policies, given its nominal equivalence in power and status with the other secretaries of the Indian government. This bureaucratic positioning engenders resentment on the part of IB managers because the IB head remains a director, rather than having status equal to his cabinet-level RAW counterpart.[83]

The RAW has become India's most powerful intelligence organization among the three referent national (military, domestic, and foreign) intelligence agencies.[84] The organization has expanded beyond its original external intelligence mandate to become a powerful stakeholder in domestic policies as well.[85] Technically, under the jurisdiction of the Ministry of External Affairs, the RAW sits at the behest of the prime minister's cabinet and is said to conduct propaganda and disinformation campaigns, espionage, sabotage, and intelligence gathering in neighboring countries—particularly in Pakistan.[86]

The two agencies overlap structurally only as members of the Joint Intelligence Committee, a component of the National Security Council.[87] However, the increasingly more politically salient issue of foreign-based, locally conducted terrorism constitutes a natural and contentious domain overlap between the two agencies. The two agencies also cooperate on an ad hoc basis with the military in COIN operations.[88]

As Indian bureaucracies evolved with the right to much greater secrecy in operations, the Indian intelligence services reinforced interorganizational insistence on turf boundaries. As evidence of this insularity and blunt arrogance, for the first time in its history the RAW responded to a nonofficial request for information in early 2007 but only with a solemn reminder to the public that it was not obliged to comply with any "Right to Information" laws.[89] Standard external authority controls on insular bureaucracies have seemingly been applied with limited effect. For example, while not

uncommon, the appointment of outsiders to senior leadership positions in both the IB and RAW causes debilitating resentment and internal withdrawal of cooperation. The recent appointment of a retired former senior IB counterintelligence official to head the bureau was discussed publicly as a positive step to get the agency's senior managers on board with new operations.[90] Animosity within an organization can slow the process of swapping information across agencies. Avoiding paralyzing internal or cross-boundary turf battles often means appealing to the highest levels of government and of each agency to obtain and to integrate data; normally this struggle requires considerable political interest and policy benefits to be at stake.[91] The top-down imposition of integrating organizations has not worked well. Particularly after 9/11, the public and political concerns with intelligence failure that lingered from the 1999 Kargil conflict rekindled efforts to reform the Indian intelligence agencies' widely known reputation for insularity. The IB, in particular, was blamed for the lack of domestic cooperation producing actionable intelligence for internal security. In 2000, the central government appointed a senior-level task force headed by former RAW chief Girish Chandra Saxena to investigate and propose necessary reforms to intelligence agencies. The confidential report focused on organizational structures, interactions, and staffing, forcing two new wings onto the IB by late 2001: the Multi-Agency Centre and the Joint Task Force on Intelligence.[92] In the next year, the military would be forced to accept the IDIA as a new institution as well. Despite the intent of these integrating solutions and a common CT obligation, each of the three—the IDIA, RAW, and IB—has its own internally developed strategies to defend. Improvements in interagency coordination on joint counterterrorist plans at the national level have not been apparent.[93]

Leaving aside the political power of agency self-interest, India's political leaders are fundamentally conflicted in their support for integrating these insular organizations. Occasionally, the political parties use the intense competition between agencies as a way to control each otherwise imperial bureaucracy. Despite the formal sanctions on agency violations of all of India's standard bureaucratic procedures, both parliament and the central government's senior officials have limited direct influence on these agencies in the face of the life tenure of intelligence officials. They also face a legally supported lack of openness to public inquiry inherited from the British. Using the disputes between agencies adds some leverage to an otherwise limited toolkit for civil control of operations and policy

implementation.[94] Furthermore, incidents of terrorism have not changed the situation because many senior politicians continue to regard terrorism solely as a law and order problem that does not require greater attention across cooperating and proactive intelligence agencies.

On the bright side, information not considered critical to bureaucratic battles is usually shared on the systemic level in some fashion, though it may not be timely or comprehensive.[95] Exchanges meant to be more substantive, entailing specialized expertise, usually involve midlevel-to-midlevel emissaries rather than the wholesale provision of databases in paper or of access to digital holdings. On an ad hoc basis, both agencies send midlevel officers to meet with military commanders for specific COIN operations, usually in the northwest or northeast section of the country.[96] Figure 4 presents the intelligence agencies participating in the Indian CT knowledge nexus development.

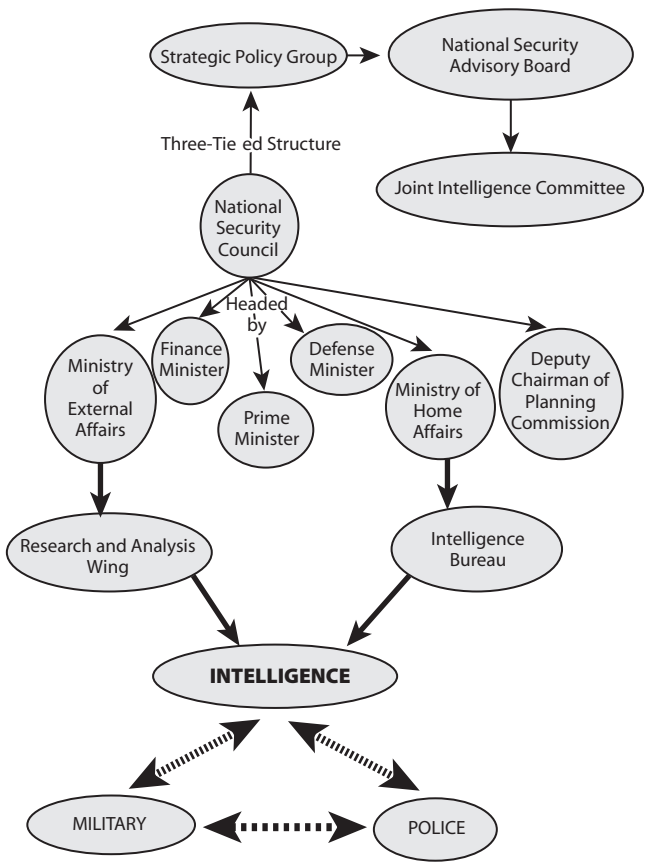

Figure 4. Intelligence agencies in the Indian CT knowledge nexus. (Adapted from Demchak and Werner, " 'Knowledge Nexus.' ")

Police Forces in the Nexus

Since their state-by-state establishment under British rule in the early 1800s, the structure and internal presumptions of the Indian state police forces have remained virtually unchanged.[97] Established to maintain authority for the British Raj, the police's administrative role and vast powers were intended for keeping civil order, not for preventing and detecting crime or, for that matter, terrorism.[98] In 1860, the first reorganization of Indian police began and took place and is still in force today, roughly 145 years later and over 50 years after Indian independence.[99] The Indian Police Act (IPA) of 1861 put the police under the control of the provincial (now state) governments and distinguished between police and military functions. The reorganization's intention was to create an aggressive civilian police force that would relieve the British army of onerous and manpower-intensive duties.[100]

In principle, state police forces are standardized in their operations, in leadership loyalty to all India standard operating procedures, and across critical structures involving lethal force. The Indian Penal Code, Code of Criminal Procedure, and Indian Evidence Act form the basic legal system for police operations throughout India. Similarly, the laws governing the structure of the police organization, officer training, and even the administrative forms and rules are virtually uniform across the country. A director general belonging to the Indian Police Service, the federally recruited body from across India, heads each state police organization and, in principle, this federally trained and selected appointee has jurisdiction over all subordinate units (districts, urban cities, and rural areas) in a particular state. Furthermore, on the national level, key players such as the federal police services, most of the paramilitary forces, and the internal intelligence capabilities found in the IB are subordinate to the federal Ministry of Home Affairs.

In reality, the effective extent of this federally led standardization is limited. The 1861 IPA added to the large overlapping pyramid of national, state, and local police agencies an unusual dual internal separation of all police officers into two vertical branches: armed or unarmed. This structural bifurcation has had profound fragmenting effects on organizational development paths, administrative cultures, and attitudes across state police forces.[101] Indian police forces below the federal level reflect Indian states' ethnicity, language, and culture in their recruits, organizational operations, and local presumptions about roles and behaviors. The result is a wide range in state police competencies and initiative beyond merely maintaining rough social order. Each urban city has its own city

police with a variety of departments. The larger districts are subdivided into police station jurisdictions, with 70 percent of the staff consisting of beat constables with no investigative roles. Compared to other English speaking countries (United Kingdom, United States, Australia, and Canada), India has only a small portion of police staff available for investigative duties and associated paperwork.[102] This arrangement limits the knowledge collection and potential analytical contributions to CT programs for most police units.[103]

In the age of more diffuse terrorism, COIN forces have been evolving into dual-purpose forces among special police units as well as military units. The Central Reserve Police Force is a national police force that assists state and union territories in maintaining law and order and in conducting COIN operations.[104] Other national police organizations have been developed to deal specifically with international border patrol. For example, one entity encompasses the Indo-Tibetan Border Police and Border Security Force. Despite their primary task specialization, these organizations have also deployed to Kashmir and Assam for internal security duties including COIN operations and maintaining law and order.[105] Nonetheless, local police in principle have the internal law and order responsibility, and this ad hoc arrangement generally leaves the local forces politically accountable for failures to prevent terrorism.

Information sharing within and among police agencies reflects the trust, reluctance, and narrow focus common to other Indian bureaucracies. Indian police forces are strongly horizontally stratified, with promotion based on rank and seniority, rarely on critical specializations or particular demonstrations of competence. Copied from the promotion year groups of military forces, the police are organized into cadres by rank. The allocation of power and authority by rank, not position, complicates relations between the central and state police units, since equivalent ranks may occupy very different positions and experience equally different circumstances. A tangled pattern of competition and mistrust throughout these organizations shapes cooperation across police agencies in general.[106]

The 145-year-old rigid vertical division of police forces into unarmed and armed units continues to magnify the lack of cooperation, and to this are added the distinctions of class, gender, ethnic, and other organizational divisions. The 1861 IPA division assigned unarmed police administrative and patrolling duties and armed police the more prestigious tasks requiring physical force. Due to this functional division, for nearly 100 years British colonial administrative officials, including the military, gave spe-

cial attention to discipline and training for armed police. In so doing, they gave armed police considerably more status, empowering them with the ability to protect themselves.[107] In social terms, this distinction reinforced the power distance inherent in Indian society and further dampened trust and the willingness to share knowledge because unarmed police did not have access to this source of prestige.[108]

Furthermore, endemic corruption at all levels intensifies the secrecy or friction between officials. Legislatures routinely try to use police department funding as a tool to force greater efficacy in crime control. The resulting struggle to be seen as more effective against crime routinely produces predatory behaviors and the resort to illegal methods to show politically acceptable outcomes between police units. In standard police units, specialized competence is not required for promotion to senior officer positions. Promotions occur regardless of the candidate's qualifications, and many are governed by caste, favoritism, or nepotism. Ambitious officers eager for early promotions and choice postings use administrative decisions to curry favor with political leaders.[109] With no checks and balances in administrative oversight other than competitive predation and superficial achievements, the cumulative effect of this system of generalist training, turbulent working conditions, patriarchal and repressive management rules, and particularistic and erratic leadership practices is inevitably a lack of trust and cooperative information sharing.

The constitutionally mandated federal-state superstructure for law enforcement also generally inhibits information sharing. The competing centralized and decentralized structures make the Indian police more complex than those in other democracies. While states have their own relatively autonomous police jurisdiction, the central government's history included periods of heavy central control. A great many control mechanisms from those periods persist in the form of, for example, standard procedures and recruiting.[110] State-level police forces buffer themselves procedurally and operationally between the often conflicting demands of these overarching centralizing and decentralizing administrative forces. Endemic budgetary shortfalls contribute to the burdens on officers. For the average officer with too little time, technical training, leverage, and professionalism, joint operations with other departments are unattractive if they require additional efforts (as information sharing often does). Furthermore, such activities inevitably induce disputes over whose budget absorbs the inevitable additional expenses associated with new operations or relationships. These conditions reinforce bureaucratic tendencies to avoid increases in one's

own agency's expenses in terms of time or resources, or in threats to one's personal political prospects.[111]

Among state police forces, routine knowledge sharing is generally sluggish and reactive; when federal forces are involved, normally it is as poor, if not worse. In this highly classed society, if federal forces are called upon to aid state police forces in nonroutine events, historically in both budgets and authority, the national-level forces demand—and inevitably receive—operational dominance. Sudden events that overwhelm local state police forces will usually prompt the central government to send army or paramilitary forces ostensibly to "aid" the civil police force. The federal forces, however, are entirely under central government control, thus demeaning the role and status of the state police forces being "assisted."[112] Efforts by the Ministry of Home Affairs to intervene in purely state business have noticeably increased since the establishment of a federal police in the 1970s.[113] During such ad hoc and usually reactive "assistance" operations, turf battles between state police, paramilitary, and federal police forces often become matters for public discussion.[114] Figure 5 presents the Indian state police organizations participating in the Indian CT knowledge nexus development.

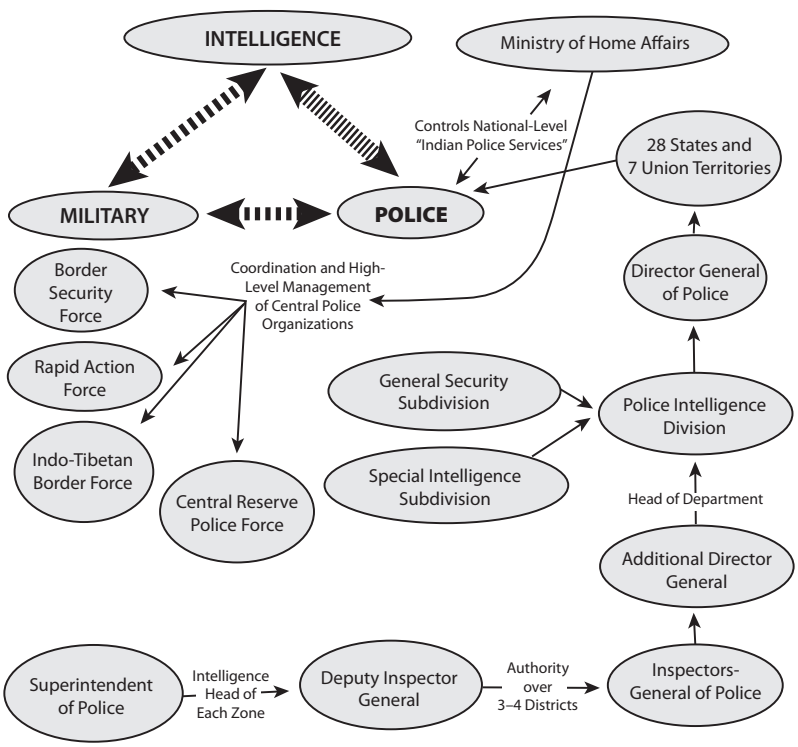

Figure 5. Police elements supporting the Indian CT knowledge nexus. (Adapted from Demchak and Werner, "'Knowledge Nexus.'")

Findings: State-Level Antiterrorist Squad as Emergent Nexus

With this structural, cultural, and institutional history, the evidence of an emergent CT knowledge nexus anywhere in the Indian bureaucracy would seem unlikely. Given the presumptions about power distance, patriarchal management, and centralized control, if any nascent institutionalization in a CT knowledge nexus were to be found, we expected the central government's interest in CT to drive its birth and development. Yet, we found the evidence of a nascent nexus much more compelling at lower levels, closer to the experience of terrorism by the organizations more acutely aware of the consequences of a lack of knowledge. Furthermore, these lower-level organizations apparently responded earlier and more favorably to the status and professionalism boost associated with acting proactively to solve an urgent and life-threatening problem.

As our research suggests, state police forces breached their organizational walls first to begin the institutionalization across the Indian CT knowledge nexus and, in a sense, got lucky. The federal agencies have unexpectedly tolerated this flaunting of traditional prestige and leadership prerogatives. It is not clear why the normally rather imperious national-level agencies would not have attempted to supplant, undermine, or control the nascent institutionalization. We speculate that the state police were first past the post and already clearly operated an institutional forum readily adaptable for attracting knowledge sharing. For the military and intelligence agencies, such an outlet was not readily at hand within their communities for local political or international demonstrations of participation. Furthermore, many of the national-level senior officials have yet to accept that CT is a long-term crosscutting threat. Not making CT a prominent institutional motif in their ranks, they have also not targeted their heavy political guns on this potential institutional source of increased state police prestige. Hence, it may be that, in the bureaucratic circumstances of modern India, only a bottom-up initiative would have had a chance for success. Because of the external push and prestige, it was possible for the institutional objectives to converge on jointly building state-level ATSs without having overarching national-level bureaucratic competition impede progress as would ordinarily occur.[115]

In 1986 India created its first counterterrorist units, the National Security Guards, which were the "first bricks of India's counterterrorism architecture."[116] Numbering about 7,500 mixed military and police officers, the NSG is consid-

ered a highly valuable and experienced group in COIN in the northern state of Jammu and Kashmir, and previously in Punjab. "It is divided into two roughly equal groups—the Special Action Group (SAG) and the Special Ranger Group (SRG). The SAG is the elite offensive group, which recruits its members from the Indian Army. The SRG consists of supporting personnel recruited from paramilitary and police units such as the Border Security Force, the Central Reserve Police Force, and others. The SRG has the job of securing and isolating the target for assault by the SAG."[117] While officially under jurisdiction as a military unit, the NSG does not contain any intelligence acquisition and sharing capabilities and depends on external intelligence agencies.[118]

The mid-1980s establishment of the NSG influenced the subsequent creation, objective, mission, and training of state-level antiterrorism squads, especially in states that experienced terrorism for many years.[119] India became the first federal democracy to have state-level ATSs, in part because state police clearly have the "law and order" responsibility and in part because terrorism was historically localized in places like Kashmir and not considered a national-level problem.[120] As different types of terrorism began to expand across borders and involve multiple states in devastating terrorist attacks, state governments individually began to set up ATSs as relatively quick solutions to defuse political pressure and possibly to prevent future attacks. By 2001, but before the attack on the United States, 18 Indian states had established 10 full-time and nine near-full-time proto-ATSs.

By the end of the 1980s, part-time police attention to terrorism and the strong reliance on the army or the paramilitaries to bail out an overwhelmed police force grew less politically acceptable at the local level. In 1989 Andhra Pradesh Police created the first ATS, called the Greyhounds (reorganized in 2005). This unit was specifically dedicated to developing CT tactics and procedures acquired from the federal NSG, which in turn was modeled on the British SAS, German GSG-9, and Israeli Sayeret Matkal. This first official, full-time ATS at the state level served as a training source for other state-level units learning antiterror tactics, procedures, and operations prior to forming an ATS. This unusual sharing of tactics and techniques across normally competitive police forces led to the successful establishment of ATS institutions in other Indian states such as Orissa, West Bengal, Maharastra, and Chathisgarh.[121]

The surprising aspect of these ATSs is their unprecedented level of police, intelligence, and military cooperation fostered by what is normally seen as a lower level of the national bureaucracy. Each ATS draws essential mission training, planning skills, tactical plans, and doctrine from the military via

the NSG. From each major intelligence agency the ATSs receive seconded officers serving long-term rotations up to 18 months. The effect is a constant flow of contacts, expertise, and personally delivered access to critical data that would otherwise not be available to state-level officials.

Another particularly unexpected attribute of these ATSs—given India's complex bureaucratic architecture—is the general acceptance that the local ATS has exclusive right to collect and verify intelligence information in its jurisdiction and carry out operations in any part of the state. Tasked with coordinating between the multiple levels of intelligence agencies and analyzing inputs on terrorist activities, ATSs are formally designated as the lead actors confronting terrorist activities in their jurisdiction. It is rare, if not unprecedented, for a state police organization to have intelligence preeminence in an area also considered the domain of the national-level agencies. At the federal level, army, IB, RAW, and federal police forces have occasionally cooperated briefly for a single, usually nonroutine objective but historically have gone on to clash repeatedly over operational procedures in the aftermath of operations. The creation of ATSs and the urgency of antiterrorism successes have, in this domain, nullified the earlier system where anti-insurgency operations were the preserve of the Indian Army and the paramilitary forces, both of which report to the central government with no obligation to coordinate with state-level entities.[122]

This special position seems to have been anticipated and embedded into the mandate of these units from their initial inception in India. For example, in 2003 an ATS in Mumbai planned in advance to "co-ordinate between the city, state and intelligence agencies and analyse inputs on terrorist activities."[123] At the state level, the ATS organization facilitates more cross-jurisdictional interactions over the longer term and across objectives than occurs normally in overlapped federal operations. Hence, all things being equal, participating in an ATS offers considerable prestige for police officers. ATS organizations are therefore more able to recruit qualified and trained professionals without as much of the intervention or precoordination processes found in the more rigid standard police or military command structure.

In particular, ATSs seem better placed to initiate antiterror operations with greater secrecy and responsiveness to local conditions.[124] While police forces themselves are distinct due to their origins and political circumstances, ATSs have specialized over time to reflect the flavor of terrorist groups in their states.[125] An ATS in Chandigarh will confront terrorist activities with a different ideology in contrast to the ATS in Andhra Pradesh, where ter-

rorist activities reflect Naxalite antiregime activities.[126] For example, Jammu and Kashmir's once proto-antiterrorism squad, the Special Operations Group (SOG) (established in 1994), has evolved from a relatively passive unit staffed by locally recruited volunteer officers to a proactive operating unit specializing in knowing the region. Reasons for volunteering for ATS duty range from passionate dedication to financial incentive. The SOG antiterrorism squad has evolved into a robust center for coordinating operations focused on the conditions of the Northwest. It is capable of coordinating large-scale operations with paramilitary forces of the Indian Army while sharing its intelligence with central government forces.[127]

Indian terrorism in both numbers of incidents and casualties declined after 2001, and yet the rate of establishment of ATSs did not. Since the United States had not yet made terrorism a household word prior to 2001, it is fair to attribute the stimulus for the earlier institutions to actual experience and to an unusual history of urgency passed along among police, military, and intelligence officers rotating across CT positions. For police officers, counterterrorism operations were urgent and prestige enhancing professionally when terrorism was on the rise. The Greyhounds of Andhra Pradesh demonstrated early on an unusual willingness to integrate officers from other services into these activities, offering interesting work and more resources. As officers rotated across state ATS and proto-ATS (those with part-time CT duties), the greater professional and social interaction also likely increased trust, broader intelligence sharing, and more effective joint state operations against terrorists operating across states. This positive feedback loop appears to have continued even as the incidents themselves declined. Service at a state level ATS in the heart of the knowledge nexus appears to have become desirable across the police officer community.

After 9/11, the international community also contributed to the enhanced prestige of ATS service. After 2001, in its efforts to have as much intelligence provided as possible from all conceivable allies, the United States pushed very publicly and internationally to make antiterrorism activities status enhancing across the various international referent groups—police, military, and intelligence officers.[128] The US-framed argument was compelling in light of the deepening of globalization and dependence of many nations, including India, on the global sociotechnical infrastructure (GSTI) sustaining economic growth.[129] Representatives of the United States argued that members of the developed and advancing world of democracies are part of a vital GSTI threatened by terrorism. The message emphasized that attacks on one will inevitably harm others

and, hence, all must corral the civil-military capabilities of each nation to protect ourselves as well as others.[130] Being a stalwart warrior ready for the coming battles against terror from globalized radical groups thus not only offered local professional pride, but also the possibility of US resources to the country.

This public marketing had an underlying truth in the objective reality of interdependence that was—and is—obvious. The influence of the remaining superpower, the United States, to force an item to become important on the world's agenda added to the attraction of security officials in many nations to be seen as part of the grand alliance saving democracies from this existential threat. For Europeans, the post-9/11 attacks on Madrid and London reinforced the US message, deepening the worldwide salience of CT as an issue for senior political and professional leaders to consider.

Furthermore and not least, the global war on terror, so named by the United States, came with the vague promise of financial or other benefits to those democracies signing up to participate.[131] Although the evidence is spotty that this benefit has been widely distributed, nonetheless, the bilateral possibility has helped spread the prestige of association with the program.[132] For public agencies with few clear-cut ways to demonstrate effectiveness, prestige among stakeholders and military, intelligence, and police referent groups offer a substitute performance measure.[133]

With the bureaucratic reality of being public agencies in India, all three security communities would, in principle, find international referent group and local political prestige advantages to be seen as participating in the transnational antiterrorism cause. One would expect national-level agencies to attempt to take the forefront in order to absorb the bulk of the available prestige, but their bureaucratic instruments were already tied up in the army or paramilitaries with a mixed bag of traditional obligations. The prestige tended to gravitate toward the community with an existing institutional model, the state police.

As a result, from 2001 to 2005, over a scant four years—despite declining local experience with terrorism—eight new ATSs were formally designated; five were new institutions, and three were reorganized from part-time to full-time ATSs. To move quickly, there was only one solid game in town and that was the ATS instrument now firmly within the power of the state police to create and run. The timing of this growth strongly suggests that, by this time, the prestige and possible effectiveness of this institutional instrument were driving its support across all three communities. Figure 6 summarizes this acceptance of the central position of the ATS in the CT domain and in the Indian CT knowledge nexus.

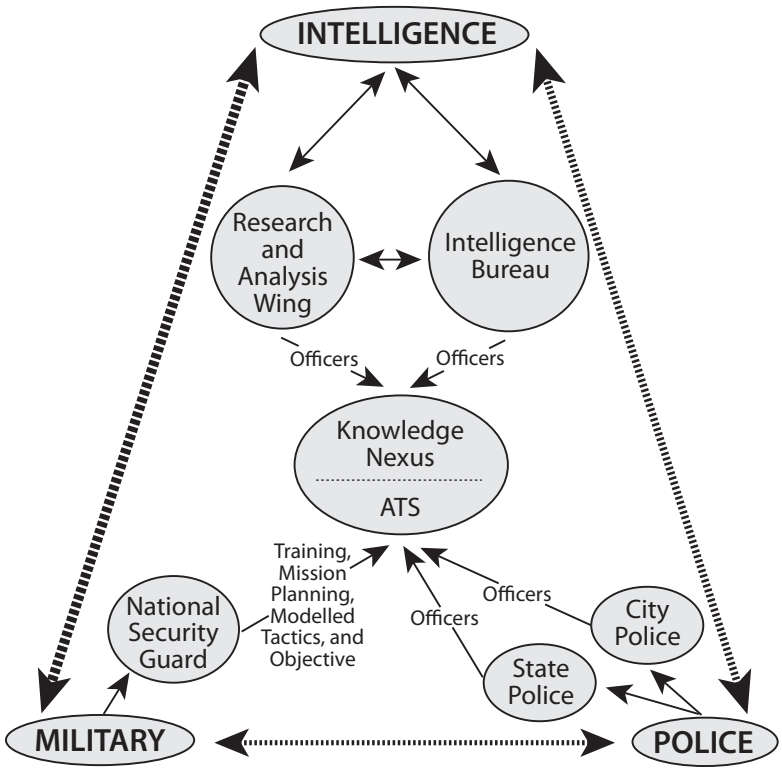

Figure 6. Nascent Indian knowledge nexus. (Developed by Demchak and Werner, 2007.)

Conclusion

By 2005, nearly every state in India had an ATS operating in its territory, each with contacts to the military and seconded officers from the IB and the RAW. In the process of personnel rotation, CT operations, and shared daily experiences, previously unobtainable intelligence information flowed between these organizations. By our definition, a nascent knowledge nexus emerged, as shown by the organizational evidence of collaboration, acceptance, and presence in public reports. We found no evidence of this nexus being pursued along technical lines in terms of functioning information technology systems. It is possible to have some networked exchanges, especially after a seconded officer has returned to the national agency but retains some friendship and loyalty for the ATS in which he served. However, consistent with the history of information technologies within Indian public agencies so far, it is unlikely that extensive technical systems are being built and used.[134] The more likely technical scenario involves rudimentary technical means such as e-mail, occasional data disks, and some Web access.

This work explored a hypothesis that a lack of knowledge felt by an organization concerning something really important would generate action to fill that gap and that reaching outside the organization is a reasonable next step unless cultural, organizational, or other obstacles stop the search. If these obstacles exist routinely in abundance, then our model suggests the importance of the problem has to be even greater to push organizational insiders to reach out to other organizations or to be receptive to being contacted for knowledge. As long as the knowledge is needed and the stimulus elevated, we hypothesized that the sharing would continue.

A secondary hypothesis held that CT seems to present that kind of powerful stimulus in India. We began by presuming the mass casualty goals of terrorists would be sufficiently important to inspire a knowledge search outside organizations. To test this idea, we looked for evidence of such sharing overcoming rather enormous obstacles in order to obtain missing knowledge, as well as for evidence that terrorism's enduring presence would result in the slow formalization of this sharing into institutional linkages in a nexus. The stronger the need, the more these links would mature. Hence, we looked at a really tough case—the very turf-bound Indian bureaucracy—for evidence that terrorism could force otherwise unlikely knowledge sharing.

Both of these hypotheses proved to be valid. However, the surprise for us was the path taken. The least prestigious of the three communities—military, intelligence, and police—ended up sponsoring the kernel and growth of the nexus. The state police filled in the empty institutional space where such exchanges among the communities could be had, were definitely needed, and could endure over time as the problem persisted. In the process, their institution—the state police ATS—became the model for expanding antiterrorism activities as more ATSs were established despite a decline in actual domestic Indian terrorism.

The Indian experiences offer some lessons for the United States in its counterterrorism efforts. First, reaching outside organizational boundaries is often not successful if merely imposed from the top. The desire to find missing knowledge must be felt urgently by those who will participate in the creation of a knowledge nexus. Experience with bad outcomes, without the missing knowledge, is historically the best stimulant for organizational members to reach outside; but often enough a clear, unmistakable prestige associated with participating in the nexus also furthers its development. Senior leaders can clearly enhance the prestige of knowledge sharing by

participating in nexus exchanges and by using the social tools they already have to reward change agents at midlevels or even lower.

Second, working with another organization must be institutionally seen as easy as well as useful. In the Indian case, the officers seconded to ATS were left in place longer than were their compatriots in other positions, making the process of exchange and networking a natural part of the workday. In the United States, the use of "Atrium" cyberspaces into which all individuals rotate at set points in their careers makes exchanges easier and more likely to develop the missing knowledge by tapping into tacit knowledge. The appendix has a short description of this model of collaborative tacit knowledge development applied to joint operations. The key is that the computer as a colleague provides a virtual institutional arena in which everyone must periodically enter to operate with others. Assigned to or simply accessing the Atrium, each member at some point plays out hypotheses collectively, exchanges observations, and extracts new knowledge as needed.

Third, technological advances do not operate as integrators or effective knowledge development tools unless the social groundwork has been laid to make the knowledge nexus processes both useful and easy to pursue. The case for expeditiously finding missing knowledge must be unmistakably and ever present, and the means must be readily at hand and easily grasped up and down the ranks of the organizations that will form the nexus. In India, the early pressure from ballooning terrorism met the useful requirement, and the Indian/British habit of widely seconding officers made it easier to redirect them into the emerging state-level police innovation called an ATS. The organizational innovations spread as a result, institutionalizing the CT knowledge nexus in India. The US Department of Homeland Security was a top-down imposition into the otherwise moribund CT knowledge nexus of the United States and has yet to fulfill its collaborative knowledge development mandate. For the US military, even in an Atrium joint military, the social construction of knowledge nexus development will be a bigger challenge than assembling the technical systems. SSQ

Notes

1. Our many thanks to Craig R. Haubrich, whose research assistance at the outset of this project in investigating several candidate case study countries brought India's interesting knowledge nexus path to our attention.

2. The classical literature on organization theory and the formation of the modern political state is voluminous. As a result, we will not cite beyond a few classical authors for the benefit of scholars new to the field. See James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory* (New York: McGraw-Hill, 1967) for a discussion of organizations and their search for

certainty. See Philip Selznick, *Leadership in Administration: A Sociological Interpretation* (Berkeley, CA: University of California Press, 1984) for a discussion of institutionalization. David Easton, *A Systems Analysis of Political Life* (New York: Wiley, 1965) discusses basic political theory in modern democracies. See W. Richard Scott, *Organizations: Rational, Natural, and Open Systems* (Upper Saddle River, NJ: Prentice Hall, 2003) for a nearly peerless review of the notions of organization theory and institutions. See Easton, *Systems Analysis,* and James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989) for discussions of how bureaucracies develop their internal notions of what must be pursued and how. For a more recent discussion of these prior notions and their cross-cultural implications, see Geert H. Hofstede and Gert Jan Hofstede, *Cultures and Organizations: Software of the Mind,* 2nd ed. (New York: McGraw-Hill, 2005).

3. While few would argue with the destructive consequences of war, the need for certainty under conditions of widespread survival-threatening surprise historically forced enormous institutional innovation. In Europe, these led to the formation of the modern Westernized state. For one of the best explanations of this process, see Tilly's tour de force on the interactions of war, capital, and the church in the formation of the modern European state. Charles Tilly, *Coercion, Capital, and European States*, *AD 990–1992* (Cambridge, MA: Blackwell Publishers, 1992).

4. See William Seymour, *Decisive Factors in Twenty Great Battles of the World* (London: Sidgwick & Jackson, 1988); and Katy Bindon, "Arrogant Armies: Great Military Disasters and the Generals Behind Them," book review, *Historian* (Allentown) 60, no. 3 (Spring 1998): 687–88.

5. Wilson, *Bureaucracy.*

6. Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999).

7. Thomas L. McNaugher, *New Weapons, Old Politics: America's Military Procurement Muddle* (Washington, DC: Brookings Institution Press, 1989).

8. Israel is an exception for obvious reasons. See George P. Fletcher, *Romantics at War: Glory and Guilt in the Age of Terrorism* (Princeton, NJ: Princeton University Press, 2002); Walter Laqueur, *A History of Terrorism* (New Brunswick, NJ: Transaction Publishers, 2001); A. H. Garrison, "Terrorism: The Nature of Its History," *Criminal Justice Studies: A Critical Journal of Crime, Law and Society* 16*,* no. 1 (2003): 39–52; and Richard K. Betts, "Striking First: A History of Thankfully Lost Opportunities," *Ethics and International Affairs* 17, no. 1 (2003): 17–26.

9. Isaac Cronin, ed., *Confronting Fear: A History of Terrorism* (New York: Thunder's Mouth Press, 2002).

10. R. M. Cassidy, *Peacekeeping in the Abyss: British and American Peacekeeping Doctrine and Practice after the Cold War* (New York: Praeger, 2004).

11. Austin Long, *On "Other War": Lessons from Five Decades of RAND Counterinsurgency Research* (Santa Monica, CA: RAND Corp., 2006).

12. See Michael Howard's seminal writings on innocence and war and the role played by this expectation of protection by governments. Michael Eliot Howard, George J. Andreopoulos, and Mark R. Shulman, eds., *The Laws of War: Constraints on Warfare in the Western World* (New Haven, CT: Yale University Press, 1994). See also Castells' tour de force on the evolutions of the modern Westernized world and the interdependent ripple effects. Manuel Castells, *The Information Age: Economy, Society and Culture,* vol. 1, *The Rise of the Network Society*; and vol. 3, *End of Millennium* (Malden, MA: Blackwell Publishers, 2000).

13. John Urry, "The Global Complexities of September 11th," *Theory, Culture and Society* 19, no. 4 (1 August 2002): 57–69.

14. David Cole, *Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism* (New York: New Press, 2003).

15. Scholars in the field of LTS have an enormous brief: to study the societal implications of the massive explosion in organizationally integrating technologies across widely influential sociotechnical systems. The basic works in this literature first emerged 30 years ago and are nearly drowned today by the vast amounts of support research into the wider institutional and societal realities of the still emerging information and terrorism ages. For a basic understanding of the term *LTS* and the field, see Summerton. Jane Summerton, ed., *Changing Large Technical Systems* (Boulder, CO: Westview Press, 1994).

16. Globalspecialoperations, "United Kingdom Special Air Service Regiment," http://www.globalspecialoperations.com/sas.html.

17. "GSG-9," *Wikipedia*, Wikipedia.com.

18. SpecWarNet, "Germany's GSG [*Grenzschutzgruppe*]-9," http://www.specwarnet.net/europe/gsg9.htm.

19. Sergio Catignani, "The Security Imperative in Counterterror Operations: The Israeli Fight against Suicidal Terror," *Terrorism and Political Violence* 17, nos. 1/2 (Winter 2005): 245–64.

20. Bruce Newsome, "Expatriate Games: Interorganizational Coordination and International Counterterrorism," *Studies in Conflict and Terrorism* 29, no. 1 (2006): 75–89.

21. Chris C. Demchak, *Military Organizations, Complex Machines: Modernization in the U.S. Armed Services* (Ithaca, NY: Cornell University Press, 1991).

22. R. M. Hodgetts and F. Luthans, *International Management: Culture, Strategy, and Behavior* (New York: McGraw-Hill, 2006).

23. Tilly, *Coercion, Capital, and European State*s.

24. Selznick, *Leadership in Administration*; and Thompson, *Organizations in Action*.

25. Michael N. Schmitt, *Counter-terrorism and the Use of Force in International Law* (Garmisch-Partenkirchen, Germany: George C. Marshall European Center for Security Studies, 2002).

26. Selznick, *Leadership in Administration*.

27. Castells, *Information Age*.

28. Paul J. DiMaggio and Walter W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review* 48, no. 2 (April 1983): 147–60.

29. Robert L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression* (New York: Oxford University Press, 1989).

30. DiMaggio and Powell, "Iron Cage Revisited," 147–60.

31. Annmarie Hauck Walsh, *The Public's Business: The Politics and Practices of Government Corporations* (Cambridge, MA: MIT Press, 1978).

32. Michael E. O'Hanlon et al., *Protecting the American Homeland: One Year On* (Washington, DC: Brookings Institution Press, 2003); and Stephen Sloan, "Organizing for National Security: The Challenge of Bureaucratic Innovation in the War against Terrorism," *Public Administration Review* 62, no. 1 (September 2002): 124–25.

33. Charles R. Wise, "Organizing for Homeland Security," *Public Administration Review* 62, no. 2 (March/April 2002): 131–44; and Jonathan Stevenson, "How Europe and America Defend Themselves," *Foreign Affairs* 82, no. 2 (March/April 2003): 75–90.

34. Anja Dalgaard-Nielsen and Daniel S. Hamilton, eds., *Transatlantic Homeland Security*: *Protecting Society in the Age of Catastrophic Terrorism* (London, UK: Routledge, 2005); Walter Enders and Todd Sandler, *The Political Economy of Terrorism* (Cambridge, UK: Cambridge University Press, 2006); and Ian S. Lustick, *Unsettled States, Disputed Lands: Britain and Ireland, France and Algeria, Israel and the West Bank-Gaza* (Ithaca, NY: Cornell University Press, 1993).

35. Stuart Corbridge, *Seeing the State: Governance and Governmentality in India* (Cambridge, UK: Cambridge University Press, 2005); and Rajesh Tandon and Ranjita Mohanty, *Civil Society and Governance: A Research Study in India* (Sussex, UK: Institute of Development Studies, June 2000).

36. Sebastian Morris, "The Challenge to Governance in India," in *India Infrastructure Report 2002: Governance Issues for Commercialization,* eds. Sebastian Morris and Rajiv Shekhar (New Delhi: Oxford University Press, 2002), 15–36; and Ferrel Heady, *Public Administration: A Comparative Perspective* (*N*ew York: Marcel Dekker, 2001).

37. K. C. Roy and C. A. Tisdell, "Good Governance in Sustainable Development: The Impact of Institutions," *International Journal of Social Economics* 25, nos. 6/7/8 (1998): 1310–25.

38. V. Subramaniam, "Comparative Public Administration: From Failed Universal Theory to Raw Empiricism—a Frank Analysis and Guidelines Towards a Realistic Perspective*," International Review of Administrative Sciences* 66, no. 4 (December 2000): 557–72.

39. K. Sriramesh, Y. Kim, and M. Takasaki, "Public Relations in Three Asian Cultures: An Analysis," *Journal of Public Relations Research* 11, no. 4 (1999): 271–92; and Michael Howlett, "Administrative Styles and Regulatory Reform: Institutional Arrangements and Their Effects on Administrative Behavior," *International Public Management Review* 5, no. 2 (2004): 13–35.

40. A. P. D'Costa, "Institutions and Industrial Governance in India: Learning to Cooperate the Japanese Way," *Asian Business and Management* 2, no. 1 (April 2003): 63–89; and Robin Mearns and Saurabh Sinha, *Social Exclusion and Land Administration in Orissa, India* (Washington, DC: World Bank, 1999).

41. M. Govinda Rao, "Tax Reform in India: Achievements and Challenges," *Asia-Pacific Development Journal* 7, no. 2 (December 2000): 59–74; and Richard Heeks, "The Approach of Senior Public Officials to Information Technology-Related Reform: Lessons from India," *Public Administration and Development* 20, no. 3 (2000): 197–205.

42. "India's Terrorist Groups," South Asia Terrorism Portal, http://www.satp.org/satporgtp/countries/india/terroristoutfits/index.html.

43. P. H. Appleby, *Public Administration in India: Report of a Survey*, 1953 (New Delhi: Cabinet Secretariat, Government of India, 1957).

44. R. K. Mishra, "National Civil Service System in India: A Critical View," in *Civil Service Systems in Asia,* eds. John P. Burns and Bidhya Bowornwathana (Cheltenham, UK: Edward Elgar, 2001), 117–51.

45. R. B. Jain, "Towards Good Governance: A Half Century of India's Administrative Development," *International Journal of Public Administration* 24, no. 12 (December 2001): 1299–1334.

46. D. K. Das and A. Verma, "The Armed Police in the British Colonial Tradition: The Indian Perspective," *Policing: An International Journal of Police Strategies and Management* 21, no. 2 (1998): 354–67.

47. Subramaniam, "Comparative Public Administration," 557–72.

48. Hofstede and Hofstede, *Cultures and Organizations*, 2005.

49. Shailendra Kumar Chaturvedi, *Metropolitan Police Administration in India* (New Delhi: B. R. Pub. Corp., 1985), 1–29.

50. Mishra, "National Civil Service System in India," 117–51; and Christopher Kingston, "Social Capital and Corruption: Theory and Evidence from India" (paper, Amherst College, Amherst, MA, 18 July 2005).

51. "Untouchables" refers to a group of people in positions of power and influences under positive discriminatory arrangements. These arrangements contain similar social elements to affirmative action and positive discriminatory arrangements. Das and Verma, "Armed Police," 354–67.

52. A. Sen, "How Well Are India and China Doing?" in *Fresh Perspectives on India and Pakistan: Essays on Economics, Politics and Culture*, ed. Iqbal Khan (Oxford: Bougainvillea Books, 1985), 85–97.

53. Samuel Paul and Sita Sekhar, "A Report Card on Public Services: A Comparative Analysis of Five Cities in India," *Regional Development Dialogue* 18, no. 2 (1997): 119–32; and D'Costa, "Institutions and Industrial Governance in India," 63–89.

54. David H. Bayley, "Comparative Organization of the Police in English-Speaking Countries," *Crime and Justice* 15 (1992): 509–45.

55. Mearns and Sinha, *Social Exclusion*.

56. R. B. Jain, "Parliament and Policy in India," *Asian Journal of Public Administration* 6, no. 2 (December 1984): 46–72; and Government of India, Department of Administrative Reform and Public Grievances (DARPG) 2005, Second Administrative Reforms Commission, *Unlocking Human Capital: Entitlements and Governance—A Case Study* (New Delhi: Ministry of Personnel, Public Grievances and Pensions, July 2006), http://arc.gov.in/index.htm.

57. Mishra, "National Civil Service System in India," 117–51.

58. Ranjan Pratyush, "Supreme Court Orders to Reform Indian Police," *India Daily,* 23 September 2006, http://www.indiadaily.org/entry/supreme-court-orders-to-reform-indian-police.

59. S. S. Negi, "Supreme Court Orders Police Reforms: Gives Centre, States 3-Month Ultimatum," *Tribune Online* (India), 23 September 2006, http://www.tribuneindia.com/2006/20060923/main1.htm.

60. Vijay and Kumar Singh, "Twin Blasts—Here's Our Anti-Terror Squad," *Rediff News*, 25 August 2004, http://http://in.rediff.com/news /2004/aug/25mum.htm.

61. S. Krishna, Sundeep Sahay, and Geoff Walsham, "Managing Cross-Cultural Issues in Global Software Outsourcing," *Communications of the ACM* 47, no. 4 (April 2004): 62–66.

62. Hodgetts and Luthans, *International Management*.

63. Col Christopher Langton, ed., *The Military Balance*, *2005–2006* (London: International Institute for Strategic Studies, October 2005).

64. C. Christine Fair, "Military Operations in Urban Areas: The Indian Experience," *India Review* 2, no. 1 (January 2003): 49–76.

65. Omar Khalidi, *Khaki and the Ethnic Violence in India: Army, Police and Paramilitary Forces during Communal Riots* (New Delhi: Three Essays Collective Press, 2003).

66. Sunil Dasgupta, "Understanding Paramilitary Growth: Agency Relations in Military Organization" (paper presented at the Curbing Human Rights Violations by Non-State Armed Groups conference, University of British Columbia, Vancouver, BC, Canada, 13–15 November 2003).

67. Rajesh Rajagopalan, "Innovations in Counterinsurgency: The Indian Army's Rashtriya Rifles," *Contemporary South Asia* 13, no. 1 (March 2004): 25–37.

68. Jonah Blank, "Kashmir: All Tactics, No Strategy," *India Review* 2, no. 3 (3 July 2003): 181–202.

69. Khalidi, *Khaki and the Ethnic Violence in India*, 2003.

70. P. Swami, "Failed Threats and Flawed Fences: India's Military Responses to Pakistan's Proxy War," *India Review* 3, no. 2 (April 2004): 147–70.

71. Ibid.

72. Stephen Peter Rosen, *Societies and Military Power: India and Its Armies* (Ithaca, NY: Cornell University Press, 1996).

73. Fair, "Military Operations in Urban Areas," 49–76.

74. Josy Joseph, "Defence Intelligence Agency Gets a New Head," *Rediff News,* 17 February 2004, http://inhome.rediff.com/ news/2004/ feb/17dia.htm?zcc=ar.

75. Rahul Bedi, "Turf Battles Hit Indian Spy in the Sky," Indo-Asian News Service, New Delhi, 19 March 2006, http://www.pakdef .info/forum/archive/ index.php/t-8033.html.

76. Joseph, "Defence Intelligence Agency."

77. Ibid.

78. Bisheshwar Mishra, "IB [Intelligence Bureau] Wants to Enter RAW Turf Now," *Times of India*, 5 February 2005.

79. Jayal, "No Time for Turf Wars"; and Girish Chandra Saxena, "Gary's People," *Rediff News*, 8 November 1999, http://www.rediff.com/news/1999/nov/09gary.htm.

80. Swami, "Failed Threats and Flawed Fences," 147–70.

81. GlobalSecurity, "Research and Analysis Wing (RAW)," http://www.globalsecurity.org/intell/world/india/raw.htm.

82. Mishra, "National Civil Service System," 117–51.

83. GlobalSecurity, "Research and Analysis Wing."

84. Ibid.

85. S. M. Hali, "RAW at War—Genesis of Secret Agencies in Ancient India," *Defence Journal,* February/March 1999, http://www.defence journal.com/feb-mar99/raw-at-war.htm.

86. Mishra, "National Civil Service System in India," 117–51.

87. Sultan Shahin, "India Shuffles Its Intelligence Pack," *Asia Times Online,* 26 September 2001, http://www.atimes.com/ind-pak/CI26Df04.html.

88. Hali, "RAW at War."

89. "No Information on Netaji, Says RAW," *Times of India*, 1 February 2007.

90. C. K. Kutty, "The Outsider, Part I: A RAW Hand," *Rediff Special*, 2 February 2005, http://www.rediff.com/news/2005/feb/03 spec1.htm.

91. Tara Shankar Sahay, "Jaswant Unhappy with Intelligence Agencies," *Rediff News*, 23 December 2003, http://www.rediff.com// news/2003/dec/22ib.htm

92. Swapan Dasgupta, "What's Wrong with RAW?" *Rediff News*, 19 July 2004, http://www.rediff.com/news/2004/jul/9swadas.htm.

93. George Iype, "Why Intelligence Fails, and Terrorists Succeed," *Rediff News*, 20 July 2006, http://ia.rediff.com/news/2006/jul/20 george.htm.

94. V. Subramaniam, "Indian Legacy of Administration," *in Handbook of Comparative and Development Public Administration*, 2nd ed., ed. Ali Farazmand (New York: Marcel Dekker 2001), 77–87; and Jain, "Parliament and Policy in India."

95. Saxena, "Gary's People."

96. Mishra, "National Civil Service System in India," 117–51.

97. David H. Bayley, "The Police and Political Order in India," *Asian Survey* 23, no. 4 (April 1983): 484–96.

98. Das and Verma, "Armed Police," 354–67.

99. Negi, "Supreme Court Orders Police Reforms."

100. C. V. Narasimhan, "Police and the Constitution," editorial, *Hindu*, 20 November 2001, http://www.thehindu.com/thehindu/op/ 2001/11/20/stories/2001112000010100.htm.

101. David H. Bayley, *Patterns of Policing: A Comparative International Analysis* (Rutgers, NJ: Rutgers University Press, 1990).

102. Bayley, "Comparative Organization of the Police," 509–45.

103. Arvind Verma and Srinagesh Gavirneni, "Measuring Police Efficiency in India: An Application of Data Envelopment Analysis," *Policing: An International Journal of Police Strategies and Management* 29, no. 1 (2006): 125–45.

104. Fair, "Military Operations in Urban Areas," 49–76.

105. Y. S. Jafa, "Defeating Terrorism: A Study of Operational Strategy and Tactics of Police Forces in Jammu & Kashmir (India)*," Police Practice and Research* 6, no. 2 (May 2005): 141–64.

106. Das and Verma, "Armed Police," 354–67.

107. Narasimhan, "Police and the Constitution."

108. Arvind Verma, "A Uniform Betrayal," *India Together*, June 2004, http://www.indiatogether.org/2004/jun/gov-betray.htm.

109. Chaturvedi, *Metropolitan Police Administration in India*, 1–29.

110. P. G. Shane, *Police and People: A Comparison of Five Countries* (London: C. V. Mosby, 1980).

111. Iype, "Why Intelligence Fails."

112. Shane, *Police and People*.

113. Shyam Nath and Partha Gangopadhyay, "Deprivation and Incidence of Urban Public Services: A Tale of Three Cities," *Review of Urban and Regional Development Studies* 13, no. 3 (November 2001): 207–20.

114. Verma, "Uniform Betrayal."

115. Newsome, "Expatriate Games," 75–89.

116. B. Raman, "Evolution of India's Counterterrorism Capabilities," paper no. 1793, online posting to South Asia Analysis Group, 5 October 2006, http://www.saag.org/papers18/paper1793.html.

117. Kenneth Conboy and Paul Hannon, *Elite Forces of India and Pakistan* (London: Osprey Publishing, 1992).

118. Ved Marwah, "India's Internal Security Challenges," *Strategic Analysis* 27, no. 4 (October–December 2003): 503–14.

119. Dr. Subhash Kapila, "India's Flawed Counter-Terrorism Responses: A Macro-Analysis," paper no. 1889, online posting to South Asia Analysis Group, 25 July 2006, http://www.saag.org/papers19/paper1889.html.

120. Das and Verma, "Armed Police," 354–67.

121. "Units—Grey Hounds: The Elite Commando Force," Andhra Pradesh (India) Police Web site, http://www.apstatepolice.org/AboutUs/units/units_greyhounds.htm.

122. Kapila, "India's Flawed Counter-Terrorism Responses."

123. Deepak Lokhande, "Rakesh Maria May Head Anti-Terror Squad," *Mid-Day*, 30 August 2003, http://www.mid-day.com/news/city/2003/august/62573.htm.

124. Somit Sen, "City Gets Its Own Anti-Terror Squad," *Times of India*, 30 July 2004.

125. Vijay and Kumar Singh, "Twin Blasts."

126. "Anti-Terrorist Squad Sanctioned for UT [Union Territory of Chandigarh]," *Tribune*, 2 October 1998, http://www.tribuneindia.com/1998/98oct02/chd.htm; and Kapila, "India's Flawed Counter-Terrorism Responses."

127. Basharat Peer, "SOG: Good Guys or Bad Guys?" *Rediff News*, 31 October 2002, http://www.rediff.com/news/2002/oct/31spec.htm.

128. John Urry, "The Global Complexities of September 11th," *Theory, Culture and Society* 19, no. 4 (1 August 2002): 57–69.

129. Thomas Donnelly and Vance Serchuk, *National Security Outlook: Fighting a Global Counterinsurgency* (Washington, DC: American Enterprise Institute for Public Policy Research, December 2003), http://www.ciaonet.org/pbei/aei/nso/dot13/dot13.pdf.

130. Ingrid Vaicius and Adam Isacson, *International Policy Report: The "War on Drugs" Meets the "War on Terror"* (Washington, DC: Center for International Policy, February 2003).

131. Jude Howell, "The Global War on Terror, Development and Civil Society," *Journal of International Development* 18, no. 1 (January 2006): 121–35.

132. Todd Moss, David Roodman, and Scott Standley, *The Global War on Terror and US Development Assistance: USAID Allocation by Country, 1998–2005*, working paper no. 62 (Washington, DC: Center for Global Development, 18 July 2005).

133. Thompson, *Organizations in Action*.

134. Heeks, "Approach of Senior Public Officials," 197–205.

Appendix

Atrium Model of Collaborative Knowledge Development for Joint Operations

The Atrium model of "computer as colleague" deliberately structures as routine the tacit knowledge collaborative development across otherwise disparate communities needed to meet critical infrastructure crises. It was originally designed for use by militaries modernizing into network warfare and needing to capture and develop tacit knowledge from many subordinate organizations in order to meet surprises. The Atrium model is intended to be an alternative sociotechnical organizational design based loosely on Nonaka and Takeuchi's original corporate hyperlinked model and incorporates the computer as a colleague, not as a library or controller.[1] Rather, the knowledge base of the organization explicitly seeks to provide a familiar place to get these lessons and to share one's own. Entering into and interacting with the Atrium is essentially acting with a major player in the institution.

One "goes into" the Atrium as a consumer, contributor, or producer. Each individual in the allied organizations cycles through every role—no exceptions for leaders—in order to provide the stabilizing locus of institutional memory and opportunity for creativity. As individuals transfer into a new long-term position, they spend several weeks as "contributor" doing a tacit data dump—including frustrations about process, data, and ideas—into their organization's share of the Atrium files. They would also spend up to half of that time in virtual simulations with other members across organizations, creating or recreating problematic situations for collaborative solutions. Noncritical identifying tags may be masked to encourage honesty, and then the knowledge is added to the central pools. While everyone routinely cycles through the Atrium to download experiences, every so often—perhaps once every six months—each person also spends a week or so as a "producer." In this role, individuals set up questions and look at the data for the benefit of their organization and the entire community. As "consumers," all Atrium organization members can tap into not only what contributors have input but also into the results of these simulations. Furthermore, they can apply simple language queries, data mining, or other applications to expanding pools of knowledge created by the producers in order to guide their future processes.

Explicit and implicit comparative institutional knowledge thus becomes instinctively valued and actively retained and maintained for use in ongoing or future operations. Frontline interrogators, for example, would try to define the kinds of questions they or people like them would like to have answered. They would also look at new data with an eye to what kinds of questions that data might answer. The goal is for them to understand what knowledge is out there beyond what they have asked so far and to see new patterns they had not thought of before. Visualization is exceptionally powerful in this process. The effect is a broader understanding of other organizational dilemmas and approaches to solutions.

This commonality in experience permits easier cycling through collaborative task forces as well—the kind of coordinated behaviors critical for crisis and deployed operations and so dependent on trust and interactor knowledge. For the members of a joint operations system, this cycling needs to be both routine and of value to their own work in their owning organization. Hence, interrogators in Iraq as well as supply reservists in California would need to find something of use for them when they share their tacit experiences in the joint Atrium. Once operations begin, each organization leaps into surprise-response activities. Through the Atrium, member organization decision makers are more aware of the roles and likely actions of other agencies in their grand alliance. They are also more likely to know many of their corresponding actors in other organizations through the simulations.

Figure A.1 shows the joint Atrium model notionally as the underlying space linking the joint organizations. It has three broad sections: the Atrium itself, the core composed of the jointly operating organizations, and the task forces deployed out of these organizations.

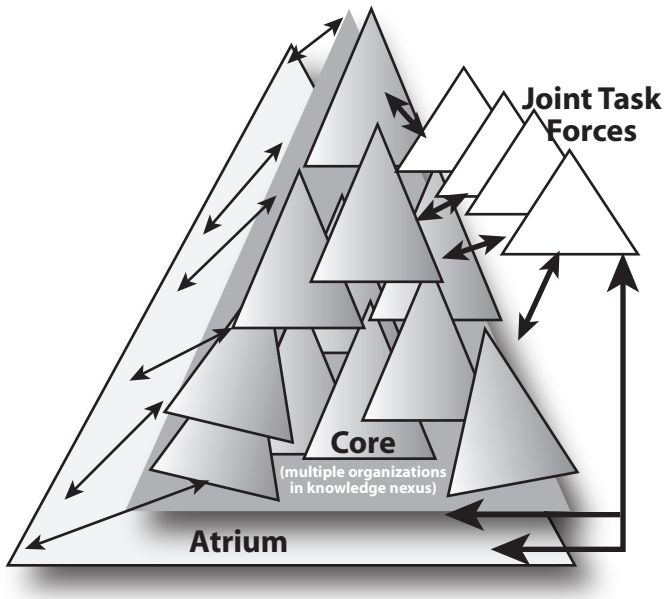

Figure A.1. Joint Atrium model. (Based on original model development in Chris C. Demchak, "'Atrium'—A Knowledge Model for Modern Security Forces in the Information and Terrorism Age," in *Proceedings of the First Annual NSF [National Science Foundation]/NIJ [National Institute of Justice] Symposium on Intelligence and Security Informatics*, Tucson, Arizona, 2–3 June 2003 [Heidelberg: Springer-Verlag, January 2003], 223–31; and Demchak, "Technology and Complexity: The Modern Military's Capacity for Change," in Conrad C. Crane, ed., Transforming Defense [Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2001].)

Note

1. Ikujiro Nonaka and Hirotaka Takeuchi, "A New Organizational Structure," in *Knowledge in Organizations,* ed. Laurence Prusak (Boston: Butterworth-Heinemann, 1997), 99–133.