

Calvert Jones
Ph.D. Student
UC Berkeley School of Information
Spring 2006 – Preliminary Project Paper

Intelligence Reform:
The Logic of Information Sharing

“One has the vague feeling that information and meaning may prove to be something like a pair of canonically conjugate variables in quantum theory, they being subject to some joint restriction that condemns a person to the sacrifice of the one as he insists on having much of the other.”

- Warren Weaver¹

I. Introduction: The Primacy of Information in Intelligence Reform

A cornerstone of the reforms underway in the U.S. intelligence community is “information sharing” as a means of adapting to contemporary security challenges and, more generally, post-Cold War uncertainty. Failures to share information figure prominently in the 9/11 Commission’s analysis of how the September 11 plotters foiled our national security apparatus, and greater information sharing through centralized control is a main recommendation. The intelligence community, it explains, is ill suited to today’s “loosely affiliated but networked adversaries.”² A fragmented assortment of lumbering, sluggish bureaucracies, it was built for that distant era, the Cold War, when information was scarce and the enemy more slow-moving and predictable. Today’s rapidly evolving threats, by contrast, call for “quick, imaginative, and agile responses.”³

To meet these challenges, in the Commission’s view, information must be shared more widely. “A ‘smart’ government,” it argued, “would *integrate* all sources of information to see the enemy as a whole.” It called for a new position, National Intelligence Director, to ensure effective information sharing throughout the intelligence community, and National Intelligence Centers to institutionalize a culture of sharing. Information should be set loose from the outdated need-to-know standard for sharing that constricted its flow during the Cold War. Formal information sharing procedures should be drafted, and information itself must be made as “shareable” as possible.⁴ Influenced by this view, the Intelligence Reform Act of 2004 instructed the President to create an Information Sharing Environment (ISE), a mixture of policies, procedures, and technology for the “sharing of terrorism information” among all “all appropriate Federal, State, local, and tribal entities, and the private sector...” The Act established a new position, Program Manager, who is responsible for information sharing among these disparate actors, and an Information Sharing Council to assist the Program Manager in overseeing the ISE. A chief duty of the new Director of National Intelligence is to ensure that information flows freely throughout the intelligence community, unencumbered by information stovepipes.⁵

Amid this enthusiasm, the wisdom of information sharing has not been seriously questioned, though observers have criticized other recommendations, particularly the “intelligence czar” concept and organizational focus of reform.⁶ Intelligence scholars have emphasized the

¹ Warren Weaver, “Some Recent Contributions to the Mathematical Theory of Communication,” in Mathematical Theory of Communication 16 (Claude Shannon and Warren Weaver, University of Illinois Press, 1964).

² Final Report of the National Commission on Terrorist Attacks upon the United States 87 (2004).

³ 9/11 Commission Report at 399.

⁴ For these excerpts, see information sharing recommendations in 9/11 Commission Report at 416-419.

⁵ Intelligence Reform and Terrorism Prevention Act of 2004, Title I, § 1016(a)-(f).

⁶ For example, former chief of the CIA’s Bin Ladin unit, Michael Scheuer, along with a number of former intelligence officers accused the Commission of introducing unnecessary and costly organizational overhauls when individuals and senior management, rather than organization, were to blame (Shaun Waterman, “Whistleblowers

importance of other potential reforms, including more human intelligence, incorporation of open sources, improved leadership and management, and a closer relationship between policymakers and intelligence.⁷ Yet few have flagged information sharing – a central component of actual reforms underway – as a proposal in need of further analysis. 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 information is hardly very controversial, providing the security protocols are in place. But the broadly conceived “Information Sharing Environment” represents more than technical adjustments and organizational reworking; it suggests a new conceptual framework for intelligence, with a strong flavor of technological determinism and uncertain consequences for the craft of analysis.

Drawing on information and communications theory, this paper explores the conceptual underpinnings for intelligence after Pearl Harbor, how “information” is conceptualized in the new framework, and the consequences of these shifts for analysis.⁸ It critiques the logic of information sharing, highlighting problems of interpretation and sense-making that have not been fully addressed in the rush to implement a “culture of sharing.” The paper situates this logic in Sherman Kent’s highly influential postwar theory of intelligence, pointing out its far-reaching assumptions about how much information was needed to avoid another surprise attack. With this legacy, and attempting to be as flexible and adaptable as our adversaries are thought to be, these reforms may privilege the *flow* of information and its sheer volume at the expense of the context that makes it meaningful. Good analysis is increasingly imagined to be a function of *how much* information is accessible, with the risk of reducing analysts into its passive consumers. To address these problems, the paper suggests improving the environment of analysis by diversifying tools of interpretation and cultivating connectivity in ways that support innovation and sense-making.

II. Intelligence after Pearl Harbor

The conceptual underpinnings for a U.S. intelligence community with increasingly expansive needs for information grew out the Pearl Harbor experience of surprise attack. In the months leading up to December 7, 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. These included reports of Japanese code burning; MAGIC intercepts showing Tokyo’s mounting desperation and frustration with the failure of negotiations; an intercepted order telling a Japanese agent in Honolulu to divide the waters of Pearl Harbor into five sub-areas; a suspicious conversation overheard between a Japanese dentist in Hawaii and a Tokyo newspaper office; and the “winds

slam 9/11 report, reforms,” United Press International, September 14, 2004). 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 (Rowman & Littlefield Publishers, Inc. 2005).

⁷ See, for example, the following two edited volumes of scholarly reactions to the reforms, emphasizing these other areas: Jennifer E. Sims and Burton Gerber (eds.), Transforming U.S. Intelligence (Georgetown University Press 2005) and Bruce Berkowitz (ed.), The Future of American Intelligence (Hoover Institution Press 2005).

⁸ Given the primacy of information in all matters of intelligence, 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. See Pearl Harbor: Warning and Decision (Stanford University Press 1962).

code” set-up hinting at Japanese preparations for war. According to investigators, Army and Navy intelligence in Honolulu were not sharing information regularly, nor was Washington sharing what it knew with the military commands in Hawaii to a sufficient degree.⁹ 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 the National Security Act of 1947.¹⁰ Responsible for “all source” analysis, the new agency was tasked with coordinating the nation’s intelligence efforts by pooling all sources of information together in one place.

Recent memories of Pearl Harbor put preventing another surprise attack through better information coordination at the core of the evolving intelligence mission, leading to what CIA historian Rhodri Jeffreys-Jones calls an “obsession with crisis prediction.”¹¹ In his view, Pearl Harbor tilted the mission of intelligence toward absolute prediction of events and the elimination of surprise. Later accusations of intelligence failure demonstrate a tendency to equate nonprediction with failure, with the CIA blamed for failing to provide exact predictions of events even when, in some cases, it did issue fairly specific warnings. For example, the CIA was charged with nonprediction in April 1948 when the assassination of a Liberal Party opposition leader in Bogotá sparked a series of riots in Colombia. The ensuing unrest surprised and unsettled the American delegation attending the Ninth International Conference of American states taking place in the city, especially with suspicions of Communist involvement in the air. Although the CIA was blamed for its failure to predict the riots, CIA Director Hillenkoetter had in fact warned of plans to interfere with the conference and harass the American delegates.¹²

Even with improved coordination, how was the intelligence community expected to go about eliminating surprise? In *Strategic Intelligence for American World Policy*, Sherman Kent described intelligence as a social science research-based endeavor with very broad and wide-ranging assumptions about how much information was needed to prevent being “caught off balance by an unexpected happening.”¹³ Because of his considerable influence over how intelligence was conceptualized in these early years, he is considered one of the U.S. 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, Kent promoted a conceptual framework for intelligence that has remained a powerful and far-reaching, if not unchallenged, authority on the subject.

⁹ See Wohlstetter, *Pearl Harbor* and Loch Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (Yale University Press 1996).

¹⁰ However, many investigators of the Pearl Harbor intelligence failure have emphasized problems other than intelligence coordination. For example, Wohlstetter argues that the mass of irrelevant “noise” prevented intelligence analysts and policymakers from recognizing the signals warning of impending attack. She also highlights U.S. under-estimation of the Japanese foe, naïve hope that negotiations would succeed, and false assumptions about Japanese decision-making, particularly that a military presence at Pearl Harbor would deter a Japanese attack and that Japan would not choose to attack because of the likelihood of defeat.

¹¹ Rhodri Jeffreys-Jones, *The CIA and American Democracy* 249 (Yale University Press 2003).

¹² Jeffreys-Jones at 53-54.

¹³ Sherman Kent, *Strategic Intelligence for American World Policy* 39 (Princeton University Press 1949).

Kent proposed that intelligence, as a specific kind of knowledge, can be 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). All three elements require voluminous information. 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...”¹⁴

How much information is necessary? An immense amount, if we must know how people feel about “filial piety, bodily cleanliness, capitalism, love” and the rest before analysis will be productive. Chapters are not finished until “knowledge has been assembled to answer these questions, and many others...”¹⁵ 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.”¹⁶ 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. Kent accentuates the point with a metaphor: assembling such quantities is necessary “so that the speculative take-off will be from the most extreme point on the runway and the flight of imagination aimed in what will prove to be the truest direction.”¹⁷ The more information, the better equipped analysts are to make accurate predictions.

At least two qualifications limit this more-is-more approach, however. First, Kent emphasizes that no amount of information can overshadow the importance of the human interpreter. “Whatever the complexities of the puzzles we strive to solve, and whatever the sophisticated techniques we may use to collect the pieces and store them,” he argues, “there can never be a time when the thoughtful man can be supplanted as the intelligence device supreme.” Only with “knowledge, wisdom, and plain horse-sense” can analysts expect to make sense of this information.¹⁸ Second, Kent is acutely aware that his view of intelligence seems to cover a “staggeringly large area of continuing human activities,” and foresees what might today be called the problem of information overload. Somewhat unconvincingly, he assures the reader his book is not an “exhortation...to keep every square inch of [the world] under active and systematic observation.” Yet he offers only vague guidance about how to keep the scope of information

¹⁴ Kent at 13

¹⁵ Kent at 17.

¹⁶ Kent at 14.

¹⁷ Kent at 44.

¹⁸ Kent at xxiv.

manageable – limiting it to “fragments,” for example, that are relevant to current national problems, in addition to “other problems” that “appear to be coming.”¹⁹

Kent’s conception of intelligence, with its emphasis on preventing surprise attacks, ingrained very broad assumptions about the volume of information necessary for intelligence to carry out its mission. Although his 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 vast stores of information without theoretical guidance.²⁰ 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.’” If Kendall were to critique today’s reforms, he might well air these same doubts about an information sharing regime dedicated to processing information into its most “shareable” form.

III. 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 that “If one theme runs through this book, it is *intelligence is information*.”²¹ 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.”²² The free flow of information will make it possible for analysts to cope with this uncertainty, assigning and re-assigning themselves to problems as needs change. In *Reshaping Intelligence for an Age of Information*, Gregory Treverton echoes this market-based rationale, recommending flexibility and widespread information sharing because “intelligence’s business is information, not secrets.”²³

Considering how to adapt to globally networked terrorism, the 9/11 Commission invokes a similar information-centric logic: greater information sharing will enhance the flexibility needed to forestall future attacks in a “more fluid international environment with uncertain, changing goals and interests.”²⁴ 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.²⁵ Guidelines regulating the flow of information under the Foreign Intelligence Surveillance Act

¹⁹ Kent at 37.

²⁰ For this comment and those that follow, see Wilmoore Kendall, “The Function of Intelligence,” 1 *World Politics* 542, 549-550 (1949).

²¹ Bruce Berkowitz and Allan Goodman, *Best Truth: Intelligence in the Information Age* x (Yale University Press 2000).

²² Berkowitz and Goodman at 82, 63.

²³ Gregory Treverton, *Reshaping Intelligence for an Age of Information* 17 (Cambridge University Press 2001).

²⁴ *9/11 Commission Report* at 91.

²⁵ *9/11 Commission Report* at 91.

(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.²⁶ Not unlike investigators of the Pearl Harbor intelligence failure, the Commission emphasized specific failures to share and coordinate information in the months leading up to the terrorist attacks. Although it qualifies this narrative by noting that more information sharing may not have prevented the attacks, it recommends a conceptual framework for intelligence rooted in vast information sharing.

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. In this new framework, the Commission argues, the Cold War’s need-to-know standard for information sharing, increasingly vilified, is no longer appropriate.²⁷ It calls for a “need-to-share” culture of integration to take its place, relying selectively on the Markle Foundation Task Force on National Security in the Information Age.²⁸ The Commission’s recommendations form the basis for the sweeping Information Sharing Environment, along with its imperatives to bureaucratize sharing and convert information itself into its “most shareable” form.

Critics have begun to highlight drawbacks to this information sharing framework, particularly the possibility of promoting consensus in analysis when more diversity is actually required and heightened risks to security posed by wider information sharing.²⁹ Scholars have also noted the inherent difficulties of intelligence that are unlikely to be solved through further information sharing, such as the sheer difficulty of making accurate predictions about complex phenomena and persistent cognitive biases that interfere with any decision making.³⁰ In addition, enforcement of information sharing behavior patterns through greater centralized control is not likely to be effective.³¹ Examining this reform logic through the lens of information and communication theory uncovers additional problems with the proposed mechanisms of sharing, discussed in the next sections

IV. 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

²⁶ 9/11 Commission Report at 80.

²⁷ 9/11 Commission Report at 417.

²⁸ See Markle Foundation Task Force reports, Creating a Trusted Information Network for Homeland Security (Markle Foundation, 2003) and Protecting America’s Freedom in the Information Age (Markle Foundation, 2002).

²⁹ Gary Schmitt touches on the consensus problem in “Truth to Power? Rethinking Intelligence Analysis,” in The Future of American Intelligence 41 (Peter Berkowitz ed., Hoover Institution Press 2005). The report (2005) created by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (“WMD Commission”) gently highlights the security risks, saying they are “too infrequently” noted in calls for more information sharing (429).

³⁰ See, for example, Richard Betts, “Analysis, War, and Decision: Why Intelligence Failures Are Inevitable,” in Strategic Intelligence: Windows Into a Secret World 97 (Loch Johnson and James Wirtz ed., Roxbury Publishing Company 2004); and Robert Jervis, American Foreign Policy in a New Era 116-124 (Routledge 2005).

³¹ Posner, Preventing Surprise Attacks (2005).

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. Reddy marshals evidence from everyday English demonstrating 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....”).³²

To draw out the conduit metaphor’s implications, Reddy describes an alternate model of communication, 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.³³ A message is not physically “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. Similarly, 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 mechanically unpacking meaning out of the “sent” message.³⁴ In his work, he sounded a prescient note of caution about the promise of mass communications technologies to improve communication, if they neglect the ability to make sense of information.

The 9/11 Commission’s information sharing regime, with its optimism about the benefits 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. The Commission expects formal procedures and incentives to share to generate a “smart” government by maximizing the flow of information. It selectively adopts the Markle Foundation Task Force’s reasoning that a “culture of distribution” with “distributable products...created at the outset” is the proper way to stimulate the “flow of information necessary to fight terrorism.”³⁵ The Commission’s logic assumes problematically that the meaning and significance of information will flow through the conduits of information sharing routines in a networked intelligence and national security community. Far from a “smart” government, however, the outcome may be a swamped, confused government, besieged 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.

³² Michael Reddy, “The Conduit Metaphor: A Case of Frame Conflict in our Language about Language” in *Metaphor and Thought* 164 (Andrew Ortony ed., Cambridge University Press 1993).

³³ See Shannon and Weaver, *Mathematical Theory of Communication* (1964).

³⁴ While constructivism also emphasized the importance of the subjective interpreter and local context, 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.

³⁵ *Creating a Trusted Information Network* at 24. The Markle Foundation Task Force 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.

Intelligence information is typically very ambiguous, with several plausible interpretations. Understanding the context of information, therefore, is a fundamental tool of analysis. It is the 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.³⁶ 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.”³⁷ 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 will 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.”³⁸ The agent urged establishing liaison with these schools, analysis of his theory in the intelligence community, and obtaining visa information about flight school applicants. Although this memo was shared with the FBI’s Radical Fundamentalist Unit and CIA’s Bin Ladin Unit, these recipients did not even see it, according to the report, and no action was taken. The deluge of decontextualized information unleashed by the proposed “culture of distribution” is likely to meet with the same fate, unless tools 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 U.S. visas. Interestingly, the Commission also

³⁶ Of course, there is a long recognized tension between the need for *multiple* 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 massive network of untested users will probably not enhance analysis at any of these centers.

³⁷ For these excerpts from the report, see information sharing recommendations in 9/11 Commission Report at 416-419.

³⁸ 9/11 Commission Report at 272.

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.³⁹ 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 says, “that the local commanders would have been further enlightened if they had had the pieces of the puzzle that were denied them.”⁴⁰ Indeed, “it would have created endless confusion if Washington had tried to relay all available signals to the overseas commands.”⁴¹ 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.

V. Information as Power

In the logic of reform, bureaucratized information sharing is *itself* seen as the central means of making sense of information and picking out the relevant signals. Instead of personal ingenuity, expertise, level of concentration, quality of information, and other factors routinely emphasized by intelligence scholars, good analysis is arguably thought to be a function of *how much* information is accessible out there in the ether of the Information Sharing Environment. Information sharing is seen as inherently good, the security concerns far less significant in the current threat environment. The work of Geoff Nunberg, a linguist studying the information age, highlights some of the risks in relying too devotedly on “information” for insights.

Nunberg traces the evolving meanings of the word “information,” from the particularistic sense of answering a specific question with a specific answer to the more nebulous, though intrinsically positive, sense of information evoked by information age manifestos. In this sense, 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.⁴² This abstract sense of information – “information in the large” – is disconnected from the particular situations it is

³⁹ *9/11 Commission Report* at 269-273, 355.

⁴⁰ Wohlstetter at 226.

⁴¹ Wohlstetter at 131.

⁴² Geoffrey Nunberg, “Farewell to the Information Age,” in *The Future of the Book* 103, 107 (Geoffrey Nunberg ed., University of California Press 1996).

about as well as the people who are *informed*. Decontextualized and fungible, it can be “liberated and manipulated as a kind of pure essence.”⁴³ It is also different from the older sense of “information” as the material that leads people to become informed through instruction and learning; the *work* of understanding information produced the erudite, insightful individual Jane Austin intended with the phrase a “man of information.” By contrast, 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....”⁴⁴

In the rhetoric of intelligence reform, analysts too look increasingly like passive consumers of “information in the large,” their work reduced to mechanically processing as much of it as possible. “The biggest impediment to...a greater likelihood of connecting the dots,” the Commission argues, “is the human or systemic resistance to sharing information.”⁴⁵ Experiences, background, education, willingness to doubt, level of concentration – all the tools analysts brings to bear as they engage in the difficult process of analysis pale in comparison to the “resistance to sharing information.” Some of the language in the Markle Foundation report also suggests a reliance on information, implying the “agency of instruction” migrating to the information itself, rather than the analyst.⁴⁶ Grasping the significance of information becomes, in the Commission’s logic, a natural consequence of the ability to access it.

Leaving it to information to forestall attacks, however, reflects undue faith in the network age concept of “information in the large,” with the value of information attached to how “distributable” it is made to be. This faith in information neglects the craft of analysis, the hard and personal work involved in studying ambiguous intelligence information, thinking about it from different perspectives, and evaluating it critically. 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.”⁴⁷ As long as all the information is available, 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. On the contrary, analysts will probably be overwhelmed by all the information available in a “culture of distribution” and hard pressed to make sense of it in its decontextualized “most shareable” form.

Moreover, analysts 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 won’t 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.⁴⁸ In fact, if search algorithms are cumbersome and exhibit low recall, analysts could be left with far less information than they might otherwise have accessed, had

⁴³ Nunberg at 107.

⁴⁴ Nunberg at 113.

⁴⁵ 9/11 Commission Report at 416.

⁴⁶ Creating a Trusted Information Network at 2.

⁴⁷ Kendall at 549.

⁴⁸ 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,” 30 Communications of the ACM 964 (1987).

they relied on their social networks and other search techniques. In addition, depending on how the Information Sharing Environment is technically implemented, 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 in all 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.”⁴⁹ With every analyst drawing conclusions based on the same presentation of information, the herd mentality problem identified by the WMD Commission would worsen.⁵⁰

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.⁵¹ 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 alternate 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.⁵²

In the new framework, analysts are nonetheless portrayed as “empowered” merely by virtue of their access to vast amounts of information.⁵³ In their concept of information age intelligence, Berkowitz and Goodman imagine analysts “assigning themselves” to problems, assembling and re-assembling themselves in a “new configuration” as needs change, as if analysts were Legos and fruitful collaboration effortless and automatic as long as the information is there.⁵⁴ Although the 9/11 Commission introduces organizational centralization where they reject it in favor of their market-based approach, both embrace the idea that analysts are *empowered* through access to information networks, reflecting the flawed logic of technological determinism. Nonetheless, these reformers are aware of the signals to noise ratio, the difficulties in sorting relevant signals from irrelevant noise in vast amounts of information. For example, the Markle Foundation report stresses the importance of sense-making, though its metrics to gauge progress focus

⁴⁹ 9/11 Commission Report at 344.

⁵⁰ Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005).

⁵¹ Richard J. Heuer, Jr., “Do You Really Need More Information?” 23 Studies in Intelligence 15 (1979).

⁵² Robert Jervis has also emphasized this approach to alleviate problems of misperception in making political decisions, in “Hypotheses on Misperception,” 20 World Politics 454 (1968). 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.

⁵³ See 9/11 Commission Report at 419.

⁵⁴ Berkowitz and Goodman at 74, 82.

mainly on how much information is flowing.⁵⁵ The Commission makes it clear that “connecting the dots” amid the noise of so much information is a matter of eliminating obstacles to information sharing. This belief in the value of information sharing itself may have obscured the drawbacks of the approach. Improved sense-making and interpretation do not necessarily follow from enhanced information sharing and flow.

VI. Sense-making and Interpretation

It is increasingly clear to organizational theorists 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.⁵⁶ Research in this area emphasizes analysts’ physical context; the social setting of their work; exposure to alternate conceptual approaches that value information differently; availability of diverse technical search and analysis tools; and opportunities to engage in informal, low-risk communication in which tentative ideas can be aired.⁵⁷ Routinization, standardized patterns of interaction, stability, and an absence 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, also through routines and bureaucratic procedures, may not be advisable.⁵⁸ Instead, methods to improve the environment of analysis should build on insights from this literature, promoting connectivity in ways that encourage sense-making, diverse tools of interpretation, and exposure to alternate viewpoints.

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.⁵⁹ Not unlike aspects of intelligence analysis, arbitrage involves both “pattern recognition” (matching data to existing models) and “re-cognition” (making unanticipated associations). The manager deliberately configured the room and its social atmosphere to facilitate interpretation and sense-making. While each desk applies a distinct evaluative principle to select out and assign value to certain information, desks are positioned near one another with ample opportunity for informal information exchange and discussion of competing interpretations. The manager also rotated people around from time to time to introduce variety and challenge, exposing them to heterogeneous value frameworks for assessing information. Although the intelligence community’s practice of “competitive analysis” is intended to promote this kind of analytic diversity, its bureaucratic formality and routine quality diminish its effectiveness and the credibility of its estimates.

⁵⁵ Creating a Trusted Information Network at 15.

⁵⁶ See, for example, John Sealy Brown and Paul Duguid, The Social Life of Information (Harvard Business School Press 2000) and Richard K. Lester and Michael J. Piore, Innovation: The Missing Dimension (Harvard University Press 2004).

⁵⁷ In addition to the references in note 56, see Marcie J. Tyre and Eric von Hippel, “The Situated Nature of Adaptive Learning in Organizations,” 8 Organization Science 71 (1997); Daniel Beunza and David Stark, “Tools of the trade: the socio-technology of arbitrage in a Wall Street trading room,” 13 Industrial and Corporate Change 369 (2004); and AnnaLee Saxenian, Regional Advantage: Culture and Competition in Silicon Valley and Route 128 (Harvard University Press 1994).

⁵⁸ 9/11 Commission Report at 344.

⁵⁹ Beunza and Stark, “Tools of the trade: the socio-technology of arbitrage in a Wall Street trading room” (2004).

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.⁶⁰ The introduction and re-introduction of newcomers learning the ropes led the researchers to compare the ship to a school, focused on teaching the complex, interrelated activities involved in overall coordination and adaptation to changing tactical circumstances. The 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.⁶¹ 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 another 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.⁶²

By activating domestic agencies in the search for Mihdhar and Hazmi, FBI analyst "Mary" did immediately what the CIA failed to do for almost two years, since early 2000 when its analysts learned of their terrorist associations and U.S. 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 "zone defense" as "John" indicated. 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 on flight decks also illustrates how introducing newcomers into the various sections of high-reliability organizations can promote awareness and attention to a collective mission.⁶³

Intelligence managers should explore how to apply these techniques to the environment of 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

⁶⁰ Gene I. Rochlin, Todd R. La Porte, and Karlene H. Roberts, "The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea," *NWC Review* (1998).

⁶¹ See *9/11 Commission Report* at 266-272.

⁶² 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 (270), it also indicates that the FBI as a whole did *not* and "and thus did not take adequate action..." (356)

⁶³ See Karl E. Weick and Karlene H. Roberts, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," 38 *Administrative Science Quarterly* 357 (1993).

sense of information, in addition to providing access to it, through social network analysis, exploratory modeling, visualization, and other methods.⁶⁴ These tools should be situated in the larger contextual environment of analysis. Managers should see their own roles as cultivating interpretative communities, marrying diverse technical tools with social and physical configurations that promote meaningful connectivity. For example, they might deliberately expose analysts to alternate 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 inhibiting fear of being wrong or risking their careers.⁶⁵ The Markle Foundation report also recommends rewarding managers who actively try to understand what interpretative difficulties analysts are experiencing, and figure out what information or collaborative assistance outside their reach would mitigate those difficulties.⁶⁶

VII. Conclusions: The Logic of Information Sharing

In the logic of information sharing, reformers expect the free flow of information to foster a robust marketplace of ideas, encouraging the diverse, competitive analysis necessary for the intelligence community to adapt to a complex, rapidly evolving threat environment. This paper does not argue against information sharing in principle; analysts need information to do their jobs, of course, and quite frequently they need a lot of it. It does argue that the logic and proposed mechanisms of sharing, with problematic assumptions about “information” and the advantages of its free flow, are not sufficiently developed. While embracing Sherman Kent’s belief in the great volume of information needed to avoid surprise, the new framework 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.”⁶⁷ This paper also cautions against placing too much faith in information, if the human ability to make sense of it is neglected and context disregarded.

Designers of the Information Sharing Environment 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.⁶⁸ Not only will these security concerns persist, however, undermining efforts to routinize information sharing, but it is not clear that they *should* be dismissed as readily as the Commission seems to want. Indeed, the Commission describes today’s threats as “less visible,” networked adversaries hidden in the fabric of our own society, suggesting that security concerns

⁶⁴ See, for example, Kevin M. O’Connell, “The Role of Science and Technology in Transforming American Intelligence,” in The Future of American Intelligence 139 (Bruce Berkowitz ed., Hoover Institution Press 2005); James R. Gosler, “The Digital Dimension,” in Transforming U.S. Intelligence 96 (Jennifer E. Sims and Burton Gerber eds., Georgetown University Press 2005); and Creating a Trusted Information Network.

⁶⁵ Research on Silicon Valley has shown that a social tolerance for failure encouraged entrepreneurial experimentation with different ideas, fostering a “culture of innovation.” See Saxenian, Regional Advantage (2004).

⁶⁶ Creating a Trusted Information Network at 23.

⁶⁷ Kent at 184.

⁶⁸ 9/11 Commission Report at 417.

might be heightened in such an environment.⁶⁹ 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 agile, adaptable, and flexible as security experts think, what will prevent them from *adapting* to newly relaxed security procedures, dismissed in the name of information sharing?

Reformers will need to address these trade-offs more thoroughly, weighing information sharing and a “culture of distribution,” for example, against 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; 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, if they can be persuaded to do so. Further research should explore how to map methods drawn from the literature on coordination in high-reliability organizations and innovation in the private sector to the evolving intelligence community.

⁶⁹ 9/11 Commission Report at 399.