Intelligence Reform: The Logic of Information Sharing

CALVERT JONES

A cornerstone of US intelligence reform is 'information sharing' as a means of adapting to contemporary security challenges. It was a central recommendation of the 9/11 Commission, reflected in the wide-ranging 'Information Sharing Environment' mandated by the Intelligence Reform and Terrorism Prevention Act of 2004. Yet the underlying logic of information sharing for intelligence reform has received little attention. Drawing on information and communications theory, this paper critiques the logic by highlighting problems of sense-making and interpretation overlooked amid the scholarly enthusiasm for an intelligence 'culture of sharing'. With their impersonal, technical, and highly bureaucratic approach, today's reforms may favor the flow of information and its sheer volume at the expense of the context and analytic tradecraft that render it meaningful, actionable intelligence. For effective information sharing, the paper suggests reformers pay more attention to the socio-technical environment of analysis when interpreting ambiguous, uncertain information.

INTRODUCTION

'Information sharing' is a cornerstone of the American strategy for intelligence reform. It is conceived as a central means of adapting to contemporary security challenges, in particular from transnational non-state actors such as the evolving Al Qaeda threat. According to the influential report of the 9/11 Commission, the intelligence community is ill suited to these 'loosely affiliated but networked adversaries'.[1] A fragmented assortment of lumbering, sluggish bureaucracies, in the Commission's analysis, the community was built for the Cold War, when information was scarce and the enemy slow-moving and predictable. Today's rapidly evolving threats, by contrast, call for 'quick, imaginative, and agile responses'.[2] To develop this capability, information must be shared more widely. Information should be set loose from the outdated need-to-know standard for sharing that

Intelligence and National Security, Vol.22, No.3, June 2007, pp.384 – 401
ISSN 0268-4527 print 1743-9019 online
DOI: 10.1080/02684520701415214

constricted its flow during the Cold War. Formal information sharing procedures should be drafted, and information itself made as 'shareable' as possible. In these ways, a 'smart' government will be able to '*integrate* all sources of information to see the enemy as a whole'.[3] Information sharing is thus a chief recommendation, championed as the nervous system of a more collaborative, networked intelligence community better suited to today's threats.

Amid this enthusiasm, the logic of information sharing for intelligence reform has not been fully examined. It was accepted, largely uncritically, as the basis for the Intelligence Reform Act of 2004, which instructed the President to create an 'Information Sharing Environment' (ISE) as a new framework for intelligence – a mixture of policies, procedures, and technology for the 'sharing of terrorism information' among 'all appropriate Federal, State, local, and tribal entities, and the private sector'.[4] The Act established an 'Information Sharing Council' and new position of Program Manager, improbably tasked with ensuring information sharing among these disparate actors, extending well beyond the intelligence community itself. The new Director of National Intelligence is similarly expected to ensure that information flows freely, unencumbered by information 'stovepipes'. A 'culture of information sharing' is held to be a necessary and proper adaptation to the current security environment.[5]

Although intelligence scholars have studied certain elements of this reform agenda, especially the 'intelligence czar' concept of centralization and radical organizational overhaul, few have flagged information sharing itself as a proposal in need of further analysis.[6] Echoing the revolution in military affairs literature, several have supported aspects of its core logic as a natural evolution of 'intelligence in the information age', an important step forward to counter diffuse transnational terrorism.[7] Critical debate has been confined largely to the consequences for civil liberties of further information sharing, and the panoply of cultural, legal, and technological obstacles standing in the way. Flaws in the underlying logic of the proposal, however, as well as the drawbacks to its implementation for intelligence analysis have been largely overlooked. On one level, updating information systems such that databases can communicate, letting analysts, border patrol agents, immigration personnel, and others search for names of terrorist suspects and other items amid wider swathes of information, is not particularly controversial and greatly needed.[8] In the area of analysis, further information sharing may well be crucial. But the vastly conceived 'Information Sharing Environment' represents more than technical adjustments and organizational reworking. With its strong flavor of technological determinism, it suggests a new conceptual framework for intelligence, one based on uncertain assumptions about the nature of the current threat environment and the power of 'information' itself to address it.

Drawing on information and communications theory, this paper explores the logic of information sharing for the improvement of intelligence analysis. The approach is familiar to students of the field: Roberta Wohlstetter famously applied information theory, which took shape in the late 1940s around the same time as the intelligence community itself, to her analysis of the Pearl Harbor intelligence failure.[9] This paper similarly draws out problems of interpretation and sense-making that have not been fully addressed in the enthusiasm to foster a culture of sharing. Situating the logic historically, the paper highlights enduring assumptions about how much information was needed to avoid another surprise attack in the conceptual underpinnings for intelligence after Pearl Harbor. With this legacy, and the objective to be as flexible and adaptable as our adversaries are thought to be, today's reforms may privilege the *flow* of information and its sheer volume at the expense of the context and analytic tradecraft that render it meaningful, actionable intelligence. To address these problems, the paper suggests improving the socio-technical environment of analysis by diversifying tools of interpretation and cultivating connectivity in ways that help analysts make sense of information.

INTELLIGENCE AFTER PEARL HARBOR

The conceptual underpinnings for a US intelligence community with expanding needs for information grew out the Pearl Harbor experience of surprise attack. In the months leading up to 7 December 1941, crucial bits of information were scattered among Army and Navy intelligence in Hawaii, their counterparts in Washington, the State Department, the White House, and Ambassador Grew's office in Tokyo, among other players. According to investigators, Army and Navy intelligence personnel in Honolulu were not sharing information regularly, nor was Washington sharing what it knew with the military commands in Hawaii to a sufficient degree.[10] This analysis of the Pearl Harbor intelligence failure – with inadequate coordination of information considered a root cause – prompted the establishment of a Central Intelligence Agency (CIA) in 1947 to achieve better information sharing and integrated analysis. As the intelligence community evolved, persistent memories of Pearl Harbor put preventing another surprise attack at the core of its mission. According to several intelligence scholars, the event had the unfortunate legacy of leaving intelligence with highly unrealistic goals, in particular the absolute prediction of events and the elimination of surprise altogether.[11]

How was the new intelligence community expected to achieve these goals? In his highly influential *Strategic Intelligence for American World Policy*, Sherman Kent described intelligence in 1949 as a social science

research-based endeavor requiring vast amounts of information to prevent being 'caught off balance by an unexpected happening'.[12] In his framework, intelligence can be understood as a specific kind of knowledge, divided into three general categories: the basic descriptive element (descriptions of the world), current reportorial element (descriptions of day-to-day *changes* in the world), and the speculative-evaluative element (predictions about how the world *will* change). For example, the basic descriptive element of intelligence consists of 'encyclopedias' that compile information in the following manner:

> Take the chapter on 'people' for instance. Here one finds the latest population estimates – breakdowns according to age, sex, consumer groups, regional distribution, and so on . . . one also finds sections on social structure and social attitudes, with analyses of the groupings of society – ethnic groupings, minority groupings, religious groupings, clubs, lodges, secret societies, etc., and how these groups and their members feel about God, education, filial piety, bodily cleanliness, capitalism, love, honor, and the stranger.[13]

Chapters are not finished until 'knowledge has been assembled to answer these questions, and many others'.[14] As Kent takes the reader through the quantities of information necessary for effective intelligence, he makes the importance of such quantities clear: 'If he has not these data, strategic intelligence has failed.'[15] Indeed, the encyclopedias of the basic descriptive element are the 'groundwork which gives meaning' to the other two categories, the current reportorial and speculative-evaluative elements. The more information is assembled and shared, the better equipped analysts are to make accurate predictions. Kent's framework left intelligence with very broad assumptions about the volume of information necessary for the analytic branch to fulfill its duties, chief among them being the prevention of another surprise attack. Similarly broad and unproven assumptions support today's enthusiasm for 'information sharing' to prevent another terrorist attack.

Although Kent's views were powerful, especially when he was Chair of the CIA's Board of National Estimates from 1952 to 1967, they were not accepted uncritically. In an early review of Kent's book, Wilmoore Kendall called the approach 'crassly empirical', accumulating great quantities of information without theoretical guidance.[16] He argued that Kent embodied a wartime view of intelligence, characterized by a 'compulsive preoccupation with *prediction*, with the elimination of ''surprise'' from foreign affairs' rather than seeking opportunities to influence the world through American policy. He worried that the practical effect of Kent's conception would be to make analysis 'a matter of somehow keeping one's head above water in a tidal wave of documents, whose factual content must be ''processed'''. These

same risks complicate the contemporary logic of information sharing and the mechanisms for its implementation, though they have not been acknowledged and discussed in sufficient detail.

INFORMATION AS INTELLIGENCE

Fifty years after Kent struggled to define intelligence as a specific kind of *knowledge*, Bruce Berkowitz and Allan Goodman would preface their work on how to adapt to the post-Cold War security environment with the declaration: 'If one theme runs through this book, it is *intelligence is information*.'[17] To deal with an uncertain panoply of rapidly evolving threats, they argue, intelligence agencies must become 'flexible information integrators', capable of accessing 'information, wherever it may reside, whenever the need arises'.[18] The free flow of information will make it possible for analysts to cope with this uncertainty, assigning and reassigning themselves to problems as needs change. A similar theme runs through other scholarship on intelligence reform and the role of information technologies. In *Reshaping Intelligence for an Age of Information*, for example, Gregory Treverton recommends wider information sharing because 'intelligence's business is information, not secrets'.[19]

This concept of intelligence as information emphasizes open sources, collaboration with actors outside of intelligence, reduced hierarchy, and, of course, extensive information sharing to confront a diffuse, uncertain threat environment. For a state to combat 'netwar' adversaries, for instance, John Arquilla and David Ronfeldt argue for a more networked, fluid intelligence community.[20] Robert Steele proposes reducing the emphasis on secrecy and bureaucracy in favor of a 'virtual intelligence community', with the free flow of information giving rise to 'smart nations'.[21] The Markle Foundation Task Force on National Security in the Information Age has also promoted intelligence refashioned into a more open, decentralized network of information sharing.[22] Although these approaches to reform vary in the details, they have in common a dedication to the free flow of information in a more flexible networked infrastructure.

Influenced by this trend, perhaps, the 9/11 Commission invokes a similar logic. In its narrative of why we were surprised, the inadequacy of information sharing is a pervasive theme. Due to concerns about security 'bordering on paranoia', information in the intelligence community was 'compartmentalized' and sharing discouraged.[23] Guidelines regulating the flow of information under the Foreign Intelligence Surveillance Act (FISA) 'further blocked the arteries of information sharing' between the CIA and FBI, and within the FBI itself between the intelligence and criminal investigation divisions.[24] Faced with diffuse, transnational threats, the

Commission argues, the Cold War's need-to-know standard for information sharing, increasingly vilified, is no longer appropriate.[25] It calls for a 'need-to-share' culture of integration to take its place, with bureaucratic information sharing procedures drafted and information converted into its 'most shareable' form for widespread distribution.

These recommendations are the foundation for the sweeping 'Information Sharing Environment' in the reforms underway. Their logic – if deliberately oversimplified – holds that greater information flow will generate the diverse, competitive analysis necessary for the intelligence community to adapt to a complex, rapidly evolving threat environment, to see its elusive adversaries 'as a whole'. Given the far-reaching influence of Kent's intelligence model, with its sprawling assumptions about the need for information, it is not surprising that information sharing should be conceived as the way forward after another surprise attack. Yet the problems of interpretation and sense-making posed by these reforms require further attention if meaningful information sharing is to take place.

THE EROSION OF CONTEXT

The 9/11 Commission's information sharing proposal reflects a certain conception of the nature of information transmission, one based on the language used to describe communication. In 1979, Columbia professor Michael Reddy published a paper arguing that communication is overwhelmingly described in the English language through the use of a 'conduit metaphor'. In the metaphor, language accomplishes communication by physically transferring ideas and thoughts from one person to another through a conduit. A speaker 'inserts' these ideas into words, sends them through the conduit, and a listener 'extracts' or 'unpacks' the meaning out of the words as received, without great effort. Evidence from everyday English demonstrates the metaphor's pervasiveness (phrases such as 'Try to *get* your thoughts *across* better', 'None of Mary's *feelings came through* to me', and 'You have to *put* each concept *into* words').[26]

To draw out the conduit metaphor's implications for the design of communications technologies, Reddy describes an alternative model, the 'toolmaker's paradigm', based on insights from the mathematical information theory developed by engineers Warren Weaver and Claude Shannon in the late 1940s. Information theory envisioned an information source (speaker) which selected a message to send; a transmitter that associated the chosen message with signals systematically through a code; a communication channel that transmits the signals; a receiver that uses the same code to reconstruct a message from the signals; and the final destination (listener) for the reconstructed message.[27] A message is not 'sent' from person to person in

this model; it must be reconstructed on the basis of the signals and the receiver's local set of tools for interpretation. In Reddy's 'toolmaker's paradigm', listeners must work to make sense of communicated signals using the tools available in their local context, rather than effortlessly unpacking meaning out of 'sent' messages.[28]

The 9/11 Commission's optimism about the benefits for intelligence analysis of a vastly increased 'flow' of information reveals an undue reliance on the conduit metaphor. The greater the flow, according to this logic, the better equipped intelligence will be to predict and prevent future terrorist attacks. Formal procedures, routines, and incentives to share are expected to generate a 'smart' government by maximizing the flow of information. In its report, the Commission endorses the Markle Foundation's strategy of a 'culture of distribution' in the intelligence community with 'distributable products . . . created at the outset', without heeding the Foundation's warnings about information overload.[29] Unfortunately, the Commission's logic assumes problematically that the meaning and significance of information will flow through the conduits of information sharing routines in a more networked intelligence and national security community. Far from a 'smart' government, however, the outcome may just as easily be a swamped, confused government, overwhelmed by Kendall's 'tidal wave of documents'.

Even more worryingly, the Commission privileges this bureaucratized flow of information largely at the expense of the *context* that makes the information itself meaningful to analysts. Intelligence information is typically very ambiguous, with several plausible interpretations. Understanding the context of information, therefore, is a fundamental tool of analysis. It is one reason for housing both collection and analysis capabilities in the CIA. Intelligence collectors are most familiar with the context of information gathered – its reliability, timeliness, relationship to other information, and so on. Hesitant to distribute it widely for legitimate security reasons, they are more inclined to contextualize it for analysts they know and trust.[30] Yet maximizing information flow is so important in the Commission's view that collectors and analysts are now required to make information as 'shareable' as possible for immediate dissemination into a vaguely defined Information Sharing Environment with unknown, untested recipients.

The Commission improbably proposes standardized routines to ensure that a report's 'data be separated from the sources and methods by which they are obtained', using tear-lines and other techniques to redact classified material as it is processed. 'Intelligence gathered about transnational terrorism', it recommends, 'should be processed, turned into reports, and distributed according to the same quality standards, whether it is collected in Pakistan or in Texas'.[31] As analysts and collectors are pressured to commoditize their ambiguous, sensitive information 'according to the same quality standards',

they will understandably generate information stripped of context. Ironically, in its 'most shareable' form, this information may not be meaningful to its large number of recipients. It will be information, already indefinite and nebulous, with context sacrificed in the name of information flow.

This erosion of context is particularly problematic given that the Commission's own report suggests the failure to grasp the significance of information and act on it was more important than the lack of information sharing per se. For example, in July 2001, an FBI agent in Phoenix wrote a memo warning about the 'possibility of a coordinated effort by Usama Bin Ladin to send students to the United States to attend civil aviation schools'.[32] The agent urged the intelligence community to examine his theory and track visa status on flight school applicants. Although this memo was shared with the FBI's Radical Fundamentalist Unit and CIA's Bin Ladin Unit, according to the report, no action was taken. The deluge of decontextualized information unleashed by the proposed 'culture of distribution' may well meet with the same fate unless ways to interpret and manage it are given more emphasis.

Another example of information shared without great consequence is the FBI's receipt of the names of two suspected terrorists in August 2001, future hijackers Khalid al Mihdhar and Nawaf al Hazmi. The Commission rightly criticizes the CIA for its failure to share these names earlier with the FBI and State Department, particularly when it found that the latter had entered the United States in March 2000 and that both had US visas. Interestingly, the Commission also asserts that, in January 2001, when a terrorist associated with the *Cole* bombing was linked to these two – making them even more suspicious – the CIA still did not pass on these names. Yet former DCI George Tenet and Cofer Black, former chief of the CIA's Counterterrorism Center, testified otherwise, claiming the information *was* available to the FBI at that time. Although *when* this information was distributed is a key point for the Commission, at no time did the CIA or the FBI judge it to be very important amid the mass of incoming threat reports. Even when the FBI did get it for certain in August 2001, the search for Mihdhar was given a low priority and proceeded slowly.[33] So 'information sharing' did not lead the FBI to recognize the significance of this information and act appropriately.

Roberta Wohlstetter's classic analysis of the Pearl Harbor intelligence failure makes the same point, further undermining the wisdom of conduit metaphor-based intelligence reform. Although warning signals were scattered in different agencies, she does not conclude that a greater flow of information would have made a difference. 'It is doubtful', she argues, 'that the local commanders would have been further enlightened if they had had the pieces of the puzzle that were denied them.'[34] Indeed, 'it would have created endless confusion if Washington had tried to relay all available signals to the

overseas commands'.[35] In her analysis, the profound difficulties in separating signals from noise, sorting relevant from irrelevant information, explain the Pearl Harbor experience better than failures to share information. In addition, the more information was shared without context – in its 'most shareable' form – the more often interpretation went astray, with noise diluting the significance of relevant signals. Even the infamous 'war warning', in which Washington wanted to indicate that war with Japan was imminent, was so watered down as to make its impact negligible in Pearl Harbor.

INFORMATION AS POWER

Contemporary theory on the concept of the 'information age' also highlights problems in the logic of information sharing for intelligence reform. These theorists have explored what is meant by 'information' itself, seeking to explain its current power as a guiding light of reform and evolution in so many fields of endeavor. One theorist, Geoffrey Nunberg, who has studied the sense of 'information' evoked by information age manifestos and reform agendas, describes a tendency to imagine the 'content' of information as separate from and superior to that which 'contains' it.[36] In these manifestos, information's 'content is a noble substance that is indifferent to the transformation of its vehicles', liberated by technology from the trappings of the physical world.[37] As John Perry Barlow famously argued against attempts to 'bottle' or control information in the digital age, 'Information wants to be free'.[38] The theorist describes this abstraction as 'information in the large', disconnected from the particular situations it is *about* as well as the people who are *informed*. Decontextualized and fungible, it is thought capable of being 'liberated and manipulated as a kind of pure essence'.[39] It no longer signifies the material that leads people to inform themselves through instruction and learning of their own initiative. Rather, information in the large 'resituated the agency of instruction in the text and its producers, and reduced the reader to the role of a passive consumer of content'.[40]

An overzealous information sharing regime risks turning analysts too into the passive consumers of 'information in the large', their work reduced to processing, commoditizing, and distributing as much of its 'content' as possible. Partly because such content is considered fungible, its value arises from how 'shareable' it is made to be. Instead of personal ingenuity, expertise, critical skill, and level of concentration on the analyst's part, factors routinely emphasized by intelligence scholars, good analysis is thought to be a function of *how much* information is accessible. 'The biggest impediment to . . . a greater likelihood of connecting the dots', the Commission asserts, 'is the human or systemic resistance to sharing information.'[41] Experiences, background, education, willingness to doubt – all the tools

analysts bring to bear in their work pale in comparison to the 'resistance to sharing information'. As Kendall wrote of Sherman Kent's calls for more and more information, 'The course of events is conceived . . . as a tape all printed up inside a machine, and the job of intelligence is to tell the planner how it reads.'[42] So long as all the information is at their fingertips, the logic suggests, analysts will be able to 'tell the planner how it reads'. Indeed, the Commission writes of the Cold War's more restricted need-to-know standard for information sharing as if, were it gone, analysts would be all-knowing creatures.

Not only could analysts be quite overwhelmed by a 'culture of information sharing', however, but they will still 'need to know' what they are after in the mass of data available in digital form. Lifting strict need-to-know criteria for access will not solve basic problems of information search and retrieval, including how a user arrives at an information need, how well formulated the need is, how it is processed based on a system's indexing of information, and how well results match.[43] In fact, if search algorithms are improperly designed, with low recall and other limitations, analysts could be left with far less information than they might otherwise have accessed, had they used more diverse search techniques spanning both people and technology. Moreover, depending on implementation, indexing schemes that organize information in the various intelligence databases might be standardized to promote interoperability and integration. If information is indexed, presented, and retrieved all in the same way, processed 'according to the same quality standards' as the Commission proposes, diversity in intelligence analysis could suffer, and imagination wane – even though the Commission also proposes 'institutionalizing imagination'.[44] With analysts drawing conclusions based on the same presentation of information, the herd mentality problem identified by the WMD Commission may worsen.[45]

Psychologists studying the craft of analysis have also argued against a data-driven approach to interpreting the ambiguous information involved in intelligence. For example, Richard Heuer investigated the relationship between amount of information available to an expert, accuracy of his predictions, and his level of confidence in those predictions.[46] He found that once experts felt they had the 'minimum information necessary' to make a judgment, more information did not increase the accuracy of these judgments. It did increase their confidence in their own estimates, and sometimes made them overconfident. This tendency would exacerbate another problem noted by the WMD Commission, the failure to explore alternative explanations of ambiguous information, if analysts have unwarranted confidence in their own views. Instead of a 'mosaic approach' calling for as much information as possible – information in the large – Heuer promotes conceptually driven analysis, which focuses on diversifying the

mental models analysts use to filter and interpret information. Rather than 'passively review information flowing through the in box', analysts should seek out evidence that disproves various hypotheses, bringing them closer to accurate assessments.[47]

In the new framework, analysts are nonetheless portrayed as 'empowered' merely by virtue of their access to vast amounts of information.[48] In their concept of information age intelligence, Berkowitz and Goodman imagine analysts 'assigning themselves' to problems, assembling and reassembling themselves in a 'new configuration' as needs change, as if fruitful collaboration were automatic as long as information is available.[49] The scholars are, of course, aware of the signal to noise ratio, the difficulties in sorting relevant signals from irrelevant noise in vast amounts of information. The Markle Foundation reports, in particular, stress the importance of filtering information.[50] But the Commission makes it clear that 'connecting the dots' amid the noise of so much information is largely a matter of eliminating obstacles to information sharing. Unfortunately, the organizational ability to make sense of information and interpret it innovatively does not necessarily, or even usually, follow from greater information flow.

MAKING SENSE OF INFORMATION

Organizational research increasingly demonstrates that the more information is available to many players, the more decisive is the strategic advantage of those with superior means of interpretation, rather than access to more information.[51] This literature emphasizes analysts' physical context; the social setting of their work; exposure to alternative conceptual approaches that value information differently; availability of diverse search and analysis tools; and informal, low-risk communication allowing tentative ideas to be aired.[52] Routine, standardized patterns of interaction, stability, and limited sources of challenge or variety tend to inhibit the ability to interpret information innovatively. The Commission's proposal to 'find a way of routinizing, even bureaucratizing, the exercise of imagination' on information that is shared – through standardized routines and bureaucratic procedures no less – may therefore not be advisable.[53] Instead, methods to improve the socio-technical environment of analysis should build on insights from this literature, avoiding where possible the kind of bureaucratic standardization that stifles innovation.

For example, an ethnography of arbitrage traders in a Wall Street trading room underscored the role of the manager in cultivating an 'interpretative community' for effective analysis of large amounts of market information.[54] Not unlike aspects of intelligence analysis, arbitrage involves both 'pattern recognition' (matching data to existing models) and 're-cognition' (making

unanticipated associations). According to the study, the manager deliberately influences the social configuration and communication patterns of the room to facilitate interpretation and sense-making, not through daily, predictable routines of information sharing but through ad hoc, informal adjustments. While each desk applies a distinct evaluative principle to select out and assign value to certain information, desks are positioned near one another to promote informal information exchange and discussion of competing interpretations. The manager rotates analysts around to introduce variety and challenge, exposing them to heterogeneous value frameworks for assessing information, so they are less likely to fall into the habit of using only one approach or data set. Although the intelligence community's practice of 'competitive analysis' is intended to promote this kind of analytic diversity, its bureaucratic formality and routine quality may diminish its effectiveness and the credibility of its estimates.

Research on how high-reliability organizations, in particular, function under conditions of high stress, high stakes, and low tolerance for failure could also yield insights for improving connectivity in intelligence analysis, without sacrificing diversity and context. Social scientists studying an aircraft carrier found that the officers and crew members rotated in and out of different ships, positions, and responsibilities, facilitating the complex coordination of activity on the carrier despite the high turnover.[55] The introduction and reintroduction of newcomers learning the ropes led the researchers to compare the ship to a school aimed at teaching the complex, interrelated activities involved in overall coordination and adaptation to changing circumstances. This circulation of people built a base of shared experience, while also exposing crew members to a variety of approaches they brought to bear in their work.

Significantly, in the 9/11 Commission's discussion of late leads, many of the people who came closest to grasping the importance of information and acting on it were analysts working outside of their home agency.[56] For example, amid the flood of threat reports in mid-2001, it was a CIA official detailed to the FBI's International Terrorism Operations Section who had the insight to look again at the key information concerning the January 2000 meeting of suspected terrorists in Kuala Lumpur. Although 'John', perhaps a regional analyst, was deeply involved in Malaysia and did not think to inform the FBI of the names of these future hijackers, he had the 'good instinct' to ask another analyst, 'Mary', to take a look. 'Mary' was an FBI analyst detailed to the CIA's Bin Ladin unit. Unlike 'John', she 'immediately grasped the significance of this information'. She arranged for Mihdhar and Hazmi to be put on the State Department's TIPOFF list in August 2001, and initiated an FBI search for Mihdhar.[57]

By activating domestic agencies in the search for Mihdhar and Hazmi, FBI analyst 'Mary' did immediately what the CIA had failed to do for almost two

years, since early 2000 when its analysts learned of their terrorist associations and US travel but did not alert these agencies. At that time, the CIA lost their trail in Bangkok, and understandably moved on to other pressing issues in foreign intelligence, playing a kind of 'zone defense'. Despite the high level of noise in mid-2001, 'John' and 'Mary' focused on the right signals, and they stand out because of their external appointments and relationships with people outside their home agencies. Their exposure to diverse perspectives and capabilities in intelligence, like the rotating crew members on the aircraft carrier, may have improved their ability to piece together the relevant clues and take appropriate action.

Research should explore how to apply similar techniques to the environment of intelligence analysis, many of which are well developed in the literature on organizational innovation and learning in conditions of uncertainty. Many scholars have encouraged using technology to make sense of information, in addition to providing access to it, through social network analysis, exploratory modeling, visualization, and other methods.[58] These tools should be situated in the larger contextual environment of intelligence and its collective mission. Managers should see their own roles as cultivating interpretative communities, blending diverse technical tools with social and physical configurations that promote meaningful connectivity. For example, they might deliberately expose analysts to alternative interpretative frameworks, introducing them into new collaborative relationships with other analysts they will like and trust, with their own approaches, data sets, and resources. Another strategy would involve online information exchanges, in which analysts with pseudonyms could air tentative, or politically unpopular, ideas without the fear of being wrong or risking their careers.

THE LOGIC OF INFORMATION SHARING

In the logic of information sharing, intelligence reformers expect the free flow of information to stimulate a robust marketplace of ideas, encouraging diverse, innovative analysis appropriate for dealing with more complex, rapidly evolving threats. Such threats are held to be fast-moving and elusive, requiring broader information sharing to render intelligence agencies just as dynamic and adaptable. This paper does not argue against information sharing in principle; analysts need information to do their jobs, of course, and more collaboration and openness may well be essential. It does argue that the logic and proposed mechanisms of sharing, based on problematic assumptions about 'information' and the advantages of its free flow through network infrastructures and bureaucratic routines, are not sufficiently developed. Wider information sharing does not necessarily lead to a more agile, innovative intelligence capability. While embracing Sherman Kent's belief in

the great volume of information needed to avoid surprise, the logic glosses over the role of interpretation in analysis, so fundamental in his theory. He warned of the 'irresponsibility of intelligence', were it to become 'satisfied with dishing up information without trying to make sense out of what appears senseless'.[59] This paper also cautions against placing too much faith in information, if the human ability to make sense of it is overlooked and context disregarded.

Reformers might argue they intend to preserve the context of information, and that making information 'shareable' does not imply stripping it of context. The very point of these reforms, they might respond, is to ensure that more information *with* context is available to analysts, since the security concerns that 'sanitized' it into obscurity no longer apply.[60] Not only will these security concerns persist, however, undermining efforts to routinize information sharing as discussed in this paper, but it is not clear they should be dismissed so readily. Indeed, the Commission describes today's threats as 'less visible', networked adversaries hidden in the fabric of our own society, suggesting security concerns might be heightened in such an environment.[61] It recommends broader information sharing precisely because information warning of an attack could be anywhere, due to the decentralized character of these adversaries who could themselves be anywhere. Ironically, the reasons leading these reformers to promote further information sharing also underscore the security concerns that have traditionally limited it. In addition, if terrorists are as adaptable as security experts believe, what will prevent them from adapting to newly relaxed security protocols, dismissed in the name of information sharing?

Another assumption in this logic deserving further scrutiny is the image of the current threat environment as fragmented, diffuse, and decentralized. This assumption may have led rather too quickly to the conclusion that intelligence must adapt by itself, evolving into a more decentralized network of information sharing. As part of the reforms underway, the Bin Laden Unit at the CIA was disbanded in July 2006, reportedly reflecting this view.[62] But it is not clear what role Bin Laden and his Al Qaeda network play in terms of leadership over the evolving jihadist threat.[63] Even if their role is more inspirational than operational, it may not be wise to neglect their possible importance based on tenuous, underdeveloped assumptions about the threat environment. Michael Scheuer, terrorism expert and former chief of the Bin Laden Unit, criticized the change as premature, arguing that it succumbed to Al Qaeda's stated strategy of 'spreading out' security and intelligence forces.[64] This strategy, in his view, aims to obscure the significance of genuinely important, professional, and talented leaders like Al Qaeda, shielding them from analysts' attention through the distraction of lesser, more amateurish players dispersed around the world. Thus, the image of a

fragmented, diffuse threat environment, frequently invoked in the logic of information sharing for intelligence reform, should be examined in greater depth.[65]

Reformers will need to address the assumptions and trade-offs in their logic more thoroughly, weighing information sharing and a 'culture of distribution' against, for example, persistent security concerns that remain legitimate and perhaps heightened after the end of the Cold War. For meaningful information sharing to take place, moreover, they will need to look beyond the flow of information. Depending on how information sharing imperatives are understood and implemented, the costs to analysis of further integration might include a loss of contextual richness; confusion and indecision; reduced diversity and imagination; and over-reliance on information access at the expense of analytic tradecraft. The Information Sharing Environment is vaguely defined, and its first Program Manager, John Russack, resigned after six months in frustration after attempting to design and implement it from above. The field is open for intelligence managers at all levels to experiment with strategies to address these costs. Further research should explore how to map methods drawn from innovation in the private sector to high-reliability organizations, attempting to match the intelligence community's needs for innovation with its national security mission.

NOTES

1 National Commission on Terrorist Attacks on the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States: Official Government Edition* (Washington, DC: U.S. G.P.O. 2004) p.87.
2 Ibid. p.399.
3 For these excerpts, see information sharing recommendations in ibid. pp.416–19.
4 Intelligence Reform and Terrorism Prevention Act of 2004, Title I, § 1016(a)–(f).
5 Ibid (d)(3).
6 See, for example, the following two edited volumes of scholarly reactions to the reforms: Jennifer E. Sims and Burton Gerber (eds.) *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press 2005) and Peter Berkowitz (Ed.), *The Future of American Intelligence* (Stanford, CA: Hoover Institution Press 2005). Judge Richard Posner has also criticized the Commission's embrace of greater centralization in *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (Stanford, CA: Rowman & Littlefield Publishers, Inc. 2005).
7 See, for example, Gregory Treverton, 'Reshaping Intelligence to Share with ''Ourselves''', Canadian Security Intelligence Service, *Commentary*, No.82, 16 July 2003; and Michael Herman, 'Counter-Terrorism, Information Technology and Intelligence Change', *Intelligence and National Security* 18/4 (2003) pp.41–58.
8 See the Markle Foundation Task Force reports, *Creating a Trusted Information Network for Homeland Security* (New York, NY: Markle Foundation, 2003) and *Protecting America's Freedom in the Information Age* (New York, NY: Markle Foundation, 2002).
9 Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press 1962).
10 See Wohlstetter, *Pearl Harbor* and Loch Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven, CT: Yale University Press 1996).

11 See Rhodri Jeffreys-Jones, *The CIA and American Democracy* (New Haven, CT: Yale University Press 2003) p.249; Abram Schulsky and Gary Schmitt, *Silent Warfare: Understanding the World of Intelligence* (Dulles: Brassey's, Inc. 2002) pp.162–4; and Wilmoore Kendall, 'The Function of Intelligence', *World Politics* 1 (1949) pp.549–50.
12 Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press 1949) p.39. Because of his considerable influence over how intelligence was conceptualized in these early years, Kent is considered one of the US intelligence community's intellectual 'founding fathers'. His key role is reflected in the CIA's official training body for analysts, the Sherman Kent School for Intelligence Analysis. A veteran of the Office of Strategic Services, the precursor to the CIA, and history professor at Yale University, Kent promoted a conceptual framework for intelligence that has remained a powerful and far-reaching, if not unchallenged, authority on the subject.
13 Ibid. p.13.
14 Ibid. p.17.
15 Ibid. p.14.
16 For this comment and those that follow, see Wilmoore Kendall, 'The Function of Intelligence', *World Politics* 1 (1949) pp.549–50.
17 Bruce Berkowitz and Allan Goodman, *Best Truth: Intelligence in the Information Age* (New Haven, CT: Yale University Press 2000) p.x.
18 Ibid. pp.82, 63.
19 Gregory Treverton, *Reshaping Intelligence for an Age of Information* (Cambridge: Cambridge University Press 2001) p.17.
20 John Arquilla and David Ronfeldt (eds.) *Networks and Netwars* (Santa Monica, CA: RAND 2001).
21 Robert Steele, *On Intelligence: Spies and Secrecy in an Open World* (Oakton, VA: OSS International Press 2001).
22 See Markle Foundation Task Force on National Security in the Information Age reports (note 8).
23 *9/11 Commission Report*, p.91.
24 Ibid. p.80.
25 Ibid. p.417.
26 Michael Reddy, 'The Conduit Metaphor: A Case of Frame Conflict in our Language about Language' in Andrew Ortony (ed.) *Metaphor and Thought* (Cambridge: Cambridge University Press 1993) p.164.
27 See Warren Weaver, 'Some Recent Contributions to the Mathematical Theory of Communication' in Claude Shannon and Warren Weaver, *Mathematical Theory of Communication* (Urbana: University of Illinois Press 1964) p.16.
28 While concepts such as the subjective interpreter and role of context are emphasized in various traditions, Reddy's contribution was to show how embedded the conduit metaphor is in our language and thinking, and warn of its influence over the design and management of information and communications technologies.
29 Markle Foundation Task Force, *Creating a Trusted Information Network*, p.24. The report rightly highlights the difficulties in making sense of vast amounts of information. Unlike the Commission, it anticipates that broader information sharing could overwhelm analysts, and recommends some technical tools to assist them in this respect.
30 Of course, there is a tension between the need for multiple and competing centers of analysis to generate diverse interpretations of ambiguous intelligence – requiring broader information sharing – and analysis positioned close to collection so the information analyzed is contextualized and meaningful. However, requiring the immediate distribution of information in its 'most shareable' form, likely to be decontextualized and hard to grasp, into a vast network of untested users will probably not enhance analysis at any of these centers.
31 For these excerpts from the report, see information sharing recommendations in *9/11 Commission Report*, pp.416–19.
32 Ibid. p.272.
33 Ibid. pp.269–73, 355.
34 Wohlstetter, *Pearl Harbor*, p.226.

35 Ibid. p.131.
36 Geoffrey Nunberg, 'Farewell to the Information Age' in Geoffrey Nunberg (ed.) *The Future of the Book* (Berkeley, CA: University of California Press 1996).
37 Ibid. p.107.
38 John Perry Barlow, 'The Economy of Ideas', *Wired Magazine* 2.03 (1994).
39 Nunberg, 'Farewell to the Information Age', p.107.
40 Ibid. p.113.
41 *9/11 Commission Report*, p.416.
42 Kendall, 'The Function of Intelligence', p.549.
43 There is a large literature devoted to these problems and socio-technical solutions in the fields of information retrieval and human-computer interaction. See, for example, F.W. Furnas, T.K. Landauer, L.M. Gomez and S.T. Dumais, 'The Vocabulary Problem in Human-System Communication', *Communications of the ACM* 30 (1987) p.964.
44 *9/11 Commission Report*, p.344.
45 United States Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States: Official Government Edition* (Washington, DC: U.S. G.P.O. 2005).
46 Richard J. Heuer, Jr., 'Do You Really Need More Information?', *Studies in Intelligence* 23/1 (1979) pp.15–25.
47 Robert Jervis has also emphasized this approach to alleviate problems of misperception in making political decisions, in 'Hypotheses on Misperception', *World Politics* 20/3 (1968) pp.454–79. And Karl Popper, of course, is well known for his emphasis on proof by falsification in empirical work, ruling out false hypotheses rather than attempting to prove the truth of any one hypothesis.
48 See *9/11 Commission Report*, p.419.
49 Berkowitz and Goodman, *Best Truth*, pp.74, 82.
50 Markle Foundation Task Force, *Creating a Trusted Information Network*, p.15.
51 See, for example, John Sealy Brown and Paul Duguid, *The Social Life of Information* (Cambridge, MA: Harvard Business School Press 2000) and Richard K. Lester and Michael J. Piore, *Innovation: The Missing Dimension* (Cambridge, MA: Harvard University Press 2004).
52 In addition to the references in note 51, see Marcie J. Tyre and Eric von Hippel, 'The Situated Nature of Adaptive Learning in Organizations', *Organization Science* 8/1 (1997) pp.71–83; Daniel Beunza and David Stark, 'Tools of the Trade: The Socio-technology of Arbitrage in a Wall Street Trading Room', *Industrial and Corporate Change* 13/2 (2004) pp.369–400; and AnnaLee Saxenian, *Regional Advantage: Culture and Competition in Silicon Valley and Route 128* (Cambridge, MA: Harvard University Press 1994).
53 *9/11 Commission Report*, p.344.
54 Beunza and Stark, 'Tools of the trade: the socio-technology of arbitrage in a Wall Street trading room.'
55 Gene I. Rochlin, Todd R. La Porte and Karlene H. Roberts, 'The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea', *Naval War College Review* 40/4 (1998) pp.76–91.
56 See *9/11 Commission Report*, pp.266–72.
57 The search was, however, labeled 'routine' and proceeded very slowly. Although the Commission indicates that the FBI analyst 'Mary', working with the CIA, understood the significance of this information (p.270), it also indicates that the FBI as a whole did *not* and 'and thus did not take adequate action' (p.356).
58 See, for example, Kevin M. O'Connell, 'The Role of Science and Technology in Transforming American Intelligence' in Peter Berkowitz (ed.) *The Future of American Intelligence* (Stanford, CA: Hoover Institution Press 2005) pp.139–74; and James R. Gosler, 'The Digital Dimension' in Jennifer E. Sims and Burton Gerber (eds.) *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press 2005) pp.96–114; Alan Dupont, 'Intelligence for the Twenty-First Century', *Intelligence and National Security* 18/4 (2003) pp.15–39; and the Markle Foundation Task Force reports.
59 Kent, *Strategic Intelligence*, p.184.
60 *9/11 Commission Report*, p.417.

61 Ibid. p.399.
62 Mark Mazzetti, 'CIA Closes Unit Focused on Capture of Bin Laden', *New York Times*, 4 July 2006.
63 On the uncertainty over how much hierarchical control Al Qaeda's remaining leadership is able to exercise – operationally, logistically, and ideologically – see Kenneth Katzman, 'Al Qaeda: Profile and Threat Assessment', *CRS Report for Congress* (2005); Randy Borum and Michael Gelles, 'Al-Qaeda's Operational Evolution: Behavioral and Organizational Perspectives', *Behavioral Sciences and the Law* 23 (2005), pp.467–83; and Daniel L. Byman, 'Al-Qaeda as an Adversary: Do We Understand Our Enemy?', *World Politics* 56 (2003), pp.139–63.
64 Michael Scheuer, 'The New York Plot: The Impact of Bin Laden's Campaign to Inspire Jihad', *Terrorism Focus* 3/28 (2006) pp.6–7.
65 See, for example, Calvert Jones, 'Al Qaeda's Innovative Improvisers: Learning in a Diffuse Transnational Network', *Cambridge Review of International Affairs* 19/4 (2006) pp.555–69, for more discussion of this image and the assumptions underlying it, in particular regarding the supposed agility and flexibility of networked non-state threats in comparison to states.