September 11 and the Imperative of Reform in the U.S. Intelligence Community

Additional Views of Senator Richard C. Shelby
Vice Chairman, Senate Select Committee on Intelligence

December 10, 2002

> "In actual practice, the successful end to the Cold War and the lack of any national intelligence disasters since then seem to militate in favor of keeping the existing structure until some crisis proves it to be in dire need of repair. . . . Thus we are likely to live with a decentralized intelligence system – and the impulse toward centralization – until a crisis re-aligns the political and bureaucratic players or compels them to cooperate in new ways."
>
> — Deputy Chief, CIA History Staff
> publication dated 2001[1]

Our country's Intelligence Community was born because of the devastating surprise attack the United States suffered at Japanese hands at Pearl Harbor on December 7, 1941. In the wake of that disaster, America's political leaders concluded "that the surprise attack could have been blunted if the various commanders and departments had coordinated their actions and shared their intelligence." This was the inspiration behind the National Security Act of 1947, which "attempted to implement the principles of unity of command and unity of intelligence."[2]

---

[1] *Central Intelligence: Origin and Evolution* (Langley, Virginia: CIA History Staff, CIA Center for the Study of Intelligence, 2001), from the Historical Perspective by Dr. Michael Warner [hereinafter "Warner"], at 2 & 18.

[2] Warner, *supra*, at 1.

Sixty years later, on September 11, 2001, we suffered another devastating surprise attack, this time by international terrorists bent upon slaughtering Americans in the name of their God. This second attack is the subject of the findings and recommendations of the unprecedented Joint Inquiry conducted by the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). In this document, I offer my own assessments and suggestions, based upon my four and a half years as Chairman of the SSCI and one and a half years as its Vice Chairman. These additional views are intended to complement and expand upon the findings and recommendations of the Joint Inquiry.

Long before the September 11 attacks, I made no secret of my feelings of disappointment in the U.S. Intelligence Community for its performance in a string of smaller-scale intelligence failures during the last decade. Since September 11 I have similarly hid from no one my belief that the Intelligence Community does not have the decisive and innovative leadership it needs to reform itself and to adapt to the formidable challenges of the 21st Century.

In the following pages, I offer my suggestions about where our Intelligence Community should go from here. These views represent the distilled wisdom of my eight years on the SSCI, of innumerable hearings, briefings, and visits to sensitive sites and facilities, and of thousands of man-hours of diligent work by intelligence oversight professionals on the SSCI staff over several years. Most of all, these Additional Views represent the conclusions I have reached as a result of the work of our Joint Inquiry Staff and the many private and public committee hearings we have had into the intelligence failures that led up to September 11.

I hope that the American public servants who inherit responsibility for these matters during the 108th Congress and the second half of President Bush's first term will carefully consider my arguments herein. Thousands of Americans have already been killed by the enemy in the war declared against us by international terrorists, and though we have enjoyed some signal successes since our counteroffensive began in late September 2001, our Intelligence Community remains poorly prepared for the range of challenges it will confront in the years ahead.

Too much has happened for us to be able to conclude that the American people and our national security interests can be protected simply by throwing more resources at agencies still fundamentally wedded to the pre-September 11 *status quo*. I salute the brave and resourceful Americans – both in and out of uniform – who are even at this moment taking the fight to the enemy in locations around the world. These patriots, however, deserve better than our government's recommitment to the bureaucratic recipes that helped leave us less prepared for this crisis than we should have been.

I hope that the Joint Inquiry's report – and these Additional Views thereto – will help spur the kind of broad-ranging debate in Congress, within the Administration, and among the American

public that our present circumstances deserve. The road to real intelligence reform is littered with the carcasses of forgotten studies and ignored reports. We cannot afford to let the results of this unprecedented Joint Inquiry be forgotten as well. The American people will not forgive us if we fail to make the changes necessary to ensure that they are better protected in the future.

Executive Summary

Community Structure and Organization. With respect to the structure and organization of the U.S. Intelligence Community (IC), the story of counterterrorism (CT) intelligence work before September 11 illustrates not only the unwillingness of the Director of Central Intelligence (DCI) fully to exercise the powers he had to direct resources and attention to CT, but also the institutional weakness of the DCI's office within the Community. Caught ambiguously between its responsibilities for providing national-level intelligence and providing support to the Department of Defense to which most IC agencies owe their primary allegiance, the Community proved relatively unresponsive to the DCI's at least partly rhetorical 1998 declaration of "war" against Al-Qa'ida. The fragmented nature of the DCI's authority has exacerbated the centrifugal tendencies of bureaucratic politics and has helped ensure that the IC responds too slowly and too disjointedly to shifting threats. Ten years after the end of the Cold War, the Community still faces inordinate difficulty responding to evolving national security threats.

To help alleviate these problems, the office of the DCI should be given more management and budgetary authority over IC organs and be separated from the job of the CIA Director, as the Joint Inquiry suggests in urging that we consider reinventing the DCI as the "Director of National Intelligence." Moreover, the DCI (or DNI, as the case may be) should be compelled actually to use these powers in order to effect real IC coordination and management. An Intelligence Community finally capable of being coherently managed as a Community would be able to reform and improve itself in numerous ways that prove frustratingly elusive today – ultimately providing both its national-level civilian and its military customers with better support. Congress should give serious

consideration, in its intelligence reform efforts, to developing an approach loosely analogous to that adopted by the Goldwater-Nichols Act in reforming the military command structure in order to overcome entrenched bureaucratic interests and forge a much more effective "joint" whole out of a motley and disputatious collection of parts.

Most importantly, Congress and the Administration should focus upon ensuring an organizational structure that will not only help the IC respond to current threats but will enable our intelligence bureaucracies to change themselves as threats evolve in the future. We must not only learn the lessons of the past but learn how to keep learning lessons as we change and adapt in the future. To this end, the IC should adopt uniform personnel and administrative standards in order to help ensure that its personnel and organizational units remain unique and valuable individual resources but also become administratively fungible assets, capable of being reorganized and redirected efficiently as circumstances demand. It will also be necessary to break the mindset within the IC that holds that only intelligence professionals actually employed by the traditional collection agencies can engage in collection or analysis of those agencies' signature types of intelligence. The traditional collection agencies' expertise in "their" areas should be used to enrich the Community's pool of intelligence know-how rather than as barriers to entry wielded in defense of bureaucratic and financial "turf." Instead, the collection agencies should be charged with certifying – but not running or controlling – training curricula within other IC agencies that will produce competent specialists in the relevant fields.

Ultimately, Congress and the Administration re-examine the basic structure of the intelligence provisions of the National Security Act of 1947 in light of the circumstances and challenges our country faces today. Returning to these roots might suggest the need to separate our country's "central" intelligence analytical functions from the resource-hungry collection responsibilities that make agencies into self-interested bureaucratic "players."

Information-Sharing. Our Joint Inquiry has highlighted fundamental problems with information-sharing within the IC, depriving

analysts of the information access they need in order to draw the inferences and develop the conclusions necessary to inform decision-making. The IC's abject failure to "connect the dots" before September 11, 2001 illustrates the need to wholly re-think the Community's approach to these issues.

The CIA's chronic failure, before September 11, to share with other agencies the names of known Al-Qa'ida terrorists who it knew to be in the country allowed at least two such terrorists the opportunity to live, move, and prepare for the attacks without hindrance from the very federal officials whose job it is to find them. Sadly, the CIA seems to have concluded that the maintenance of its information monopoly was more important that stopping terrorists from entering or operating within the United States. Nor did the FBI fare much better, for even when notified in the so-called "Phoenix Memo" of the danger of Al-Qa'ida flight school training, its agents failed to understand or act upon this information in the broader context of information the FBI already possessed about terrorist efforts to target or use U.S. civil aviation. The CIA watchlisting and FBI Phoenix stories illustrate both the potential of sophisticated information-sharing and good information-empowered analysis and the perils of failing to share information promptly and efficiently between (and within) organizations. They demonstrate the need to ensure that intelligence analysis is conducted on a truly "all-source" basis by experts permitted to access all relevant information – no matter where in the IC it happens to reside.

The IC's methods of information-sharing before September 11 suffered from profound flaws, and in most respects still do. In order to overcome bureaucratic information-hoarding and empower analysts to do the work our national security requires them to do, we need to take decisive steps to reexamine the fundamental intellectual assumptions that have guided the IC's approach to managing national security information. As one witness told the Joint Inquiry, we may need "to create a new paradigm wherein 'ownership' of information belonged with the analysts and not the collectors." In addition, the imbalance between analysis and collection makes clear that in addition to being empowered to conduct true "all-source" analysis, our analysts will also need to be supplied with powerful new tools if they are to provide analytical value-added to the

huge volumes of information the IC brings in every day. Recent development and initiatives in comprehensive databasing and data-mining suggest that solutions to these challenges may be within our reach. The information-analysis organization within the new Department of Homeland Security als has great potential to contribute to effective CT information-sharing and analyst-empowerment within the U.S. Government – and Congress has given it the legal tools it needs to play this crucial catalytic role. Meanwhile, Congress should take decisive steps to help stem our contemporary culture of endemic "leaking" of national security information to the media, so as better to ensure that our analysts remain better informed about terrorists than the terrorists do about them.

Intelligence-Law Enforcement Coordination. The September 11 story also illustrates the tremendous problems of coordination between U.S. law enforcement and intelligence entities that developed out of a long series of misunderstandings, timorous lawyering, and mistaken assumptions. Congress and the Administration have made progress since September 11 in breaking down some of the mythologies that impeded coordination. Thanks to Congress' passage of the USA PATRIOT Act of 2001 and the Justice Department's success in appellate litigation to compel the Foreign Intelligence Surveillance Court to implement these changes, for instance, the legally fallacious "Wall" previously assumed to exist between intelligence and law enforcement work has been breached and years of coordination-impeding Justice Department legal reticence has been overcome.

With luck, we will never again see the kind of decision-making exhibited when the CIA refused to share information with FBI criminal investigators about two known Al-Qa'ida terrorists (and soon-to-be suicide hijackers) in the United States, and when the FBI – only days before the September 11 attacks – deliberately restricted many of its agents from participating in the effort to track down these terrorists on the theory that this was work in which criminal investigators should play no role. Hopefully we will also no longer see the kind of fundamental legal misunderstanding displayed by FBI lawyers in the Moussaoui case, in which investigators in Minneapolis were led on a three-week wild goose chase by a faulty analysis of the Foreign Intelligence Surveillance Act

(FISA). It will take sustained Congressional oversight in order to ensure compliance with the information-sharing authorities and mandates of the USA PATRIOT Act, but it is imperative that we ensure that such problems do not recur. To help achieve this, Congress should modify the Act's "sunset" provisions and should approve legislation proposed by Senators Kyl and Schumer to modify FISA's "foreign power" standard.

Domestic Intelligence. The story of September 11 is also replete with the FBI's problems of internal counterterrorism and counterintelligence (CI) coordination, information-sharing, and basic institutional competence. The FBI was unaware of what information it possessed relevant to internal terrorist threats, unwilling to devote serious time, attention, or resources to basic intelligence analytical work, and too organizationally fragmented and technologically impoverished to fix these shortfalls even had it understood them and really wished to do so. These problems persisted, moreover, through a major FBI reorganization ostensibly designed to address these problems, which had been well known for years.

The FBI's problems in these respects suggests that the Bureau's organizational and institutional culture is terribly flawed, and indeed that the Bureau – as a law enforcement organization – is fundamentally incapable, in its present form, of providing Americans with the security they require against foreign terrorist and intelligence threats. Modern intelligence work increasingly focuses upon shadowy transnational targets, such as international terrorist organizations, that lack easily-identifiable geographic loci, organizational structures, behavioral patterns, or other information "signatures." Against such targets, intelligence collection and analysis requires an approach to acquiring, managing, and understanding information quite different from that which prevails in the law enforcement community. The United States already has a domestic intelligence agency in the form of the FBI, but this agency is presently unequal to the challenge, and provides neither first-rate CT and CI competence nor the degree of civil liberty protections that would obtain were domestic intelligence collectors deprived of their badges, guns, and arrest powers and devoted wholly to CI and CT tasks.

This pattern of dysfunction compels us to consider radical reform at the FBI. A very strong argument can be made for removing the CI and CT portfolios from the Bureau, placing them in a stand-alone member of the Intelligence Community that would be responsible for domestic intelligence collection and analysis but would have no law enforcement powers or responsibilities. Alternatively, it might be sufficient to separate the CI and CT functions of the FBI into a semi-autonomous organization that reports to the FBI director for purposes of overall coordination and accountability, but which would in every other respect be wholly separate from the "criminal" components of the FBI. A third approach might be to move the FBI's CI and CT functions to the new Department of Homeland Security, thereby adding a domestic collection element to that organization's soon-to-be-created Undersecretariat for Information Analysis and Infrastructure Protection. Some kind of radical reform of the FBI is long overdue, and should be a major item on the "intelligence reform" agenda for the 108th Congress. The Bush Administration and the 108th Congress should make it a high priority to resolve these issues, and to put the domestic components of our Intelligence Community on a footing that will enable them to meet the challenges of the 21st century.

Human Intelligence. The status quo of IC approaches to human intelligence (HUMINT) was tested against the Al-Qa'ida threat and found wanting. The CIA's Directorate of Operations (DO) has been too reluctant to develop non-traditional HUMINT platforms, and has stuck too much and for too long with the comparatively easy work of operating under diplomatic cover from U.S. embassies. This approach is patently unsuited to HUMINT collection against nontraditional threats such as terrorism or proliferation targets, and the CIA must move emphatically to develop an entirely new collection paradigm involving greater use of non-official cover (NOC) officers. Among other things, this will necessitate greater efforts to hire HUMINT collectors from ethnically and culturally diverse backgrounds, though without a fundamental shift in the CIA's HUMINT paradigm diversity for diversity's sake will be of little help. The CIA should also spend more time developing its own sources, and less time relying upon the political munificence of foreign liaison services.

Covert Action. The CIA's decidedly mixed record of success in offensive operations against Al-Qa'ida before September 11 illustrates the need for the President to convey legal authorities with absolute clarity. If we are not to continue to encourage the kind of risk-averse decision-making that inevitably follows from command-level indecision, our intelligence operators risking their lives in the field need to know that their own government will make clear to them what their job is and protect them when they do it. Congress should bear this in mind when conducting its legitimate oversight of covert action programs in the future, even as it struggles to cope with the oversight challenges posed by the potential for the Defense Department to take a greater role in such activities.

Accountability. The story of September 11 is one replete with failures: to share information, to coordinate with other agencies; to understand the law, follow existing rules and procedures, and use available legal authorities in order to accomplish vital goals; to devote or redirect sufficient resources and personnel to counterterrorism work; to communicate priorities clearly and effectively to IC components; to take seriously the crucial work of strategic counterterrorism analysis; and most importantly, to rise above parochial bureaucratic interests in the name of protecting the American people from terrorist attack.

The DCI has declared us to be at "war" against Al-Qa'ida since 1998, and as the President has declared, we have really been so since at least September 11. Some have suggested that this means that we should postpone holding anyone accountable within the Intelligence Community until this war is over and the threat recedes. I respectfully disagree.

The threat we face today is in no danger of subsiding any time soon, and the problems our Intelligence Community faces are not ones wisely left unaddressed any longer. Precisely *because* we face a grave and ongoing threat, we must begin reforming the Community immediately. Otherwise we will be unable to meet this threat. The metaphor of "war" is instructive, for wise generals do not hesitate to hold their subordinates accountable while the battle still rages, disciplining or cashiering those who fail to do their duty. So also do wise Presidents dispose of their faltering generals under fire. Indeed, failures in wartime are traditionally considered

less excusable, and are punished more severely, than failures in times of peace.

Nor should we forget that accountability has two sides. It is also a core responsibility of all good leaders to reward those who perform well, and promote them to positions of ever greater responsibility. In urging the Intelligence Community to hold its employees accountable, the IC must therefore both discipline those who fall down on the job and reward those who have excelled.

For these reasons, it is disappointing to me that despite the Joint Inquiry's explicit mandate to "lay a basis for assessing the accountability of institutions and officials of government" and despite its extensive findings documenting recurring and widespread Community shortcomings in the months and years leading up to September 11, the Joint Inquiry has not seen fit to identify *any* of the individuals whose decisions left us so unprepared. I urge President Bush to examine the Joint Inquiry's findings in order to determine the extent to which he has been well served by his "generals" in the Intelligence Community.

Some have argued that we should avoid this issue of accountability lest we encourage the development of yet more risk-aversion within the Community. I do not believe this is the case. The failings leading up to September 11 were not ones of impetuousness, the punishment for which might indeed discourage the risk-taking inherent in and necessary to good intelligence work. The failures of September 11 were generally ones not of reckless *commission* but rather of nervous *omission*. They were failures to take the necessary steps to rise above petty parochial interests and concerns in the service of the common good. These are not failings that will be exacerbated by accountability. Quite the contrary. And, more importantly, it is clear that without real accountability, these many problems will simply remain unaddressed – leaving us needlessly vulnerable in the future.

I advocate no crusade to hold low-level employees accountable for the failures of September 11. There clearly were some individual failings, but for the most part our hard-working and dedicated intelligence

professionals did very well, given the limited tools and resources they received and the constricting institutional culture and policy guidance they faced. The IC's rank-and-file deserve no discredit for resource decisions and for creating these policies.

Ultimately, as the findings of the Joint Inquiry make clear – though they stop short of actually saying so – accountability must begin with those whose job it was to steer the IC and its constituent agencies through these shoals, and to ensure that all of them cooperated to the best of their abilities in protecting our national security. Responsibility must lie with the leaders who took so little action for so long, to address problems so well known. In this context, we must not be afraid publicly to name names. The U.S. Intelligence Community would have been far better prepared for September 11 but for the failure of successive agency leaders to work wholeheartedly to overcome the institutional and cultural obstacles to inter-agency cooperation and coordination that bedeviled counterterrorism efforts before the attacks: DCIs George Tenet and John Deutch, FBI Director Louis Freeh, and NSA Directors Michael Hayden and Kenneth Minnihan, and NSA Deputy Director Barbara McNamara. These individuals are not responsible for the disaster of September 11, of course, for that infamy belongs to Al-Qa'ida's 19 suicide hijackers and the terrorist infrastructure that supported them. As the leaders of the United States Intelligence Community, however, these officials failed in significant ways to ensure that this country was as prepared as it could have been.

I. *Intelligence Community Structure*

A. *The DCI's Problematic "War" of 1998*

The Director of Central Intelligence (DCI) testified before Congress in February 2001 that he considered Usama bin Laden and Al-Qa'ida to be *the most important national security threat*

faced by the United States.[3] In December 1998, in fact – in the wake of the terrorist bombings of the U.S. embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya – he had proclaimed that "[w]e are at war" with Al-Qa'ida.[4] The story of this "war," however, underlines the problematic nature of the U.S. Intelligence Community's management structure.

As the Joint Inquiry Staff (JIS) has noted in its presentations to the Committees, "[d]espite the DCI's declaration of war in 1998, there was no massive shift in budget or reassignment of personnel to counterterrorism until after September 11, 2001."[5] Indeed, the amount of money and other resources devoted to counterterrorism (CT) work after the DCI's "declaration of war" in 1998 barely changed at all. The budget requests sent to Congress relating to the CIA's Counterterrorism Center (CTC), for instance, rose only marginally – in the low single-digit percentages each year into Fiscal Year 2001 – and at rates of increase essentially unchanged from their slow growth before the "war." (These requests, incidentally, were met or exceeded by Congress, even to the point that the CIA ended Fiscal Year 2001 with millions of dollars in counterterrorism money left *unspent*.[6])

In his 1998 "declaration of war," the DCI had declared to his deputies at the CIA that "I want no resources or people spared in this effort, either inside the CIA or the Community."[7] CIA officials also told the HPSCI on March 4, 1999 – in a written response to questions about the CIA's proposed budget for Fiscal Year 2000 – that "the Agency as a whole is well positioned" to work against Al-Qa'ida targets, and that they were "confident that funding could be redirected internally, if needed, in a crisis."[8]

---

3 Senate Select Committee on Intelligence, hearing into "Worldwide Threats to National Security" (February 7, 2001) (remarks of George Tenet, declaring that "Osama bin Laden and his global network of lieutenants and associates remain the most immediate and serious threat.")

4 JIS, written statement submitted to joint SSCI/HPSCI hearing (September 18, 2001), at 9.

5 JIS, written statement submitted to joint SSCI/HPSCI hearing (September 18, 2001), at 10.

6 The detailed figures remain classified.

7 JIS, written statement submitted to joint SSCI/HPSCI hearing (September 18, 2001), at 9.

8 Central Intelligence Agency, response to "HPSCI Questions for the Record" (March 4, 1999) (declassified portion).

Shortly thereafter, however, a study conducted within the CTC found that it was unable to carry out more ambitious plans against Al-Qa'da for lack of money and personnel,[9] and CIA officials reported being "seriously overwhelmed by the volume of information and workload" before September 11, 2001.[10] According to former CTC chief Cofer Black, "before September 11, we did not have enough people, money, or sufficiently flexible rules of engagement."[11] The troops fighting the DCI's "war," in short, didn't have the support they needed. (Even when the DCI requested additional counterterrorism money from Congress, it almost invariably did so in the form of supplemental appropriations requests – thus denying Community managers the ability to prepare long-term plans and programs because these increases were not made a part of the Community's *recurring* budgeting process.)

Under the National Security Act of 1947, the DCI has considerable budgetary power over the U.S. Intelligence Community. His consent is needed before agency budget requests can be folded into the National Foreign Intelligence Program (NFIP) budget proposal, and he has authority over reprogramming both money and personnel between agencies.[12] Simultaneously serving as Director of the CIA, the DCI also has essentially complete authority over *that* organization, both with respect to budget requests and day-to-day management. If a DCI were willing actually to *use* the full range of powers available to him, these statutory levers would give him considerable influence over the Community. One of the great unanswered questions of our September 11 inquiry, therefore, is how the DCI could have considered himself to be "at war" against this country's most important foreign threat without bothering to use the full range of authorities at his disposal in this fight.

Unfortunately, part of the reason for this failure is the current DCI's longstanding determination – which he expressed quite frankly to some of us at a SSCI off-site meeting – that he does not really *consider* himself to be DCI. His principal interest and focus in office, he has told us, revolves around his role as head of the CIA, rather than his role as head of the

---

[9] This was the conclusion presented to an internal CIA conference on September 16, 1999. Further information about this internal study, however, has not been declassified.

[10] JIS, written statement submitted to joint SSCI/HPSCI hearing (September 18, 2001), at 13.

[11] Cofer Black, written statement submitted to joint SSCI/HPSCI hearing (September 26, 2001), at 10.

[12] *See* 50 U.S.C. § 403-4(b), (c), and (d).

Community as a whole. (The DCI has also publicly supported the creation of an Undersecretary of Defense for Intelligence [USDI], which seems likely only to reduce his influence over the Defense components of the U.S. Intelligence Community.) Part of the reason may also lie in the merely rhetorical nature of the DCI's 1998 proclamation: since September 11 the DCI has pointed to his "declaration of war" as a token of his pre-September 11 seriousness of purpose against Al-Qa'ida, but it does not appear to have been circulated or known outside a small circle of intimates before that date. And part of the reason that more was not done may also lie at higher levels of political authority. The nature of the "war" contemplated in 1998 certainly pales in comparison to the use of that term after September 11, and officials have suggested in the press that they undertook, as much as was politically possible at the time.[13]

That said, there can be no gainsaying that even if the DCI *had* really meant to "declare war" against Al-Qa'ida in 1998, the fragmented structure of the Intelligence Community and his tenuous authority over its component agencies would have greatly handicapped any effort to conduct an effective counterterrorist campaign from the DCI's office. His existing budget and reprogramming authorities under Section 104 of the National Security Act, for instance, extends by its terms only to the NFIP budget – and not to the Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Accounts (TIARA) budgets.[14] For this reason, no serious plan to reform the U.S. Intelligence Community can ignore the problem of Community management and the weaknesses of the *office* of the DCI as the Community's nominal head.

B. *Reinvigorating the Office of the DCI?*

The most obvious problem with respect to the IC's ability to act as a coherent and effective whole is the fact that more than 80 percent of its budgets and personnel resources are controlled by the Department of Defense (DOD). The DCI may be the titular head of the

---

[13] *See, e.g.*, Barton Gellman, "Broad Effort Launched After '98 Attacks," *Washington Post* (December 19, 2001), at A1 (quoting former Assistant Secretary of State for South Asian Affairs Karl Inderfurth that "Until September 11th, there was certainly not any groundswell of support to mount a major attack on the Taliban."); Bob Drogin, "U.S. Had Plan for Covert Afghan Options Before 9/11," *Los Angeles Times* (May 18, 2002), at A14 (quoting former Clinton Administration State Department official that invasion of Afghanistan was "really not an option" before September 11).

[14] Section 104 only discusses the NFIP. *See* 50 U.S.C. §§ 403-4(b) (budget approval); 403-4(c) (reprogramming); & 403-4(d) (transfer of funds and/or personnel).

Intelligence Community, but the National Security Agency (NSA), National Imagery and Mapping Agency (NIMA), National Reconnaissance Office (NRO), Defense Intelligence Agency (DIA), and military service intelligence arms are all DOD organizations and report first and foremost to the Secretary of Defense. (The heads of NSA and DIA, and the service intelligence agencies are active duty military officers, and the NRO Director is an Undersecretary of the Air Force.) Only the CIA itself – and a comparatively tiny "Community Management Staff" (CMS) – is unambiguously under the authority of the DCI.

The domination of the IC by the Department of Defense is perhaps the most fundamental bureaucratic fact of life for anyone who aspires to manage the Community as a whole. As one organizational history of the CIA has noted, "[t]he DCI never became the manager of the Intelligence Community," and decisions over the years to "us[e] declining resources first and foremost to support military operations effectively blunted the Congressional emphasis upon centralization by limiting the wherewithal that DCIs and agency heads could devote to national and strategic objectives."[15]

Nor is this arrangement entirely accidental. This awkward balance of authority between DCI and the Secretary of Defense reflects an inability finally to decide whether agencies such as NSA and NIMA are "really" national intelligence agencies that should report to the DCI or "combat support agencies" that should report to DOD. The U.S. military, of course, is an enormous – and, in wartime, perhaps the most important – consumer of certain sorts of intelligence product, particularly signals intelligence (SIGINT), photographic and other imagery (IMINT), and mapping products. Without immediate access to such support, our armed forces would have difficulty knowing where they are, where the enemy is, and what the enemy is doing. The reason that the military possesses integral service intelligence arms and cryptologic support components, in fact, is precisely because the imperatives of war planning and operational decision-making do not permit these functions to be entirely separated from the military chain of command. This attitude, however, also exists at the national level: DOD officials insist that organizations such as NSA and NIMA are, above all else, "combat support agencies." Implicitly, this means that in any unresolvable resource-allocation conflict between the Secretary of Defense and the DCI, the Secretary must prevail.

The difficulty lies in the fact that the DOD components of the Intelligence Community are also vital parts of the *national* intelligence system, and provide crucial intelligence products to

---

[15] Warner, *supra*, at 8 & 17.

national-level consumers, including the President. To the extent that DOD's domination of IC resources impedes the Community's ability to provide adequate national-level support – and to the extent that such high-level bureaucratic stand-offs hamper the IC's ability to reorient itself against dangerous emerging threats, or to *reform* itself in response to intelligence failures – we face grave challenges.

These problems have led many to suggest the need finally to empower the DCI to act as the *true* head of the U.S. Intelligence Community. At one pole, such suggestions have included proposals to give the DCI full budgetary and management authority over all IC components – effectively taking them out of DOD and establishing the DCI as something akin to a cabinet-level "Secretary of Intelligence." (Former National Security Advisor Brent Scowcroft has allegedly recommended something to this effect, but his report has never been released – supposedly due to Defense Department opposition.) At the other pole, some in Congress have suggested merely ending the "dual-hatted" nature of the DCI's office by separating the roles of DCI and CIA Director.

In my view, these two poles leave us with a Hobson's choice between the virtually unworkable and the clearly undesirable. Creating a *true* DCI would entail removing dozens of billions of dollars of annual budgets from the Defense Department, and depriving it of "ownership" over "its" "combat support organizations." In contemporary Washington bureaucratic politics, this would be a daunting challenge; DOD and its Congressional allies would make such centralization an uphill battle, to say the least.

Indeed, if anything, the trend in the post-September 11 world is *against* DCI centralization. DOD has asked for, and Congress has now established, a new Undersecretary of Defense for Intelligence (USDI) to oversee and coordinate DOD's intelligence components, creating what may well be, in effect, a Pentagon DCI – and one, moreover, likely to have at least as much influence over the agencies in question than the DCI himself. DOD's Joint Intelligence Task Force for Counterterrorism (JITF-CT) already reproduces at least some of the analytical functions of the CIA's CTC, DIA analysts already supply all-source analysis across a wide range of functional and regional specialties, and press accounts suggest that the Pentagon is increasingly interested in establishing its own parallel covert action capability using Special Operations Forces (SOF) troops.[16] DOD is, in short, creating a parallel universe of intelligence organs increasingly

---

[16] Susan Schmidt & Thomas E. Ricks, "Pentagon Plans Shift in War on Terror; Special Operations Command's Role to Grow With Covert Approach," *Washington Post* (September 18, 2002), at

independent of the DCI. Particularly under a DCI who prizes his role as CIA Director above his Community responsibilities, the prospects for DCI centralization are grim indeed.

On the other hand, without more, proposals merely to separate the DCI's office from that of the CIA Director will likely only make the situation worse. At the moment, one of the few sources of bureaucratic power the DCI enjoys is his "ownership" of what is, in theory at least, the nation's premier intelligence analysis organization – and its only specialist HUMINT collection agency – the CIA. Heading the CIA gives the DCI at least "a seat at the table" in national-level debates: a DCI *without* the limited but non-trivial bureaucratic clout of the CIA behind him would find himself even more marginalized and ineffective than the office is today.

My experience with the fragmented and disjointed Community management process have led me to conclude that the best answer is probably to give more management and budgetary authority over IC organs to an effective DCI focused upon issues of IC coordination and management – as the Joint Inquiry has suggested by urging that we consider the creation of a "Director of National Intelligence" with powerful new Community-management authority. Because he will need to use these new powers to arbitrate between and set policies for self-interested bureaucratic "players" within the Intelligence Community rather than *be* one of them, this augmented DCI (or DNI, as the case may be) should not simultaneously hold the position of CIA Director.

The "combat support" argument is, in my view, overblown. There is nothing to suggest that organizations like NSA and NIMA would *deny* crucial support to the Defense Department the moment that they were taken out of the DOD chain of command. Any lingering doubts about the effectiveness of the Pentagon's "combat support" from intelligence agencies could be allayed by improving the effectiveness and resources devoted to the services' organic intelligence and cryptologic components. (Civilian directors of NSA and NIMA – appointed with DCI and Secretary of Defense concurrance – could serve as Assistant DCIs for SIGINT and IMINT, respectively, serving alongside an Assistant DCI for Military Intelligence, a high-ranking military officer charged with ensuring that the IC is at all times aware of and responsive to military needs.) Best of all, an Intelligence Community finally capable of being coherently managed *as a Community* would be able to reform and improve itself in numerous ways that prove frustratingly elusive today – ultimately providing both its national-level civilian *and* its warfighter customers with better support.

A1.

Congress took a remarkable step in reforming the basic structure of the military command system in 1986 with the passage of the Goldwater-Nichols legislation.[17] This landmark legislation – which reformed the roles of the Chiefs of Staff and created an entirely new system of regional unified commanders – tilted at what were thought to be bureaucratic windmills and ran into fearsome bureaucratic opposition, but it succeeded brilliantly and helped our armed forces find new strength and coherence in war-winning "joint" operations. The success of the Goldwater-Nichols reforms should be a lesson to Intelligence Community reformers today, for it teaches that it *is* possible sometimes to overcome entrenched bureaucratic interests and forge a much more effective whole out of a motley and disputatious collection of parts.

Unfortunately, Congress, the Administration, and the American public have yet to engage in much of a debate about these issues. Perhaps nothing can shock us into serious debates about the fundamental structure of our Intelligence Community if the horror of September 11 cannot, but I am hopeful that the SSCI and HPSCI will make these issues a centerpiece of their agenda for the 108th Congress. I urge them strongly to do so.

C. *An Agile and Responsive IC*

As the 108th Congress takes up these reform challenges, I would like to offer some additional suggestions that I believe would help the IC both meet the challenges it faces today and be prepared for those it may face tomorrow. One of the roots of our problems in coping with threats such as that posed by Al-Qa'ida beginning in the 1990s is that the tools with which we have had to fight transnational terrorism were designed for another era. The U.S. Intelligence Community is hard-wired to fight the Cold War, engineered in order to do a superlative job of attacking the intelligence "targets" presented by a totalitarian superpower rival but nowhere near as agile and responsive to vague, shifting transnational threats as we have needed it to be.

The lesson of September 11, therefore, should be not simply that we need to reform ourselves so as to be able to address the terrorist threat but also that *we need an Intelligence Community agile enough to evolve as threats evolve, on a continuing basis.* Hard-wiring the IC in order to fight terrorists, I should emphasize, is precisely the *wrong* answer, because such an approach would surely leave us unprepared for the next major threat, whatever it turns out to be. Our task must be to ensure that whatever we do to "fix" the problems that helped leave us unprepared in the autumn of 2001, we make sure that the Intelligence Community can change,

---

[17] Public Law 99-433 (October 1, 1986).

adapt, and move in unanticipated directions in the future. Otherwise the IC will face little but a future punctuated by more intelligence failures, more Congressional inquiries, and more Commissions.

This is perhaps the most powerful argument for strengthening the DCI's ability to lead the Intelligence Community *as a community*, insofar as it is notoriously difficult to reorient large bureaucracies under the best of circumstances, and virtually impossible to do so simply by *persuasion.* But there are additional steps that Congress and the Administration should consider in order to make the IC "quicker on its feet" in anticipating and preparing for – and, where that fails, responding to – future threats.

Well short of putting the entire Community under a "Secretary for Intelligence," one way to greatly augment the ability of the Intelligence Community to adapt flexibly and effectively to future threats would be to increase the degree of uniformity in its personnel management system. A homogenized payment and benefits structure for the Community would not necessarily require putting the agencies themselves under the DCI's operational command. It would, however, enable the IC to move personnel and reorganize organizational structures on an *ad hoc* basis much more effectively in response to future developments.

Achieving such organizational flexibility – and the conceptual flexibility that must accompany it – will be essential if the Community is not simply to replace its dangerous and inflexible Cold War hard-wiring with an equally rigid and unadaptable CT paradigm. This is what might be called the "meta-lesson" of our current round of "lessons learned" studies of intelligence failures: we must not only learn the lessons of the past but learn *how* to *keep* learning lessons as we change and adapt in the future. Adopting uniform personnel standards would help the Community ensure that its personnel and organizational units remain unique and valuable individual resources but they would also become *administratively* fungible assets, capable of being reorganized and redirected efficiently as circumstances demand.

The CIA, to its credit, has experimented in recent years with approaches to organizing "virtual stations" – *ad hoc* issue-focused organizations mimicking the structure of an overseas Directorate of Operations outpost, but simply existing within CIA Headquarters. In the future, the IC as a whole will need to learn from (and improve upon) this concept, by developing ways to "swarm" personnel and resources from various portions of the Community upon issues of particular importance as circumstances demand. At the same time, the IC will have to be willing to move personnel resources *out* of programs and organizations that no longer fulfil their missions, or whose targets have been superseded in priority lists by more important threats. We

must, in short, be willing to build new structures and raze old ones in a continual process of "creative destruction" not unlike competitive corporate approaches used in the private sector.

Concomitant with this, it will also be necessary to break the artificial definitional monopoly within the IC that holds that only intelligence professionals actually employed by the traditional collection agencies can engage in collection or analysis of those agencies' signature types of intelligence. We should be open to unconventional HUMINT collection opportunities, for instance, and should not deny non-CIA analysts a chance to provide the analytical "value-added" that can be obtained by making them more aware than they are today of the origins of their information. And we should reject the self-satisfied assumptions of NSA managers that only NSA personnel can be trusted with analyzing "raw" SIGINT data. (Unfortunately, the Administration seems to be heading in precisely the wrong direction in this respect. If recent reports are to be believed, the President intends to ratify the information-monopolistic *status quo* by issuing an Executive Order to make Homeland Security intelligence analysts dependent upon the traditional IC collection bureaucracies to tell these analysts what information is relevant.[18])

The traditional collection agencies *do* have valuable expertise in "their" areas, but this expertise should be used to enrich the Community's pool of intelligence expertise rather than simply as barriers to entry wielded in defense of bureaucratic and financial "turf." Instead, the collection agencies should be charged with certifying – but not running or controlling – training curricula within other IC agencies that will produce competent specialists in the relevant fields. A SIGINT analyst, for instance, should be properly trained to meet the relevant professional standards (*e.g.*, compliance with USSID 18), but there is no reason why he must receive his paycheck from NSA in order to make important contributions to the Community. Agencies such as CIA and NSA with special expertise in a particular "INT" should become jealous advocates and guardians of high professional standards within the Community as a whole, but they should no longer be permitted to use their expertise to maintain parochial information monopolies.

Fundamentally, Congress and the Administration should be willing, over the coming months, carefully to examine the basic structure of the intelligence provisions of the National Security Act of 1947 in light of the circumstances and challenges our country faces today. At a time in which the State Department and the military services provided the only thing resembling national-level information collection and analytical expertise in the entire U.S. Government, the

---

[18] *See, e.g.*, Dan Eggen & John Mintz, "Homeland Security Won't Have Diet of Raw Intelligence," *Washington Post* (December 6, 2002) at 43.

Act set up a "central" intelligence agency to be an objective source of information and to stand above the bureaucratic political infighting of the day. It was to be what Colonel William ("Wild Bill") Donovan had called for in October 1946: "a centralized, impartial, independent agency that is qualified to meet the atomic age."[19] In 2002, however, the CIA no longer quite fulfils that function, now existing as one of many bureaucratic fiefdoms within a sprawling – and Defense-dominated – Intelligence Community.

One possibility to which Congress and the Administration should give very careful consideration is whether we should return to the conceptual inspiration behind the intelligence-related provisions of the National Security Act of 1947: the need for a "central" national level knowledge-compiling entity standing above and independent from the disputatious bureaucracies. Returning to these roots might suggest the need to separate our country's "central" intelligence analytical functions from the resource-hungry collection responsibilities that make agencies into self-interested bureaucratic "players" – that is, to separate human intelligence (HUMINT) collection into a specialized service that would, along with other collection agencies, feed information into a national-level purely analytical organization built around the core of the CIA's Directorate of Intelligence. (The resulting pure-analysis organization would arguably be the sole institution that could appropriately be run *directly* by a new Director of National Intelligence, who would serve as the overall head of the IC and as the President's principal intelligence advisor.) Whether or not we determine that this is the right answer, however – and howsoever we determine that any such agency would interact with a more empowered DCI – our opportunity seriously to consider such changes is *now*.

II. *Information-Sharing*

Perhaps the most fundamental problem illustrated by the findings of the Joint Inquiry Staff (JIS) in connection with the intelligence failures leading up to September 11 relates to the problem of persuading U.S. Intelligence Community agencies to share information efficiently and

---

[19] Thomas F. Troy, *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency* (Langley, Virginia: CIA Center for the Study of Intelligence, 1981), *supra*, at 382 (quoting Donovan); *see also id.* at 408 (noting that "Congress wanted CIA . . . [to be] free from undue military influence as well as Department control."); *id.* at 410 (noting that Donovan "recognized that the appropriate status for intelligence was independence and that such independence required the establishment of an 'agency' free of any other department of government").

effectively. This problem is inextricably tied up with the longstanding problem of ensuring quality intelligence analysis within the Community, for without *access* to a broad range of information upon which to draw inferences and base conclusions, even the best individual analysts necessarily find themselves gravely handicapped.

There exists a fundamental tension in intelligence work between the need for security and the need for sharing information. Increasing the number of persons having access to a particular item of information inevitably leads to at least *some* increase in the likelihood of its compromise, either accidentally or deliberately (*e.g.*, in a "leak" to the press or to a foreign power through espionage). Agencies which possess sensitive information, therefore, tend to prefer to restrict others' access to "their" information. (This is particularly true in an Intelligence Community institutional culture in which knowledge literally *is* power – in which the bureaucratic importance of an agency depends upon the supposedly "unique" contributions to national security it can make by monopolizing control of "its" data-stream.)

On the other hand, *perfectly* secure information is perfectly *useless* information. Since the purpose of intelligence-gathering is to inform decision-making, restricting access inevitably degrades the value of having intelligence collectors in the first place. For good analysis to be possible, expert analysts must be able to perform what is called "all-source intelligence fusion" – drawing upon the available breadth of information in order to tease patterns of "signal" out of the mass of irrelevant and distracting "noise" that comprehensive collection invariably brings in. If good analysis is to form the basis for intelligent policy, moreover, information must be passed along to the policy community in order to inform their actions.

This tension between security and sharing has been part of the fabric of intelligence policy for years, perhaps manifesting itself most clearly in U.S.-British debates during the Second World War over when (or whether) to share high-grade communications intelligence with operational commanders who needed such information in order to win the war against Nazi Germany.[20] Today, similar debates continue as it becomes clear that the sort of sophisticated pattern-analysis

---

[20] *See, e.g.*, F.W. Winterbotham, *The Ultra Secret* (New York: Harper & Row, 1974), at 86; John Winton, *ULTRA At Sea* (New York: Morrow & Co., 1988), at 148; Patrick Beesly, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre, 1939-1945* (London: Greenhill, 2000), 89, 98-100, 189-90, & 279; David Kohnen, "F-21 and F-211: A Fresh Look into the 'Secret Room,'" in *New Interpretations in Naval History: Selected Papers from the Fourteenth Naval History Symposium* ed. Randy Carol Balano and Craig L. Symonds, (Annapolis, Md.,: Naval Institute Press, 2001), at 304 & 327-29.

and semi- or fully-automated "data-mining" capabilities that will be necessary for intelligence analysis to keep up with complex transnational threats such as those presented by Usama bin Laden's Al-Qa'ida organization are not compatible with traditional notions of inter-Intelligence Community secrecy and restrictions upon access based upon an outsider's "need to know" as determined by the agency information-holders themselves.

A. *The Intelligence Community's Failure to "Connect the Dots" Prior to 9/11*

The most fundamental problem identified by the JIS is our Intelligence Community's inability to "connect the dots" available to it before September 11, 2001 about terrorists' interest in attacking symbolic American targets. Despite a climax of concern during the summer of 2001 about imminent attacks by Al-Qa'ida upon U.S. targets, the Intelligence Community (IC) failed to understand the various bits and pieces of information it possessed – about terrorists' interest in using aircraft as weapons,[21] about their efforts to train pilots at U.S. flight schools,[22] about the presence in the U.S. of Al-Qa'ida terrorists Khalid al-Mihdhar and Nawaf al-Hazmi, and about Zacarias' Moussaoui's training at a U.S. flight school – as being in some fashion related to each other.

As the JIS concluded, the IC failed to "connect[] these individual warning flags to each other, to the 'drumbeat' of threat reporting that had just occurred, or to the urgency of the 'war' efforts against Usama bin Laden."[23] Having failed to make that connection, the IC was caught flat-footed when the attack finally came. Accordingly, no effort to "fix" the problems highlighted by September 11 should be taken seriously unless it attempts to address the pervasive problems of information-sharing that afflict our Intelligence Community.

(1) *Terrorist Names*

---

[21] For an account of information available to the Intelligence Community about terrorists' interest in using aircraft as weapons, *see* JIS, written statement presented to SSCI/HPSCI joint hearing (September 18, 2002), at 26-28.

[22] For an account of information available about terrorists' interest in acquiring aviation training at U.S. flight schools, *see* JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 3.

[23] JIS, written statement presented to SSCI/HPSCI joint hearing (September 18, 2002), at 10.

One of the serious problems identified by our Joint Inquiry is the pervasive refusal of the CIA, in the months and years before September 11, to share information about suspected terrorists with the very U.S. Government officials whose responsibility it is to keep them out of the United States: the State Department consular officials who issue visas and the INS officials who man immigration posts at every American port of entry.

As the JIS outlined in its testimony before one of our joint SSCI/HPSCI hearings, the so-called TIPOFF system provides the basic "watchlist" function by which consular and INS officials check visa applicants or U.S. arrivals against lists of suspected terrorists and other undesirables. With respect to suspected terrorists, the TIPOFF database is populated principally through the submission of names from the CIA. Crucially, however, without CIA input, these officials cannot do their job – and even terrorists *known* to the CIA will be able freely to acquire visas and be granted entry if the CIA has neglected to share their names with TIPOFF.

Alarmingly, this is apparently precisely what happened for years, because CIA was unwilling to share more than a small fraction of its information about suspected terrorists with State and INS. Based upon clear internal guidance issued on December 11, 1999, the CIA was *required* to pass to the TIPOFF program the names of *all* persons it suspected of being terrorists.[24] Before September 11, however, the Agency did not consistently do this. Instead, it often provided the names of suspected terrorists to TIPOFF if the CIA already had information indicating that the terrorist planned to travel to the United States.[25] Because of the practical impossibility of knowing the personal travel plans, in advance, of every suspected terrorist in the world, this inevitably meant that the CIA withheld hundreds or perhaps thousands of names from the TIPOFF database – names of persons who were thus free to obtain U.S. visas and walk through INS booths without notice. Indeed, even though it signed an explicit Memorandum of Understanding (MOU) in January 2001 with the FBI, NSA, and State Department on watchlist

---

[24] CIA Office of Congressional Affairs Liaison Officer Gary Dionne, unclassified telephonic communication to SSCI Minority Counsel Christopher Ford (December 9, 2002). The text of the December 11, 1999 guidance, however, is still classified.

[25] CIA officials have informed SSCI staff that this occurred because State Department officials felt overly burdened with having to process all the names. Their account, however, is not consistent with the State Department complaints about CIA practice recorded by the JIS. *See, e.g.*, JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 15. In any event, it is clear that the "rules of the road" involved the CIA passing comparatively few names in violation of its own rules: by no one's account were the 1999 guidelines actually consistently followed as written.

procedures, State Department officials have complained to the JIS that the CIA still did not share many of its terrorism-related Critical Intelligence Report (CIRs) with the TIPOFF program in the months leading up to the September 11 attacks.[26]

What's more, the CIA apparently did not take its watchlisting responsibilities very seriously even when it *did* see fit to pass some names to TIPOFF. According to the JIS, the CIA provided its employees no training in this regard.[27] Indeed, one CIA official from the Counterterrorism Center's special cell devoted to tracking Al-Qa'ida told the JIS that he didn't feel that his organization needed to worry about whether anyone watchlisted Al-Qa'ida terrorists.[28] The CIA, therefore, apparently neither trained nor encouraged its employees to follow its own rules on watchlisting – embodied in the December 1999 guidance – and they clearly did not do so.[29]

Nor, despite repeated inquiries about watchlisting standards, did the CIA apparently ever disclose the existence of this guidance to the JIS. As the JIS has recounted, "[w]e were told that there was, at the time, no formal system in place at the CTC for watchlisting suspected terrorists."[30] This, however, was not true. As noted above, the CIA's December 1999 guidance specifically provided watchlisting standards – which were often ignored. By failing to provide this information to the JIS, the CIA thus managed to keep the fact that it violated its own rules out of the formal report of the Joint Inquiry.

The magnitude of the CIA's watchlisting failures and the potential impact of this information-hoarding upon our country's preparedness for terrorist attack may be seen in the contrast between the CIA's pre-September 11 performance in this respect and its performance after the attacks. Within a month after September 11, the CIA provided more than 1,500 CIRs to

---

[26] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 15.

[27] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 7-8.

[28] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 8.

[29] Strangely, to judge from the testimony given in Joint Inquiry hearings by JIS representatives, the JIS does not seem ever to have discovered that the CIA had "hard" guidance in place requiring such watchlisting. The CIA, however, has now provided me with a copy of its classified December 1999 guidance.

[30] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 7.

TIPOFF that had it had previously withheld. The State Department reported a 455 percent increase in the number of names CIA provided during the months after the attacks – with the total provided rising from 1,761 during the three months before September 11 to 4,251 in the three months afterwards.[31] But for the shock of September 11, these *thousands* of potential terrorists would presumably still be free to obtain visas and enter the United States without anyone asking any questions, thanks to the CIA's apparent belief that only *it* can be trusted with its information. As it turns out, two of the September 11 hijackers did precisely this.

(2) *The al-Mihdhar and al-Hazmi Story*

What such watchlisting problems can mean in practice is illustrated by the failures of the CIA and FBI in dealing with Al-Qa'ida-affiliated terrorists Khalid al-Mihdhar and Nawaf al-Hazmi. Their story is ably recounted by in the body of the JIS report, but its highlights are worth repeating here. Al-Mihdhar and al-Hazmi attended a terrorist meeting in Kuala Lumpur, Malaysia, in early January 2000.[32] This meeting was known to – and surveiled by – the CIA, which already knew that al-Mihdhar possessed a multiple-entry visa permitting him to travel to the United States. The National Security Agency (NSA) also independently possessed information linking al-Hazmi to Al-Qa'ida. Neither the CIA nor NSA, however, saw fit to provide their names to the TIPOFF database.[33] There is apparently some confusion over whether the CIA told the FBI anything about al-Mihdhar and al-Hazmi. CIA e-mail traffic reviewed by the JIS, however, suggests that the CIA did brief the FBI in general terms . The CIA, however, still did not bother to tell the FBI that al-Mihdhar had a multiple-entry visa that would allow him to enter the United States.[34]

In early March 2000, the CIA learned that al-Hazmi had arrived in Los Angeles on January 15. Despite having just learned of the presence in this country of an Al-Qa'ida terrorist, the CIA told no one about this. The internal cable transmitting this information, in fact, contained

---

[31] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 15.

[32] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 5.

[33] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 6.

[34] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 6-7.

the notation: "Action Required: None, FYI."[35] This information came at the height of the U.S. Intelligence Community's alarm over Al-Qa'ida's "Millennium Plot," and al-Hazmi's arrival had occurred at about the same time the CIA knew that Al-Qa'ida terrorist Ahmed Ressam was also supposed to have arrived in Los Angeles to conduct terrorism operations.[36] Still, however, the CIA refused to notify anyone of al-Hazmi's presence in the country.

By this point, both al-Mihdhar and al-Hazmi – both terrorists known to the CIA – were living in San Diego under their true names. They signed these names on their rental agreement, both used their real names in taking flight school training in May 2000, and al-Mihdhar even used his real name in obtaining a motor vehicle identification card from the State of California.[37] In July 2000, al-Hazmi even applied to the INS for an extension of his visa, sending in this application using both his real name and his current address in San Diego (where he would remain until that December).[38] INS, of course, had no reason to be concerned, since the CIA had withheld the two terrorists' names from TIPOFF. Nor did the FBI have any reason to look for them – *e.g.*, by conducting a basic Internet search for their names or by querying its informants in Southern California – since the last it had heard from CIA was that these two terrorists were overseas.

The CIA's failure to watchlist al-Mihdhar and al-Hazmi became even more alarming and inexplicable in January 2001, when the CIA discovered that the Malaysia meeting had also been attended by a suspect in the *USS Cole* bombing. This presumably made the two terrorists even more interesting to the CIA – and their known presence in the U.S. even more dangerous, by confirming their linkages to Al-Qa'ida operational cells – but the CIA still did not bother to inform TIPOFF. This failure was particularly damaging because al-Mihdhar was overseas at the time: putting his name on the watchlist would have enabled INS agents to stop him at the

---

35 JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 7; *see also generally* CIA officer, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 3.

36 JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 8 & 10.

37 JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 8.

38 JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 8-9.

border.[39]

Even when given the opportunity to tell the FBI – in face to face meetings – about the presence of these two terrorists in the United States, the CIA refused. At a meeting in June 2001 with FBI officials from the New York Field Office who were working on the *USS Cole* case, a CIA official refused to tell them that al-Mihdhar and al-Hazmi had come to the United States.[40]

Meanwhile, Khalid al-Mihdhar was in Jeddah, Saudi Arabia, and applied for a new U.S. visa in June 2001. The State Department officials who took this application appear to have followed procedures and checked his name against their CLASS database, which incorporates TIPOFF watchlist information. Because CIA continued to refuse to put the name of this Al-Qa'ida terrorist into TIPOFF, however, no CLASS "hits" occurred, and al-Mihdhar was given a visa and returned to the United States unmolested in July.[41]

The CIA only decided to watchlist al-Hazmi and al-Mihdhar in late August 2001, by which point they were already in the United States and in the final stages of preparing for the September 11 attacks.[42] By this point, tragically, it was too late for the FBI – hamstrung by its own investigative regulations – to stop them. Although the FBI scrambled in late August and early September to locate the two terrorists in the United States,[43] it denied itself the services of any of its own agents assigned to criminal work and refused even to conduct a basic Internet search that would have revealed al-Hazmi and al-Mihdhar living under their true names in San Diego. (According to testimony from an FBI agent in New York who conducted just such an Internet

---

[39] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 9; *see also* CIA official, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 4; Michael Rolince, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 2.

[40] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 21; *see also id.* at 10.

[41] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 10.

[42] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 10; *see also* Rolince, *supra*, at 3.

[43] JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 11.

search *after* the September 11 attacks, finding al-Mihdhar's address "within hours."[44]) It also denied itself any assistance that could have been obtained from Treasury officials in tracking down al-Mihdhar and al-Hazmi through their credit card or banking transactions. As it turned out, however, on September 11, 2001, the two men boarded American Airlines Flight 77, and helped fly it into the Pentagon.

(3) *The "Phoenix Memo"*

The affair of the FBI Electronic Communication (EC) sent by the Phoenix field office to FBI Headquarters in order to warn officials about potential dangers from Al-Qa'ida-affiliated individuals training at U.S. flight schools, also illustrates the tremendous difficulty our Intelligence Community has had with sharing information and "connecting the dots" – particularly where the FBI is concerned.

The FBI special agent in Phoenix who sent the EC to headquarters on July 10, 2001, addressed his memorandum to the Usama bin Laden Unit (UBLU) and the Radical Fundamentalist Unit (RFU) within the Bureau's counterterrorist organization. Headquarters personnel, however, decided that no follow-up was needed, and no managers actually took part in this decision or even *saw* the memorandum before the September 11 attacks.[45] The CIA was made aware of the Phoenix special agent's concerns about flight schools, but it offered no feedback[46] despite the information the CIA possessed about terrorists' interest in using aircraft as weapons. Nor did the new FBI officials who saw the Phoenix EC at headquarters ever connect these concerns with the body of information already in the FBI's possession about terrorists' interest in obtaining training at U.S. flight schools.[47] The full contents of the "Phoenix Memo" have yet to be made public, but it is astonishing that so little was made of it, especially since it drew readers' attention to certain information *already in the FBI's possession* suggesting a very specific reason to be alarmed about

---

44 FBI Agent from New York Field Office, testimony before joint SSCI/HPCSI hearing (September 20, 2002), *available from* Federal News Service (response to question from Senator Shelby).

45 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 2.

46 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 6.

47 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 11-13.

one particular foreign student at an aviation university in the United States.[48]

(4) *Missed Opportunities*

Altogether, the al-Mihdhar/al-Hazmi and "Phoenix EC" stories suggest both the potential of sophisticated information-sharing and good information-empowered analysis and the dangers of *failing* properly to "connect the dots." It is impossible to know, of course, whether the September 11 plot could have been disrupted – or at least significantly delayed – had the FBI and CIA acted properly in sharing and understanding information available to them. The evidence, however, suggests a number of pregnant "what ifs":

> If the CIA had been willing to share its information about al-Mihdhar and al-Hazmi with consular and INS officials through the TIPOFF program, one or both of them might have been apprehended upon entering or reentering the United States after their Malaysia meeting.
>
> If the CIA had informed the FBI when it first knew that al-Mihdhar and al-Hazmi were in the United States – and the FBI had permitted itself to do common-sense things like use the Internet – these two terrorists might have been located at their home in San Diego (or in flight school in the area) long before the September 11 attacks. Surveillance of them might have led the FBI to other hijackers, or to operational cell leaders, or their deportation might have disrupted the plot.
>
> If the FBI had been able to "connect the dots" between the Phoenix EC and the body of information already in the FBI's possession about terrorist interest in U.S. flight schools – and information held by the Intelligence Community about terrorists' interest in using aircraft as weapons – it might have been better able to investigate Zacarias Moussaoui and obtain information on some of the other September 11 hijackers from information in Mouassaoui's computer and in his personal effects.

---

[48] FBI Special Agent in Phoenix, Arizona, electronic communication addressed to Radical Fundamentalist Unit *et al.* (July 10, 2001), at 5. The FBI declined to declassify any more specific an account of this information.

> If the FBI had understood the full significance of the Phoenix EC in light of this other information, they might have begun to conduct the follow-up work recommended by the Phoenix special agent. In May 2001, the FBI had already briefly considered opening an investigation upon one of the individuals named in the EC, but this was dropped when it was discovered he was out of the country at the time. Had the Phoenix EC spurred serious follow-up by FBI Headquarters, however, this individual's name might have been added to the TIPOFF watchlist – leading investigators right to him upon his subsequent return to the United States. Restarting the aborted investigation of this individual would likely also have led the FBI to his radical fundamentalist flight school classmate in Arizona, September 11 hijacker Hani Hanjour.[49]

The September 11 story, therefore, should be an object lesson in the perils of failing to share information promptly and efficiently between (and within) organizations, and in the need to ensure that intelligence analysis is conducted on a *truly* "all-source" basis by experts permitted to access *all* relevant information – no matter where in the Intelligence Community it happens to reside.

B. *Pervasive Problems of Information-Sharing*

That effective information-sharing and truly all-source analysis should have been such a scarce commodity in counterterrorism work during the months and years leading up to September 11 – years during which the Director of Central Intelligence supposedly believed the U.S. Intelligence Community to be "at war" with Al-Qa'ida and made fighting it his highest priority – is a testament to the recurring problems of agency parochialism and information-hoarding. Even Community-wide attempts to "fix" the problem of information-sharing, such as the DCI's ongoing development of the computerized Intelligence Community-Wide System for Information Sharing (ICSIS), simply replicate the problem. ICSIS will be built around a series of agency-specific electronic "shared spaces" accessible to users of the system, but populated only with such information as each agency sees fit to permit others to see.[50] ICSIS will, in other words,

---

[49] JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 10.

[50] It is not even clear that ICSIS will meet the Community's needs even on its own terms. In January 2001, the NIMA Commission report recommended that NIMA begin building a new information-management system essentially from scratch, notwithstanding ICSIS planned deployment over the next ten years. *See* Dr. Robert C. Norris, written statement presented to

presumably speed access to what agencies *are* willing to share, but it will do nothing to address broader issues of their unwillingness to permit experts from *other* intelligence agencies any window upon the data-streams the monopolization of which is the source of each host agency's bureaucratic power.[51]

Such information-hoarding thus goes deeper than simply being "policy," often reaching the level of simple reflex. For instance, the FBI for years monopolized the processing of information obtained from surveillance under the Foreign Intelligence Surveillance Act (FISA) – even though it fell hopelessly behind in processing FISA "raw data" and accumulated vast backlogs of untranslated tapes that were of no use to anyone. Thus also does the NSA insist that only *its* employees can be trusted with handling "raw" signals intelligence (SIGINT) data under the standards prescribed by U.S. Signals Intelligence Directive (USSID) 18. And the CIA's

---

joint SSCI/HPSCI hearing (October 1, 2002), at 4.

[51] The culture of information-holder control is formally enshrined most obviously in the "originator control" (ORCON) classification caveat, which requires that anyone given access to a certain piece of information *not* reveal it to anyone else without explicit permission from its originating agency. According to FBI official Michael Rolince, the ORCON caveat made it very difficult for the FBI to pass intelligence information to criminal investigators in terrorism cases, "even for lead purposes," because the originating agency (frequently the CIA) would refuse to allow it. *See* Michael Rolince, written statement presented to joint SSCI/HPSCI hearing (September 20, 2002), at 4. According to the JIS, ORCON rules present a major problem to efficient information-sharing, because they impose upon sharing arrangements a cumbersome and lengthy case-by-case adjudication process. *See* JIS, written statement presented to joint SSCI/HPSCI hearing (October 1, 2002), at 6. Our Joint Inquiry also discovered this to be the case, encountering frequent delays allegedly because of the necessity of clearing ORCON transmittals to Congress.

In travels and discussions with U.S. Allies currently engaged in helping us fight the war against terrorism, SSCI Members and staff have heard many complaints that the U.S. classification caveat "no foreign" (NOFORN) has also unnecessarily impeded information-sharing. Even our closest military allies have privately complained about what they describe as the unnecessary and reflexive use of the NOFORN caveat by U.S. officials. This has frequently resulted in U.S. intelligence officers stamping "NOFORN" on information provided to them by those same allies, denying these contributors to our war and intelligence efforts the ability to see the intelligence products we make out of their information. The Intelligence Committees attempted to draw attention to this "NOFORN problem" in § 831 of the Fiscal Year 2003 Intelligence Authorization Bill (Public Law 107-306), which requires that the DCI and the Secretary of Defense report to Congress on the impact of NOFORN practices upon allied intelligence-sharing relationships.

Directorate of Operations usually refuses even to let *CIA analysts* see its own operational cable traffic.

Reading the DCI's authority to protect intelligence "sources and methods" as barring the disclosure of source information not simply to the public or to U.S. adversaries but also to *anyone else in the U.S. Intelligence Community*, the CIA has proven unwilling to permit others a window upon the context that source information can occasionally provide. CIA information-hoarding is hardly a problem unique to the al-Mihdhar and al-Hazmi story. The CIA also refused requests by U.S. Navy intelligence officers to turn over highly relevant information about the source of an intelligence warning that might have prompted the Navy to direct the *USS Cole* away from Yemen in October 2000.

As the Senate and House Intelligence Committees have seen repeatedly, the Intelligence Community shares information poorly and reluctantly, at best. Especially since September 11, Community representatives have assured us on innumerable occasions that their coordination and information-sharing problems have been fixed: it has become their mantra that such cooperation is now "seamless" and "unprecedented." Even today, however, these sharing arrangements consist principally of the assignment of agency personnel for reciprocal details at counterpart agencies (*e.g.*, FBI personnel at the CIA, and CIA personnel at the FBI). (Nor is the CIA's CTC much of a "joint" center in the military sense, since the overwhelming majority of its personnel are CIA employees. It was, and remains, a CIA organization.)

Such cross-detailing, as we have long known and as testimony before our Joint Inquiry hearings has made doubly clear, is at best "an imperfect response" to the information-sharing problem.

> "The almost unanimous opinion among the detailing agencies is that host agencies still restrict access to information and limit the databases that can be queried by detailees from other agencies on grounds of personnel or information security, and intelligence policies."[52]

Such detailees commonly bring special experience and contextual knowledge to their assignments that host-agency personnel may lack, but they are seldom fully trusted by their host

---

[52] JIS, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 7.

agencies and are seldom, if ever, permitted to know as much as "real" agency employees. Moreover, even when detailees are given comparatively good access to host-agency information, they are almost invariably prohibited from passing it back to their home organizations. This, for instance, is the fate of non-FBI officials assigned to the FBI-run Joint Terrorism Tracking Task Forces (JTTFs).[53] It is also that of DIA analysts cross-assigned to other IC agencies.[54] As Rear Admiral Lowell Jacoby recounted in testimony submitted to the Joint Inquiry, cross-assigned personnel are routinely denied "unfettered and unconditional access to all relevant . . . information" and are often not permitted to transmit to their home agencies what they *are* permitted to see.[55]

Today, the "seamless" and "unprecedented" information-sharing within our Intelligence Community remains built around personal contacts and such cross-details. According to FBI Counterterrorism chief Dale Watson, the FBI's arrangements with the CIA and with other U.S. Government agencies revolve principally around the "exchange of working level personnel and senior managers at the headquarters level."[56] This may represent considerable progress compared with what prevailed before September 11, but it is woefully inadequate to our intelligence needs in the 21st century.

C. *The Future of Information-Sharing*

(1) *The Imperative of "Deep" Analyst Data-Access*

The greatest contributions that intelligence analysis can make against vague, shifting, and inherently ambiguous transnational threats such as international terrorism lie in analysts' capacity to conduct "all-source fusion" of information – performing the classic task of assembling fragmentary information into actual or inferential "mosaics" and teasing useful "signals" out of the

---

53 JIS, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 7-8.

54 JIS, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 13.

55 RADM Lowell E. Jacoby, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 5.

56 Dale Watson, written statement presented to SSCI/HPSCI joint hearing (September 26, 2002), at 4 & 6.

"noise" brought in by our wide-ranging means of intelligence collection. Problems of information-hoarding and dysfunctional sharing methodologies, however, restrict analysts' ability to apply their talent, training, and experience against intelligence targets in a truly *all-source* fashion. If they are to be expected to have success against such modern targets in the future, we will need to do a great deal to improve their ability to survey and draw patterns out of the masses of data that exist in discrete and carefully-guarded bundles throughout the Intelligence Community.

Intelligence collectors – whose status and bureaucratic influence depends to no small extent upon the monopolization of "their" information-stream – often fail to recognize the importance of providing analysts with "deep" access to data. The whole *point* of intelligence analysis against transnational targets is to draw patterns out of a mass of seemingly unrelated information, and it is crucial that the analysis of such patterns not be restricted only to personnel from a single agency. As Acting DIA Director Lowell Jacoby observed in his written testimony before the Joint Inquiry, "information considered irrelevant noise by one set of analysts may provide critical clues or reveal significant relationships when subjected to analytic scrutiny by another."[57]

This suggests that the fundamental intellectual assumptions that have guided our Intelligence Community's approach to managing national security information for half a century may be in some respects crucially flawed, in that it may *not* be true that information-*holders* – the traditional arbiters of who can see "their" data – are the entities best placed to determine whether outsiders have any "need to know" data in their possession. Analysts who *seek* access to information, it turns out, may well be the participants best equipped to determine what *their* particular expertise and contextual understanding can bring to the analysis of certain types of data.

In this vein, the Military Intelligence Board has explicitly suggested that deep information-sharing will require a re-examination of traditional concepts of "need to know" – although, not surprisingly, traditional collection agencies such as the CIA still contest this conclusion.[58] Rear Admiral Jacoby made the point firmly to our Joint Inquiry, writing that it should be the task of intelligence reformers

---

[57] RADM Lowell E. Jacoby, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 4.

[58] JIS, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 12.

> "to create a new paradigm wherein 'ownership' of information belonged with the analysts and not the collectors. In my opinion, one of the most prolonged and troubling trends in the Intelligence Community is the degree to which analysts – while being expected to incorporate the full range of source information into their assessments – have been systematically separated from the raw material of their trade."[59]

Sadly – and dangerously – the result of this systematic separation is that "groundbreaking, innovative, true all-source analysis" has become "the exception, not the rule" in today's Intelligence Community.[60]

The imperative of "deep" analyst data-access is intertwined with another dynamic. For some time, our ability to analyze information has been falling increasingly behind the enormous volumes of information collected by our intelligence agencies. This imbalance between analysis and collection has been the subject of numerous SSCI hearings. It has important implications for the future of information-sharing within the Intelligence Community because it suggests that in addition to being empowered to conduct *true* "all-source" analysis, our analysts will also need to be supplied with powerful new tools if they are to work their analytical magic upon such large information volumes.

As Rear Admiral Jacoby has suggested, the challenge for intelligence reform is thus twofold: we must persuade information-holders to give analysts "deeper" and less conditional access to data than they have ever before enjoyed, and we must equip analysts with the tools needed to "mine" these data-streams for useful information.

> "[W]e need to find a way to immediately and emphatically put the 'all' back into all-source analysis. . . . If we expect analysts to perform at the level and speed expected in a counterterrorism mission environment characterized by pop-up threats, fleeting targets, and heavily veiled communication, they require immediate, on-demand access to data from *all* sources and the ability to mine,

---

[59] Jacoby, *supra*, at 6.

[60] *Id.*

manipulate, integrate, and display all relevant information."[61]

As noted previously, making information accessible necessarily exists in some tension with keeping it secure – and some balance must always be sought between *usability* and *security*. I have come to the conclusion that our Intelligence Community, dominated by traditional collection agencies such as CIA and NSA that enjoy special status precisely because of the monopolization of "their" data-streams (*e.g.*, HUMINT and SIGINT), has drawn this line in ways incompatible with our intelligence needs in the 21st century. I thus believe, with RADM Jacoby, that we must bring about a radical change in the access collection agencies give to all-source analysts, including all-source analysts from outside their own ranks.

Such analyst empowerment must be accomplished in ways that do not leave our secrets unduly vulnerable to compromise. It is thus the challenge of reform not only to persuade recalcitrant information-hoarders into making their databases available to sophisticated analytical exploitation but also to ensure that the resulting information architectures are secure. There is no reason why appropriately cleared analysts should not be trusted with such information: they are no less patriotic, no less committed to protecting national security, and no less professional in their fields than the collection bureaucrats who would presume to deny them access. That said, of course, there is every reason to develop comprehensive security protocols and accountability systems to reduce the risk of espionage or accidental compromise that is to some degree inherent in any expansion of the universe of persons given access.

Fortunately, recent efforts to move forward in empowering analysts to conduct *true* all-source analysis provide reasons for confidence that a workable solution is possible. As the SSCI's Technical Advisory Group (TAG) – a nonpartisan group principally composed of expert private sector technologists and managers with the highest possible security clearances – has forcefully recommended, we must move forward into the realm of comprehensive databasing and data-mining *now*, and the technology we need is either in existence already or well on its way to development. As this technology advances, the TAG has suggested, agency resistance to such developments in the name of "security" is looking increasingly like a mere excuse:

> "The technology of multi-level-security databases and computer systems is highly developed, and all that stands between the present

---

[61] RADM Lowell E. Jacoby, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 7.

moment and the operation of such a database in the National interest is political will."[62]

(2) *Faltering Steps Forward*

In efforts to meet the analytical challenge of transnational terrorism, both the Department of Defense (DOD) and the Department of Justice (DOJ) have undertaken new experiments in all-source fusion aimed at the targets. At DOD, the Defense Intelligence Agency set up an organization it calls Joint Intelligence Task Force-Counterterrorism (JITF-CT). Established in the wake of the bombing of the *USS Cole* by Al-Qa'ida members in October 2000, and augmented by new assignments of personnel and resources after the September 11 attacks, JITF-CT aspires to provide its analysts with deep data access sufficient to permit real all-source fusion. According to RADM Jacoby, DIA's aim in establishing JITF-CT was to create a "stand-alone limited access data repository accredited to host the entire range of terrorism related information, regardless of source" – including not just "highly compartmented intelligence," but also "law enforcement information related to ongoing investigations or prosecutions, and security incident reporting sometimes catalogues as criminal, rather than terrorism activity." JITF-CT seeks to "apply state-of-the-practice technological tools and expertise that enhance opportunities for 'analytic discovery.'"[63]

The Attorney General established his own Foreign Terrorist Tracking Task Force (FTTTF) after September 11 in order to help develop "deep"-access data-mining techniques and apply these new methodologies to the formidable challenge of catching terrorists operating within the United States. FTTTF is co-located with the Pentagon's Joint Counterintelligence Assessment Group (JCAG, a.k.a. the Counterintelligence Field Activity, or CIFA), which provides technical support.[64] As with JITF-CT, FTTTF/JCAG aspires to bring about great innovations in analyst access to and data-mining of disparate "all-source" data-streams.

The experience of these innovative analytical cells, however, is simultaneously

---

62 SSCI Technical Advisory Group, "TAG Findings-&-Recommendatinos Post-9/11," memorandum to Senators Bob Graham and Richard Shelby (April 3, 2002), at 3.

63 RADM Lowell E. Jacoby, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 2.

64 JIS, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 15-16.

encouraging and dispiriting. It is encouraging in that it shows a commendable interest in inter-agency information-sharing on something approaching – or at least aspiring to – a truly all-source basis, and enabled by state-of-the-art analytical tools. Nonetheless, it is also dispiriting in that the available evidence suggests that these organizations are experiencing some notable "pushback" by the traditional information-holders within the Intelligence Community. According to RADM Jacoby, for instance, JITF-CT and DIA are still being denied information by "those intelligence and law enforcement organizations that are the 'owners' or 'arbiters' of unshared information." "This is no small problem" as Jacoby emphasizes, for although the

> "un-shared information falls largely into the categories of background and contextual data, sourcing, seemingly benign activities, and the like . . . it is within these categories that the critical 'connecting dot' may well be found."[65]

The CIA has its own "all-source" fusion cell devoted to terrorist targets, in the form of the DCI's Counterterrorism Center (CTC). The CTC has performed this function for some years, and not without some success. Even CTC has had difficulty penetrating the veil of agency information-hoarding. Although as an operational arm of the CIA staffed principally by Directorate of Operations personnel, the CTC is denied far less information in CIA operational cables than organizations such as JITF-CT, it still encounters information-sharing problems in dealing with *other* organizations. In particular, timely and effective access to law enforcement information has been a traditional weakness at CTC, and the NSA has refused to permit the Center access to "raw" SIGINT data. Moreover, another weakness of CTC as an *analytical* fusion cell is precisely its *operational* focus: CTC plays a vital role in spearheading our country's campaign to disrupt and dismember terrorist cells overseas, but this necessarily means that it devotes less time to purely *analytical* work on terrorism than would otherwise be the case. Indeed, not unlike FBI analysts diverted to "operational" support to ongoing investigations (see below), CTC analysts apparently spend a great proportion of their time providing analytical support to CTC's ongoing *operations*.

More than a year after September 11, there is still "no single agency or database or computer network that integrates all counter terrorism information nationwide."[66] And there is no

---

[65] RADM Lowell E. Jacoby, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 5.

[66] JIS, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 5.

center devoted entirely to counterterrorist analysis on a truly all-source basis. As former Representative Lee Hamilton emphasized in testimony before our Joint Inquiry, this is a significant unmet need within the Intelligence Community.

> "We need a center in the government for all intelligence – foreign and domestic – to come together. There is currently no place in the government where we put together data from all of our domestic and foreign sources – the CIA, FBI, Department of Defense, Department of State, NSA, and other agencies."[67]

(3) *Technological and Bureaucratic Empowerment*

(a) *"Total Information Awareness"*

To help address the need for technological change to support the kind of analyst empowerment that our Intelligence Community needs, Dr. Robert Norris of the National Defense University and RADM Jacoby of DIA argued that the IC should take its cue from the private sector and move toward a common data format standard. Such a standard, they suggested, would allow data-interoperability – as opposed to *system* interoperability, which is much more challenging and is perhaps unattainable [68] – across the Community, or even across the federal government as a whole.

> "Interoperability at the data level is an absolutely necessary attribute of a transformed intelligence environment because it enables horizontal integration of information from all sources – not just intelligence – and at all levels of classification."[69]

In this regard, RADM Jacoby suggested that the Community follow the commercial world in

---

[67] Lee Hamilton, written statement presented to SSCI/HPSCI joint hearing (October 3, 2002), at 4.

[68] Dr. Robert C. Norris, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 10 (*quoting* LTG Peter Cuviello); *see also id.* at 7 (*quoting* Brig. Gen. Michael Ennis).

[69] RADM Lowell E. Jacoby, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 8.

embracing eXtensible Markup Language (XML) was a way to ensure such data-interoperability.[70]

Interestingly, an ongoing project by the Information Awareness Office (IAO) of the Defense Advanced Research Projects Agency (DARPA) suggests that while such data-interoperability would be enormously useful, it may not be an absolute prerequisite for meaningful "deep access" data-mining within the Intelligence Community, the U.S. Government, or beyond. The SSCI has been following with great interest IAO's work on what it calls its "Total Information Awareness" (TIA) project, for this project holds out the prospect of providing the technological tools to achieve radical analyst empowerment vis-á-vis the IC's entrenched information-holders.

TIA aspires to create the tools that would permit analysts to data-mine an indefinitely-expandable universe of databases. These tools would not be database-specific, but would rather be engineered in such a way as to allow databases to be added to the analytical mix as rapidly as interface software could be programmed to recognize the data formats used in each new database and to translate queries and apply specific "business rules" into a form usable therein. Through this system, TIA hopes to enable an analyst to make search requests – either on a name-by-name basis or in order to apply sophisticated pattern-recognition software – to each among a "cloud" of remotely-distributed databases. Each analyst user would possess a complex set of individual "credentials" which would be embedded in each query and "travel" with that query through the database universe. These credentials would include information such as the user's access permissions and the specific legal and policy authorities under which each query has been conducted; they would tell the system what sorts of responses that user is permitted to get.[71] Even when the user did not have authority to see certain types of information, the system would be able to tell the analyst whether any data responsive to his query existed in any particular database, allowing him to submit a request for access to higher authority.[72] Information responsive to user queries would then be passed back through the system to an automated data

---

70 *Id.*

71 The TIA project also contemplates a system of "selective revelation of information," whereby initial responses to a query would indicate merely the presence of responsive entries or patterns. Subsequent queries – and perhaps additional levels of authority – would be needed for the analyst to "bore deeper" into the data.

72 This helps analysts get avoid the "you don't know what you don't know" dilemma, yet without compromising particularly sensitive information to unauthorized individuals.

repository, where it would be stored for analytical exploitation.[73]

The TIA approach thus has much to recommend it as a potential solution to the imperative of deep data-access and analyst empowerment within a 21st-century Intelligence Community. If pursued with care and determination, it has the potential to break down the parochial agency information "stovepipes" and permit nearly pure *all*-source analysis for the first time – yet without unmanageable security difficulties. If done right, moreover, TIA would be infinitely scalable: expandable to as many databases as our lawyers and policymakers deem to be appropriate.[74]

TIA promises to be an enormously useful tool that can be applied to whatever data we feel comfortable permitting it to access. How broadly it will ultimately be used is a matter for policymakers to decide if and when the program bears fruit. It is worth emphasizing, however, that TIA would provide unprecedented value-added even if applied exclusively *within* the current Intelligence Community – as a means of finally providing analysts deep but controlled and accountable access to the databases of collection and analytical agencies alike. It would also be useful if applied to broader U.S. Government information holdings, subject to laws restricting the use of tax return information, census data, and other information. Ultimately, we might choose to permit TIA to work against some of the civilian "transactional space" in commercially-available

---

[73] IAO officials have told committee staff that DARPA envisions the possibility of supporting analysts with semi-automated functions that would "learn" from the behavior of large numbers of other users on the system, "pushing" data out to users working on specific topics in ways loosely analogous to the way in which the software at Amazon.com recommends books to browsers based upon what *other customers* who selected a particular title also picked.

[74] What's more, the TIA architecture is being designed to create elaborate audit trails upon the initiation of each query. These audit trails, which would be accessible to intelligence oversight organs, would be specially encrypted and secured against tampering, and would allow overseers to hold each accredited user accountable for activity undertaken within the system and information gleaned therefrom. Moreover, developing TIA will apparently not involve the use of any data from actual persons (*e.g.*, information about real Americans). IAO plans to construct a "virtual" economy filled with huge numbers of "synthetic" personal transactions by millions of hypothesized people. A "red team" would develop and "carry out" attacks within this virtual environment, role-playing the parts of individual terrorists in order to create transactional trails. The software developers would then try to develop programs to identify these patterns of "terrorist" transactions, picking them out of the "noise" of the "synthetic" civilian transactions in which they will be embedded. This approach, DARPA hopes, will identify the best ways to identify real terrorists while minimizing the system's intrusion upon the transactional records of *non*-terrorists.

databases which are already publicly and legally available today to marketers, credit card companies, criminals, and terrorists alike. The point for civil libertarians to remember is that policymakers can choose to restrict TIA's application however they see fit: it will be applied only against the data-streams that our policymakers and our laws permit.

I mention TIA here at some length because it represents, in my view, precisely the kind of innovative, "out of the box" thinking of which I have long been speaking – and which Americans have a right to *expect* from their Intelligence Community in the wake of a devastating surprise attack that left 3,000 of their countrymen dead. It is unfortunate that thinking of this sort is most obvious in the Defense Department rather than among Intelligence Community leaders, and more unfortunate still that projects like TIA are likely to encounter significant *resistance* from the entrenched information-holders at the core of the traditional IC. Nevertheless, projects like this represent a bright spot in the Community's baleful recent history of counterterrorist information-sharing.

(b) *Homeland Security Intelligence Fusion*

Another bright spot is the potential for a fresh start that is presented by the new Department of Homeland Security. The Homeland Security bill signed by President Bush on November 25, 2002 contains provisions which I wrote specifically in order to help address these information-sharing problems within the Intelligence Community and between other federal agencies. Specifically, this new law makes it the responsibility of the Undersecretary for Information Analysis and Infrastructure Protection at the Department of Homeland Security to

> "establish and utilize . . . a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section . . . ."[75]

This language is complemented by the strong information-access provisions I also wrote into the bill. These provisions provide appropriately-cleared Homeland Security analysts with authority affirmatively to *access* (*i.e.*, not simply to be *given*):

---

[75] Public Law 107-296 (November 25, 2002), at § 201(d)(14).

> "*all* information, including reports, assessments, analyses, and unevaluated intelligence related to threats of terrorism against the United States . . . that may be collected, possessed, or prepared by any agency of the Federal Government."[76]

Read together, as they were intended to be, these provisions provide statutory authorization for a radical new approach to counterterrorist information-sharing in which analysts are for the first time given the ability to conduct *real* "all-source" analysis and to "connect the dots" in order to protect our nation from terrorists.

It was my hope with this legislation to begin to move our Intelligence Community, to paraphrase former DIA Director Thomas Wilson, beyond the realm of information "sharing" entirely, inasmuch as "sharing" connotes information *ownership* by the party that decides to share it, an idea that is antithetical to *truly* empowering analysts to connect all the right "dots."[77]

My views on this subject have been powerfully reinforced by the findings of the Joint Inquiry, which has recommended that Congress work diligently to ensure the success of the Homeland Security information analysis office – including ensuring that it gets "full and timely access to all counterterrorism-related intelligence information," including all the "'raw' supporting data" it needs. While it certainly remains in President Bush's power to stop his new Homeland Security organization short of leading the way toward this new paradigm, it is my hope – and it was the inspiration behind my contributions to Title II of the Homeland Security bill and the recommendations of the Joint Inquiry – that he will use this historic opportunity to bring the U.S. Intelligence Community into the 21st century. I dearly hope that, recent press reports to the contrary,[78] the Administration will not squander the opportunity to make true all-source fusion finally work to protect Americans from terrorism.

(4) *The Other Side of the Coin: Protecting National Security Information*

In the context of information sharing, a quick word should also be said about the need to

---

[76] *Id.* at § 202(a)(1) (emphasis added).

[77] *See* JIS, written statement presented to SSCI/HPSCI joint hearing (October 1, 2002), at 13 (citing VADM Thomas Wilson).

[78] *See, e.g.*, Eggen & Mintz, *supra*, at 43.

protect national security information from unauthorized disclosure. Those of us with regular access to highly classified information cannot help but be appalled by the frequency with which the publication within the Intelligence Community of enormously sensitive reports is quickly followed by sensationalistic press accounts of that very same information. The President, the Secretary of Defense, and other officials have all stated emphatically the dangers posed by the endemic culture of media "leaks" in modern Washington. As Attorney General Ashcroft has noted, "there is no doubt and ample evidence that unauthorized disclosures of classified information cause enormous and irreparable harm to the nation's diplomatic, military, and intelligence capabilities."[79] As we have learned during the course of this Joint Inquiry, our Intelligence Community's ability *personally* to track Usama bin Laden himself was lost in 1998 on account of a senior official's boasting to the media about a certain type of collection capability. We simply *cannot* hope to fight the war on terrorism with sustained success if we continue to see our intelligence activities and capabilities featured in the press as part of what Senator Pat Roberts has described as "the leak of the week."

Unfortunately, however, our current laws against disclosing classified information are far too weak, and investigations of leaks usually far too difficult, for prosecutors to have had any success in pursuing them. Indeed, in the last half-century, I am aware of only *one* non-espionage case in which someone was prosecuted for an unauthorized disclosure. The SSCI and HPSCI tried to address this issue in 2000 by placing a section in our Fiscal Year 2001 intelligence authorization bill that would have made it a felony for someone with authorized access to classified information knowingly to disclose it to someone not authorized to receive it.[80] President Clinton, however, vetoed the bill.

Now that the war on terrorism has refocused us upon the potentially appalling consequences of our culture of leaks, the 108th Congress should take up and enact this legislation anew – and President Bush should sign it. Such anti-leaks legislation will become more important than ever as we move into the 21st century world of true "all-source" fusion and automated data-mining within the Intelligence Community. We should also bear continually in mind the admonition contained in the Joint Inquiry's recommendation to consider the degree to which "excessive classification" has impeded the IC's ability to handle the information-management responsibilities we ask of it. We must both punish leaks of information *and* ensure that the only

---

[79] Attorney General John Ashcroft, letter to Vice President Dick Cheney (October 15, 2002).

[80] *See* S.2507 (106th Congress, 2d Sess.), at § 303.

information subject to classification is that which truly needs to be.

III. *Intelligence-Law Enforcement Coordination*

Another of the discouraging lessons of September 11 is the extent to which the United States' law enforcement agencies (LEAs) and its Intelligence Community (IC) still have not managed to work effectively with each other. Progress has been made in this regard since the terrorist attacks, thanks in large part to Congress' prompt passage of the USA PATRIOT Act of 2001 (Public Law 107-56). This remains an area, however, in which much improvement is needed – as well as sustained Congressional oversight to ensure that these agencies really do make cooperation part of their institutional culture over the long run.

A. *FISA and Its Discontents*

Much of the blame for the dysfunctional nature of pre-September 11 LEA/IC coordination can be traced to a series of misconceptions and mythologies that grew up in connection with the implementation of domestic intelligence surveillance (and physical searches) under the Foreign Intelligence Surveillance Act (FISA).[81] Rigid and restrictive readings of FISA in the early and mid-1990s acquired with time the apparent legitimacy of long-presumed acceptance, and created a sterile and ultimately fallacious conventional wisdom that effectively – but unnecessarily – *prevented* meaningful LEA/IC coordination.

(1) *Development of the "No Coordination" Myth*

Much of the pre-September 11 problems with FISA can be traced to confusions associated with participants' understandings of the so-called "purpose test" embodied in the statute. Under FISA as it existed before 2001, a surveillance or search order could only be obtained if, among other things, the government was able to certify – and a federal judge on the FISA court agreed – that "the purpose" of the undertaking was to collect foreign intelligence information.

Taking their cue from *non-FISA* caselaw setting forth the constitutional rules for warrantless intelligence surveillance, most courts interpreting FISA – and essentially all intra-Executive Branch officials who dealt with these matters – read FISA's "the purpose" language as

---

[81] 18 U.S.C. § 1801 *et seq.*

imposing the requirement that the "primary" purpose of the requested surveillance or search be the collection of foreign intelligence. Warrantless surveillance cases such as *Truong*[82] arising out of activities undertaken before the passage of the FISA statute, had helped create what became known as the "primary purpose" test. Technically, the seminal "primary purpose" cases did not apply to surveillance conducted under FISA, a statute enacted by Congress in order to establish a special, court-overseen system of domestic intelligence surveillance and thus to replace the pre-FISA constitutional standard with a specified statutory one. Nevertheless, it did not take long for courts and commentators alike to interpret FISA as incorporating the pre-FISA "primary purpose" test.

As the FISA Court of Review ably explained in a recent landmark decision (and the first case ever heard by that appellate body established by the FISA statute in 1978), FISA itself imposes few, if any, restrictions upon intelligence/law enforcement coordination. Indeed, according to the Court of Review, the very *idea* that there exists a "dichotomy" between "criminal" and "intelligence" purposes was merely an unwarranted assumption that subsequent participants in the FISA process imagined into the law.[83] Nevertheless, in short order it had become the conventional wisdom of U.S. intelligence oversight law that FISA incorporated the "primary purpose" test – and thus that there must at some point be a limit to the permissible degree of "criminal investigative" involvement in electronic surveillance or physical searches[84] under FISA.

More importantly – and, as it turns out, far more perniciously – this half-imagined "purpose test" itself came to be interpreted extremely rigidly, in ways that in time came to be seen effectively to preclude *any* meaningful coordination between criminal investigators and intelligence personnel even in terrorism and espionage cases. As first discussed publicly in connection with a report on the Wen-Ho Lee affairs by the Chairman of the Senate Governmental

---

82 *United States* v. *Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980).

83 *See* Foreign Intelligence Surveillance Court of Review, *In re: Sealed Case No. 02-001* (November 18, 2002) [hereinafter "Court of Review Opinion"], at 18-19.

84 Physical searches were not covered by the original FISA statute, being added to the law in 1995. (Before that point, therefore, physical searches still fell under the pre-FISA constitutional standards for warrantless surveillance.)

Affairs Committee in 1999,[85] and as subsequently detailed both in a General Accounting Office (GAO) study[86] and the declassified findings of a special Justice Department review – the Attorney General's Review Team (AGRT) headed by Assistant U.S. Attorney Randy Bellows, which produced the so-called "Bellows Report"[87] – DOJ attorneys adopted a hyper-restrictive, and legally unnecessary, approach to FISA applications. This approach, as was apparently intended, maximized the likelihood of FISA order requests being approved by the Foreign Intelligence Surveillance Court (FISC) and certainly minimized FISA "intrusions" upon American privacy.[88] It came at the cost, however, of prohibiting a great deal of useful *and quite lawful* information-sharing and coordination between intelligence and criminal investigators.

As best I have been able to piece these things together today – and in its recent decision on these matters, the FISA Court of Review (COR) disclaimed any real certainty about when these problems first arose[89] – the most damaging manifestations of this phenomenon came about after 1995, in the wake of the espionage prosecution of senior CIA officer (and Soviet mole) Aldrich Ames. Criminal and intelligence investigators in that case allegedly cooperated closely, so

---

85 Fred Thompson & Joseph Lieberman, "Special Statement on "Department of Energy, FBI, and Department of Justice Handling of the Espionage Investigation into the Compromise of Design Information on the W-88 Nuclear Warhead" (August 5, 1999), *available at* http://www.senate.gov/~gov_affairs/_080599_china_espionage_statement.html (visited August 23, 2001).

86 General Accounting Office, *Coordination Within Justice on Counterintelligence Criminal Matters is Limited* (July 2001) [hereinafter "GAO Report"].

87 Attorney General's Review Team, *Final Report on the Handling of the Los Alamos National Laboratory Investigation* (May 2000), declassified version [hereinafter "Bellows Report"].

88 These debates, of course, came up with most vehemence in connection with proposed FISA surveillance or physical searches of the property of "United States persons" – that is, U.S. citizens, lawful permanent residents, or U.S. corporations, *see* 50 U.S.C. §§ 1801(i) (providing definition) – because FISA imposes special rules for dealing with U.S. persons, *see id.* at § 1801(a), 1804(a), & 1825(a). FISA surveillance and searches are much more easily available, under the statute, against non-U.S. persons such as foreign diplomats or facilities within the United States. *See, e.g., id.* at § 1802(a)(1) (permitting surveillance of premises exclusively controlled by a foreign power without need for court approval).

89 *See* Court of Review Opinion, *supra*, at 10 (suggesting that this dynamic may have begun "at some point during the 1980s").

closely that lawyers within Attorney General Janet Reno's Justice Department apparently became convinced that they might "lose" the Ames case if defense counsel asked the trial judge to suppress evidence obtained by intelligence surveillance on the grounds that this collection had "really" been for *criminal* purposes.

As it turned out, Ames' guilty plea brought the case to a conclusion before this issue could be joined. Unsettled by the episode, Clinton Administration lawyers apparently concluded that they would in the future essentially *prohibit* coordination between criminal and intelligence investigators. The Attorney General issued special guidelines in July 1995 setting forth standards for information-sharing and coordination between FBI agents working on FISA cases or other intelligence investigations and attorneys in DOJ's Criminal Division. These guidelines *did* permit some cooperation, specifying standards for when the Criminal Division was to be notified of information.[90]

As detailed by GAO, however, these guidelines were never really enforced within DOJ. With these guidelines standing, in effect, in abeyance, DOJ attorneys – especially those within the Office of Intelligence Policy and Review (OIPR), which serves as the Department's "gatekeeper" on FISA matters – were free to interpret FISA as banning essentially *any* contact between FISA investigators and the Criminal Division. As GAO and a special internal DOJ report have recounted, coordination on intelligence cases dropped off significantly after the guidelines were issued, and what contact *was* undertaken commonly occurred so late in the process as to be substantively useless.[91] According to some participants, meetings between FBI intelligence investigators and Criminal Division attorneys became "unproductive," and even "weird" and "surreal." The new restrictions imposed by OIPR prevented the FBI from obtaining "meaningful advice from the Criminal Division during an FCI [foreign counterintelligence] investigation," and impeded "the FBI's ability to do its job."[92] In short order, OIPR attorneys turned the "primary purpose test" into a *de facto* "'exclusive' purpose" test.[93] No FISA request was permitted to go

---

[90] Attorney General Janet Reno, "Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations," memorandum to Assistant Attorney General, Criminal Division, *et al.* (July 19, 1995).

[91] *See* GAO Report, *supra*, at 14.

[92] Bellows Report, *supra*, at 732-33.

[93] *See* GAO Report, *supra*, at 14.

forward if there was *any* meaningful coordination between criminal and intelligence investigative organs, and similar "no-coordination" standards were applied to all FCI and counterintelligence investigations. Denied any meaningful ability to coordinate actions between the LEA and IC spheres, the FBI developed a Byzantine system of parallel investigative tracks for working terrorism issues: "dirty" teams of intelligence investigators and "clean" teams of purely criminal-focused agents would work the same terrorist cases at the same time, "[y]et they rarely talk[ed] to each other."[94] This organizational allergy even to the most common-sense forms of counterterrorist cooperation become infamous after September 11: a "Wall" had been built between intelligence and law enforcement.

(2) *Manifestations in the September 11 Intelligence Failure*

Spurred by Congressional attention given to OIPR's excessively restrictive approach to FISA during the Wen-Ho Lee affair – and by the scathing critique of that office offered in the Bellows Report – DOJ began to realize in the final months of the Clinton Administration that it had created a significant national security problem for itself. On January 21, 2000, Attorney General Reno promulgated some new "interim measures," but she failed to adopt new guidelines before leaving office. Revised formal guidance, however, was not forthcoming until set forth in August 2001 by Deputy Attorney General Larry Thompson.[95] This clarified the rules for coordination between law enforcement and intelligence organs, emphasizing that notification of the Criminal Division is *mandatory* when information is developed that "reasonably indicate[s] that a significant federal crime has been, is being, or may be committed."[96]

These new rules, however, did not make major changes in the 1995 guidelines, and were clearly insufficient to change the institutional culture that had developed within the FBI and the Justice Department around what was now the virtually unchallenged conventional wisdom of the "no coordination" myth. Investigators working before September 11 to get to the bottom of alarming terrorist cases such as those of Khalid al-Mihdhar, Nawaf al-Hazmi, and Zacarias Moussaoui repeatedly ran into the "Wall" and its institutional side-effects: an investigative culture

---

94 *See, e.g.*, Roberto Suro, "FBI's 'Clean' Team Follows 'Dirty' Work of Intelligence," *Washington Post* (August 16, 1999), at A13.

95 Deputy Attorney General Larry Thompson, "Intelligence Sharing," memorandum to Assistant Attorney General Michael Chertoff *et al.* (August 6, 2001).

96 *Id.* at 2.

positively allergic to LEA/IC information-sharing and coordination, and remarkably ignorant about how much such cooperation was actually allowed.

FBI special agents in the New York Field office working on the Bureau's investigation of the bombing of the Navy destroyer *USS Cole* by Al-Qa'ida, for instance, met with CIA officials in June 2001 in an effort to obtain information. At this point, the CIA knew both that al-Mihdhar and al-Hazmi were linked to a prime suspect in the *Cole* attack *and* that they were both in the United States, but it refused to give the FBI this information. Former CIA CTC chief Cofer Black later testified before Congress that the CIA's refusal to tell the FBI about these two terrorists loose in the United States had been entirely consistent with "rules against contaminating criminal investigators with intelligence information."[97] As one of the FBI agents involved in this episode put it,

> "'[t]he Wall', and implied, interpreted, created or assumed restrictions regarding it, prevented myself [sic] and other FBI agents working a criminal case out of the New York Field Office to obtain information from [the] Intelligence Community, regarding Khalid al-Mihdhar and Nawaf al-Hazmi in a meeting on June 11, 2001."[98]

Nor was this all. After the FBI was belatedly notified by the CIA in August 2001 that known Al-Qa'ida terrorists al-Mihdhar and al-Hazmi were in the United States, the Bureau began trying to track them down. Despite the urgency of this task, however, FBI Headquarters prohibited FBI criminal investigators in New York from participating in the search for these terrorists and refused even to tell them what little was known about the two men at the time. As one of the New York agents was informed in an e-mail from Washington, D.C., "that information will be passed over the wall" only if "information is developed indicating the existence of a substantial federal crime."[99] Perceiving there to be an unbridgeable gap between law enforcement and intelligence work, the FBI thus refused even to talk to *itself* in order to prevent mayhem by known Al-Qa'ida terrorists in the United States. Meanwhile, al-Mihdhar and al-Hazmi were in

---

[97] Cofer Black, written statement presented to joint SSCI/HPSCI hearing (September 26, 2002), at 3.

[98] JIS, written statement presented to joint SSCI/HPSCI hearing (September 20, 2002), at 21.

[99] JIS, written statement presented to joint SSCI/HPSCI hearing (September 20, 2002), at 21.

the final stages of their preparations for the September 11 attacks.

As noted by the JIS, these information sharing problems clearly "reflect misunderstandings that have developed over the last several years about using information derived from intelligence gathering activities in criminal investigations."[100] DOJ's "policies and practices regarding the use of intelligence information in FBI criminal investigations" helped make it enormously harder for the government to find al-Mihdhar and al-Hazmi in the last weeks before September 11[101] – even though they were both living and traveling under their true names at the time, and a simple Internet search requested by one of the New York FBI agents *after* the World Trade Center attacks yielded their address in San Diego "within hours."[102] The tragedy of this is that it was so needless: the law actually *did* not bar all cooperation across the "Wall" between law enforcement and intelligence. It was simply *assumed* to do so because years of timorous lawyering in the Justice Department and Intelligence Community reticence had created an institutional culture hostile to coordination. As FBI official Michael Rolince put it, procedures for information-sharing became so baroque and restrictive that sharing was essentially prohibited: "In terrorism cases, this became so complex and convoluted that in some FBI field offices agents perceived 'walls' where none actually existed."[103]

Coordination problems also arose in the Moussaoui case, in which FBI agents in the Minneapolis Field Office were desperate to search Moussaoui's personal effects for clues about his activity. Even though Moussaoui was in government custody, however, FBI agents were prohibited from looking through his computer and papers without court permission. FBI Headquarters actually *prohibited* intelligence investigators in Minneapolis from notifying the Criminal Division at the Justice Department about the Moussaoui situation, and *prohibited* agents

---

100 JIS, written statement presented to joint SSCI/HPSCI hearing (September 20, 2002), at 13 (*quoting* e-mail message sent on August 29, 2001, from FBI Headquarters to FBI Special Agent in New York City).

101 JIS, written statement presented to joint SSCI/HPSCI hearing (September 20, 2002), at 20.

102 FBI Agent from New York Field Office, testimony before joint SSCI/HPCSI hearing (September 20, 2002), *available from* Federal News Service.

103 Michael Rolince, written statement presented to joint SSCI/HPSCI hearing (September 20, 2002), at 4.

from pursuing a criminal search warrant against him.[104]

FBI Headquarters apparently barred the pursuit of a criminal warrant on the theory that any professed interest in criminal prosecution would jeopardize any chances of a FISA – a reasonable assumption given OIPR's longstanding approach to such matters.[105] When the FBI agents actually contacted Headquarters about obtaining such a FISA order, however, they were given inexcusably confused and inaccurate information from attorneys at the FBI's National Security Law Unit (NSLU). FBI attorneys at Headquarters told Minneapolis that in order to get a FISA, they had to produce evidence showing that Moussaoui was affiliated with one or more groups on the State Department's official list of "terrorist" organizations. This legal advice was patently false and has no basis either in the FISA statute or in DOJ policy or guidelines. Nevertheless, this bad advice led the Minneapolis agents on a legal wild goose chase for nearly three weeks, as they tried to find enough information connecting Chechen terrorist organizations – with whom Moussaoui had some ties, but who were not on the list – to Al-Qa'ida.[106]

(3) *Developments Since September 11*

Since the September 11 attacks, both Congress and the Justice Department have taken important steps to revise the law and policies restricting law enforcement/intelligence coordination. The myth that FISA prohibited essentially all coordination between intelligence and law enforcement agents, while untrue even under pre-September 11 law, was addressed by Congress' passage of the USA PATRIOT Act of 2001 (Public Law 107-56), which took aim directly at the "primary purpose" test long assumed to be part of FISA case law. Whereas FISA for years had provided that "the purpose" of FISA surveillance had to be intelligence collection, after President Bush's signature of the USA PATRIOT Act, FISA said merely that orders are to

---

104 JIS, written statement presented to joint SSCI/HPSCI hearing (September 24, 2002), at 17-18.

105 During the Wen-Ho Lee affair, for instance, OIPR chief counsel Francis Fragos Townsend had rebuffed FBI attempts to get a FISA order in early 1999 because the FBI was by that point *considering* pursuing a criminal search warrant against Lee. According to contemporaneous notes taken by FBI officials, Townsend rejected the FBI's efforts to renew FISA discussions with the dismissal that the case had become "way too criminal." *See* Thompson & Lieberman, *supra*, at 13.

106 JIS, written statement presented to joint SSCI/HPSCI hearing (September 24, 2002), at 19-20; *see also* Minneapolis FBI Agent, testimony before joint SSCI/HPSCI hearing (September 24, 2002), *available from* FDCH Political Transcripts (September 24, 2002)..

be granted where this is "a significant purpose."[107] Thereafter, no inference of a "primary" purpose test should have been permitted, much less an "exclusive purpose" standard. After October 26, 2001, the FISA statute permitted surveillance and physical searches even for undertakings that were *primarily* criminal – provided only that intelligence collection was not an *insignificant* reason for the undertaking.

It took over a year, however, for the USA PATRIOT Act changes to penetrate the U.S. Government's entrenched "no coordination" bureaucratic culture. In November 2001, immediately *after* Congress had enacted the "significant purpose" change to FISA, the Foreign Intelligence Surveillance Court broke with previous precedent and for the first time *required* DOJ and the FBI to follow the Attorney General's *July 1995 guidelines* on law enforcement-intelligence coordination.[108] Although court approval was necessary under the FISA statute for the establishment of FISA "minimization rules" for handling information on U.S. citizens or lawful permanent residents, the FISC had never before seen fit to enforce specific general rules on coordination between intelligence and law enforcement organs. The July 1995 guidelines had been the creation of the Attorney General's policy discretion, and the FISC had never required them to be followed during the long years of the late 1990s when they were being ignored by DOJ attorneys seemingly hostile to the very *idea* of such coordination. Yet the moment that Congress changed the law in order to make clear that it intended there to be no "Wall," the FISC stepped in to *impose* the very legal standards repudiated by the USA PATRIOT Act.

With its November 2001 ruling imposing the July1995 guidelines upon the post-September 11 Justice Department, the FISC necessarily established the precedent that any *changes* to the coordination guidelines required court approval. Things got still more strange after the Attorney General duly submitted draft guidelines in March 2002, seeking the FISC's approval to implement the changes written into law by the USA PATRIOT Act. These new proposals embodied the "significant purpose" changes, and permitted extensive information-sharing and coordination between intelligence and law enforcement elements within the Department and the FBI – to the point that "*all* DOJ component are free to offer advice and make recommendations, both strategic and tactical, about the conduct and goals of the

---

[107] Public Law 107-56 (October 26, 2001), at § 218.

[108] *See* Court of Review Opinion, *supra*, at 21-22 (recounting history of case).

investigations."[109]

The FISC, however, rejected the Attorney General's proposed changes, declaring in a May 17, 2002 opinion that they went too far. Wholly ignoring the USA PATRIOT Act's changes to the FISA "purpose test," this opinion explicitly *endorsed* what the FISC itself described as "the Wall" between law enforcement and intelligence – finding support for this not in the crucial "purpose test" modified by Congress but in the statute's substantively unrelated provisions on "minimization rules" to govern the handling of information specifically about U.S. persons.[110]

It was not until November 2002 that the FISA Court of Review – the never-before-used appellate body created by the statute – issued an opinion overruling the FISC's decision. Thanks to the Court of Review holding, the law thus stands today where Congress *intended* it to stand on October 26, 2001: there is no restriction upon coordination between law enforcement and intelligence organs in connection with FISA surveillance or physical searches, and such activity can lawfully be undertaken even if *primarily* done with prosecutorial intent, provided that a "significant" intelligence purpose remains.[111] Given its erratic and reflexive behavior after September 11, how faithfully the FISC actually applies this standard to individual FISA requests

---

109 "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI," memorandum from Attorney General John Ashcroft to FBI Director *et al.* (March 6, 2002), at 2.

110 *See* Foreign Intelligence Surveillance Court, *In re: All Matters Submitted to the Foreign Intelligence Surveillance Court*, Memorandum Opinion (as Corrected and Amended), multiple docket numbers (May 17, 2002) [hereinafter "FISC Opinion"], at 18 & 22-27.

111 Ironically, the law stands here today even though the Court of Review held that before the USA PATRIOT Act there really was never any "dichotomy" between a FISA order's "intelligence" and "criminal" purpose *in the first place.* As the Court of Review explained the law, under FISA as originally written, even a *wholly* prosecutorial purpose *should* have been acceptable – insofar as putting spies and terrorist behind bars and/or using the threat of prosecution to "squeeze" them for information *was* an entirely legitimate "intelligence" purpose. According to the Court of Review, the USA PATRIOT Act, by purporting to loosen a "purpose test" that Congress wrongly assumed to exist, actually *imposed* a balancing test between "criminal" and "law enforcement" purposes for the first time. The bottom line, however, is that FISA law today *actually* says what Congress *intended* it to say after the passage of the USA PATRIOT Act.

remains to be seen.[112] Provided that the FBI can persuade its NSLU attorneys to *learn* FISA law better – and provided that Attorney General Ashcroft succeeds in replacing the "Wall" culture with new attitudes devoted to effective coordination – there is reason for optimism that coordination-related problems of the sort seen in the al-Mihdhar, al-Hazmi, and Moussaoui cases will not recur.

(4) *Intelligence-Law Enforcement Information-Sharing*

In addition to problems stemming from presumed legal obstacles to passing crucial information from the Intelligence Community to law enforcement, the events of September 11 highlighted the problems of passing information in the other direction: from law enforcement *to* the Intelligence Community. Throughout the 1990s, for instance, the Justice Department, the FBI, and the offices of various U.S. Attorneys around the country accumulated a great deal of information about Al-Qa'ida and other terrorist networks operating within the United States. This information was derived from law enforcement investigations into such events as the 1990 assassination of Rabbi Meier Kahane, the 1993 World Trade Center bombing, the abortive plot to blow up various harbors and tunnels in New York City, the 1996 Khobar Towers attack, the 1998 U.S. embassy bombings, Al-Qa'ida's "Millennium Plot," and the attack on the *USS Cole* in October 2000. Most of this information, however, remained locked away in law enforcement evidence rooms, unknown to and unstudied by counterterrorism (CT) analysts within the Intelligence Community.

---

[112] There is some room for concern that the FISC's legal instincts have become too congruent with the "Wall" mentality. As the Court of Review acidly suggested in a barbed footnote to its November 2002 opinion, some of the FISC's eagerness to defend mistaken concepts of the "Wall" may have stemmed from the fact that an OIPR attorney closely associated with "Wall" thinking recently took up a position as FISA clerk to the federal district judges serving on the FISC. *See* Court of Review Opnion, *supra*, at 20 n.15. The attorney in question is Allan Kornblum, who achieved a degree of notoriety in FISA circles as the DOJ lawyer perhaps most personally responsible for the Department's much-criticized interpretation of "probable cause" under the FISA statute during the Wen-Ho Lee affair. *See* Fred Thompson & Joseph Lieberman, transcript of press conference (August 5, 1999) (*available from* Federal News Service), at 2-3 (remarks of Senator Thompson describing OIPR's "highly restrictive view of probable cause" as "a faulty interpretation") & 4 (remarks of Senator Lieberman, noting that he "disagreed" with OIPR's "judgment call"); Bellows Report, *supra*, at 482 (concluding that the Wen-Ho Lee FISA application indeed "established probable cause" and "should have resulted in the submission of a FISA application, and the issuance of a FISA order").

That this information possessed potentially huge relevance to the Intelligence Community's CT work is beyond question. Indeed, until the late1990s, at least, U.S. law enforcement offices probably had more information on Al-Qa'ida – its key members operating in the West, its organizational structure, and its methods of operation – than the CIA's CTC. Two CT specialists from the Clinton Administration's National Security Council later described court records from 1990s terrorism trials as being "a treasure trove" that contained "information so crucial that we were amazed that the relevant agencies did not inform us of it while we were at the NSC."[113] A small office within the Office of Naval Intelligence, for instance, began a whole new field of inquiry into terrorist maritime logistics networks in the summer of 2001 on the basis of a single FBI interview form (a "Form 302") and the public court transcripts from the 1998 embassy bombings trials in New York, long before anyone had even *tried* systematically to "mine" law enforcement records for intelligence-related information.[114] That most such law enforcement information remained off limits to intelligence analysts before September 11 is terribly, and perhaps tragically, unfortunate.[115]

Even apart from coordination-related concerns about the "Wall" discussed previously, the sharing of law enforcement information with the IC was fiercely resisted by law enforcement

---

[113] Daniel Benjamin & Steven Simon, *The Age of Sacred Terror* (New York: Random House, 2002), at xii-xiii.

[114] This office, known as the Maritime Target Development Division (MTDD), has since been elevated to the status of full-fledged Department office within the ONI organization.

[115] The degree to which law enforcement information remained so firmly embedded within records unsearched by intelligence analysts can perhaps be seen in the failure of our own JIS to identify within Intelligence Community records what is perhaps the earliest known reference by an Islamic fundamentalist to a plot to attack buildings such as the World Trade Center towers. After U.S. law enforcement authorities captured El-Sayyid Nosair after his assassination of Rabbi Meier Kahane in 1990, they found in one of his notebooks a lyrical description of the need to destroy "the enemies of Allah . . . by means of destroying exploding [sic], the structure of their civilized pillars such as the touristic infrastructure which they are proud of an their high world buildings which they are proud of . . . ." *See* Benjamin & Simon, *supra*, at 6. More than a decade after this evidence was seized, the JIS' searches of Intelligence Community databases for information that might have presaged the September 11 attacks has apparently produced *not a single reference* to this pregnant early warning signal by an Islamic fundamentalist now long known to have been linked to Sheikh Omar Ahmad Abdel Rahman and the terrorist cell responsible for the 1993 World Trade Center attacks and involved in plotting to blow up multiple tunnels and monuments in New York City thereafter.

officials. Some of this was unavoidable, insofar as information protected by Rule 6(e) of the Federal Rules of Criminal Procedure – that is, grand jury information – really could *not* lawfully be passed to intelligence analysts. Like the mythology of the coordination "Wall" in the years before September 11 the "Rule 6(e) excuse" acquired an unwarranted mythological dimension of its own.

Rule 6(e) restricts the disclosure of information *actually revealed* in the confidence of the grand jury chamber. This prohibition, however, does not actually reach *other* information in the possession of law enforcement entities, such as FBI "Form 302" witness interview records, documents obtained in response to search warrants, "lead" information acquired from sources, and so forth. Even during the most secretive grand jury investigation, in other words, there is a huge amount of information that can be shared with intelligence officials without running afoul of Rule 6(e). (Such information may be highly sensitive, of course, but protecting sensitive sources and methods is hardly something with which the Intelligence Community lacks experience.)

Sadly, however, Rule 6(e) increasingly came to be used simply as an excuse for *not* sharing information – leaving vital collections of *shareable* information about international terrorist groups off-limits to IC intelligence analysts. For years, it was routine FBI and DOJ practice to respond to virtually *any* Intelligence Community requests for information with the answer that "Rule 6(e)" prevented any response. As two frustrated NSC veterans describe it,

> "Rule 6E [sic] is much more than a procedural matter: it is the bulwark of an institutional culture, and as Justice Department lawyers readily admit, it is used by the Bureau far more often than it should be. It is one of the Bureau's foremost tools for maintaining the independence that the FBI views as its birthright."[116]

Indeed, by this account, NSC officials met with Attorney General Reno in 1993 about the obstacles this dynamic presented for counterterrorism analysis. "Although the issue was revisited many times over the next four years," nothing happened: "The FBI balked at the proposal, and [Attorney General] Reno, although she was [FBI Director] Louis Freeh's boss, could never bring him around."[117]

---

[116] Benjamin & Simon, *supra*, at 227.

[117] *Id.*

After the surprise attacks on September 11, the new Justice Department of Attorney General Ashcroft worked with Congress to put the Rule 6(e) issue to rest. Apparently working from the assumption that it would be easier to change the law itself than to fix a parochial and dysfunctional institutional culture that used the Rule as an excuse to prevent *all* information-sharing, they determined simply to *change* Rule 6(e) to permit information-sharing with intelligence officials. This change was incorporated into the USA PATRIOT Act.[118]

As the law stands today, even intelligence-related information that derives exclusively from revelations within the confines of the grand jury chamber may freely be shared with the Intelligence Community. The USA PATRIOT Act, in fact, permits sharing criminal wiretapping information[119] and more generally authorizes information-sharing "[n]otwithstanding any other provision of law"[120] – thus sweeping within its ambit not only Rule 6(e) but also 18 U.S.C. § 2517 and any other rule that might providing an excuse to hoard information. Indeed, Title IX of the Act included a provision that, subject to the Attorney General's establishment of procedures and standards for such sharing, *requires* law enforcement organs to pass information with intelligence significance to the Intelligence Community.[121]

(5) *Recommendations*

Organizational cultures are notoriously hard to change, and it remains to be seen how well the legal and policy changes of the post-September 11 period will become part of the institutional fabric of the Justice Department and the FBI. In the interest of ensuring that sustained progress is made in this regard, Congress probably made a mistake in subjecting the broad "notwithstanding any other provision of law" sharing provision and the "significant purpose" FISA amendment in the USA PATRIOT Act to that bill's "sunset" clause – which will cause these important provisions to expire in December 31, 2005.[122] If it wishes to see these improvements in information-sharing and law enforcement-intelligence coordination succeed in the long term, the

---

118 P.L. 107-56, at § 203(a).

119 *Id.* at § 203(b).

120 *Id.* at § 203(d).

121 *Id.* at § 905.

122 *See id.* at § 224(a) (providing for expiration of certain provisions).

108th Congress should consider exempting them from the "sunset" provision.[123]

The 108th Congress should also reintroduce and promptly approve the amendment to FISA proposed in June 2002 by Senators Kyl and Schumer. This legislation – which was introduced during the 107th Congress as S.2586 – would modify the "foreign power" definition in the FISA statute to permit the issuance of surveillance or search orders against *non*-U.S. persons suspected of international terrorist activity but whose ties to a specific foreign terrorist "group" cannot initially be shown. Debates continue in FISA circles about whether Zacarias Moussaoui's ties to the Chechen rebels were sufficient to provide a "foreign power" nexus under the existing FISA statute. Discussions of the Moussaoui case, however, have made clear that there is a potential loophole in the law that might be exploited by *future* terrorists.

Specifically, as discussed in a public hearing of the SSCI during the summer of 2002, the FISA statute is built around a 1970s-era conception of the "international terrorist group." When FISA was enacted in 1978, the typical terrorist group was a Marxist-style organization with a fairly rigid, authoritarian organizational structure and chain of command (*e.g.*, Baader-Meinhoff gang, the Red Brigades, the PLO, the Red Army Faction, the PFLP, and so forth). Terrorist organizations today, however, have increasingly "flat" or "networked" organizational structures, tending to be decentralized and comparatively resistant to institutional "decapitation." Moreover, as the FBI's Deputy General Counsel has noted, terrorism today is far more indiscriminate and more focused simply upon causing mass casualties than were terrorist groups at the time FISA

---

[123] Congress should also closely monitor the Intelligence Community's *use* of grand jury and other protected law enforcement information. Such information is quite properly subject to oversight by federal judges while it remains within law enforcement channels. When passed to the Intelligence Community, however, it leaves the courts' control and oversight. Since the Department of Justice has taken the position that the intelligence oversight committees of Congress should not be permitted to see any grand jury information, this means that there is *no* oversight of what use is made of grand jury material passed to the Intelligence Community. The Senate Select Committee on Intelligence tried to provide for such oversight in its FY03 authorization bill, *see* S.2506 (107th Cong., 2d Sess.), at § 306, but this provision was removed in conference at the insistence of the Administration. The 108th Congress would do well to consider the civil liberties implications of passing grand jury information to the Intelligence Community without effective oversight – as well as the implications for the oversight prerogatives of Congress more generally, as such information is incorporated over time into intelligence products denied to the committees because they contain such material.

was adopted.[124] Whereas terrorist groups in the 1970s tended to focus upon achieving specific political goals or upon targeting specific individuals, often using the *threat* of violence as much as violence itself (*e.g.*, in hostage-taking situations), modern terrorist groups are increasingly interested simply in annihilating their perceived enemies on as grand as scale as technologically feasible.

Modern terrorists, therefore, are both more lethal *and* harder to tie to formal "group" structures than the terrorists Congress had in mind when enacting the FISA statute's current definition of a terrorist "foreign power." Senators Kyl and Schumer have proposed to permit FISA orders to issue against even a single individual who appears to be involved in terrorism, provided that such a person is not a U.S. person and that his terrorism has an international nexus. (The proposal, therefore, would have no impact upon American citizens or lawful permanent residents, and would not affect investigations into *domestic* terrorist groups.) The Kyl/Schumer legislation is supported by the Administration, and was favorably received by the SSCI when discussed at our July 2002 hearing. It deserves the support of the 108th Congress.

IV. *Domestic Intelligence*

The findings of our Joint Inquiry Staff have also highlighted grave and continuing problems with the Federal Bureau of Investigation in connection with its national security work. Though still renowned for its criminal investigative competence, the FBI has shown a disturbing pattern of collapse and dysfunction in its counterintelligence and counterterrorism functions. These recurring problems have, in turn, led many observers – and Members of Congress – increasingly to lose faith in the Bureau's ability to meet the national security challenges it faces, despite a series of internal reorganizations over the past several years that have failed to rectify the situation.

In light of the FBI's dismal recent history of disorganization and institutional incompetence in its national security work, many of us in Congress have begun to consider whether it might better serve the interests of the American people to separate the counterintelligence and counterterrorism functions of the Bureau into an entirely separate organization – one that would be free of the structural, organizational, and cultural constraints that have greatly handicapped the FBI's ability to conduct the domestic intelligence work our

---

[124] Marion E. ("Spike") Bowman, written statement submitted to SSCI hearing (July 31, 2002), at 1.

country depends upon it to perform.

A. *Tyranny of the Casefile*

Fundamentally, the FBI is a law enforcement organization: its agents are trained and acculturated, rewarded and promoted within an institutional culture the primary purpose of which is the prosecution of criminals. Within the Bureau, information is stored, retrieved, and simply *understood* principally through the conceptual prism of a "case" – a discrete bundle of information the fundamental purpose of which is to prove elements of crimes against specific potential defendants in a court of law.

The FBI's reification of "the case" pervades the entire organization, and is reflected at every level and in every area: in the autonomous, decentralized authority and traditions of the Field Offices; in the priorities and preference given in individual career paths, in resource allocation, and within the Bureau's status hierarchy to criminal investigative work and *post hoc* investigations as opposed to long-term analysis; in the lack of understanding of and concern with modern information management technologies and processes; and in deeply-entrenched individual mindsets that prize the production of evidence-supported narratives of defendant wrongdoing over the drawing of probabilistic inferences based upon incomplete and fragmentary information in order to support decision-making.

At its core, the FBI has always been – and remains – a "casefile" organization wedded inextricably to a "casefile" mentality. This is not a bad thing: the Bureau is often, and generally accurately, described as the "world's premier law enforcement organization." It does its traditional job quite well. But the tyranny of the case file presents a fundamental obstacle to national security work, for the simple reason that law enforcement organizations handle information, reach conclusions, and ultimately just *think* differently than intelligence organizations. Intelligence analysts would doubtless make poor policemen, and it has become very clear that policemen make poor intelligence analysts.

Particularly against shadowy transnational targets such as international terrorist organizations that lack easily-identifiable geographic loci, organizational structures, behavioral patterns, or other information "signatures," intelligence collection and analysis requires an approach to acquiring, managing, and *understanding* information quite different from that which prevails in the law enforcement community. Intelligence analysts tend to reach conclusions based upon disparate fragments of data derived from widely-distributed sources and assembled into a probabilistic "mosaic" of information. They seek to distinguish useful "signals" from a

bewildering universe of background "noise" and make determinations upon the basis of vague pattern recognition, inferences (including negative inferences), context, and history. For them, information exists to be *cross-correlated* – evaluated, and continually subjected to re-evaluation, in light of the total context of what is available to the organization as a whole. Intelligence analysts think in degrees of possibility and probability, as opposed to categories of admissibility and degrees of contribution to the ultimate criminal-investigative aim of proof "beyond a reasonable doubt."

The "analyst" mindset is thus radically different than that cultivated by training and acculturation within a law enforcement environment, which necessarily focuses upon building carefully-managed bundles of information about specific individuals or organizations for specific purposes. Far from embracing probabilistic inference, "knowledge" in a law enforcement context aspires – in its ideal form at least – not only to *certainty* but also to *admissibility*, the two essential conceptual elements of being able to prove someone guilty beyond a reasonable doubt in a court of law. Within such a paradigm, information exists to be *segregated* and ultimately employed under carefully-managed circumstances for the single specific purpose for which it was gathered.

Naturally, these are only ideal types. In reality, intelligence knowledge management is more Balkanized and disaggregated than the model suggests, and law enforcement information-holdings more interconnected. Nevertheless, the basic mindsets *do* exist, and the FBI's conceptual and institutional baggage as a law enforcement "casefile" organization has made it very hard – some might conclude impossible – for the Bureau to mature as a competent player in the national security field.

(1) *Resistance to Intelligence Analysis*

(a) *Impact of "Casefile" Mentality on pre-9/11 Analysis*

The Joint Inquiry Staff (JIS) has outlined several examples of such problems within the FBI in the period leading up to the September 11 terrorist attacks. The FBI, for instance, knew that convicted terrorist Abdul Hakim Murad had been involved in an extremist Islamic plot to blow up 12 U.S.-owned airliners over the Pacific Ocean and crash an aircraft in to CIA Headquarters. Murad was not charged with a crime in connection with the CIA crash plot, apparently because it was merely at the "discussion" stage when he was apprehended. Because the CIA crash plot did not appear in the indictment, however, the FBI effectively forgot all about it.

As the JIS has recounted, the FBI's case file for the Murad case essentially ignored the air crash plot, and FBI agents interviewed as part of our inquiry confirmed that Murad's only significance to them was in connection specifically with the crimes for which he was charged: "the other aspects of the plot were not part of the criminal case and therefore not considered relevant."[125] Convinced that the only information that really matters was information directly related to the criminal investigation at hand, the FBI thus ignored this early warning sign that terrorists had begun planning to crash aircraft into symbols of U.S. power. Thus, rather than being stored in a form that would permit this information to be assessed and re-assessed in light of a much broader universe of information about terrorist plans and intentions over time, the Murad data-point was simply forgotten. Like all the other tidbits of information that might have alerted a sophisticated analyst to terrorists' interest in using airplanes to attack building targets in the United States,[126] the episode disappeared into the depths of an old case file and slipped out of the FBI's usable institutional memory.

The handling of information about the Murad air-crash plot and the flight-school information is, unfortunately, illustrative of the FBI's more general problems in "connecting the dots" in ways that good intelligence analysts are expected to do. So pervasive was the FBI's "casefile" mentality, in fact, that it bled over into the basic architecture of how the Bureau handled terrorist information even when it *tried* to do intelligence analysis.

As the JIS has recounted, the FBI for years has tracked terrorism information in ways that essentially *prohibit* broad, cross-cutting analytical assessment. If it identified a suspected terrorist in connection with a Hamas investigation, for example, the FBI would label him as a Hamas terrorist and keep information on him in a separate "Hamas" file that would be easily accessible to and routinely used only by "Hamas"-focused FBI investigators and analysts. The Usama bin Laden unit would be unlikely to know about the FBI's interest in that individual, and no one thought to establish a system for cross-referencing terrorist connections between the carefully-segregated institutional files. [127] This approach is entirely unsuited to virtually *any* long-term strategic analytical work, and is patently inappropriate to counterterrorism analysis against the

---

125 JIS, written statement presented to SSCI/HPSCI joint hearing (September 18, 2002), at 11-12.

126 For a summary of intelligence holdings – from all intelligence agencies – related to the potential use of aircraft as weapons, *see* JIS, written statement presented to SSCI/HPSCI joint hearing (September 18, 2002), at 26-28.

127 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 14.

loose, interconnected and overlapping networks of Islamic extremists that make up the modern *jihadist* movement.

The FBI's decentralized organizational structure contributed to these problems, in that it left information-holdings fragmented into largely independent fiefdoms controlled by the various field offices. The New York Field Office for years played the principal counterterrorism role within the FBI simply because it had the misfortune of hosting the 1993 World Trade Center attacks, thereby acquiring a degree of experience with Islamic fundamentalist terror groups. Even so, this work focused upon terrorism *cases* – not strategic analysis – and the FBI's decentralized structure left other field offices in the dark. As the JIS concluded, there was even great "variation in the degree to which FBI-led Joint Terrorism Task Forces (JTTFs) prioritized and coordinated field efforts targeting Bin Ladin and al-Qa'ida," and "many other FBI offices around the country were unaware of the magnitude of the threat."[128]

The culturally and organizationally fragmented nature of FBI information-holdings apparently even extended to the handling of knowledge *within* individual FBI offices themselves. In August 2001, for example, as FBI agents first sought to establish whether Zacarias Moussaoui was a terrorist, FBI agents from the local field office visited the flight school in Norman, Oklahoma, where Moussaoui had been taking flying lessons. The FBI agents were not aware that their *own* field office had become concerned about that *same* flight school two years before – because the personal pilot of Usama bin Laden (UBL) had been training there.[129]

The earlier episode in Norman, had it been remembered, may not have been much use in obtaining criminal probable cause to search Moussaoui's personal effects, but being aware of such disparate and *potentially* connected bits of information is at the core of all-source intelligence analysis "fusion." Such fusion, apparently, was quite beyond the capabilities of the FBI. Despite all the FBI knew about terrorist interest in U.S. flight schools and in the potential use of aircraft as weapons, for example, it had declared in December 2000 in a joint report with the FAA that its "investigations" did not suggest any "evidence" of terrorist plans to target U.S. domestic civil aviation.[130]

---

[128] JIS, written statement presented to SSCI/HPSCI joint hearing (September 18, 2002), at 18.

[129] JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 19.

[130] JIS, written statement presented to SSCI/HPSCI joint hearing (September 18, 2002), at 29.

By the summer of 2001, the FBI knew from the Phoenix EC about UBL-associated individuals training at U.S. flight schools, that UBL's organization also used the Norman flight school Moussaoui attended, about past Libyan efforts to send terrorists through aviation training in the U.S., and that Murad had planned to attack the CIA with an aircraft. As a result, the FBI was the U.S. Government agency probably best positioned in the late summer of 2001 to "connect the dots" with an analytical assessment warning of terrorist interest in using U.S.-trained pilots to crash aircraft into symbolic American buildings. It was also the agency best positioned to connect such analyses with Moussaoui's activity at Norman, or the presence of known Al-Qa'ida terrorists al-Mihdhar and al-Hazmi at flight school in San Diego. Follow-up investigation of the names suggested in the Phoenix EC, which might have occurred had the FBI assembled enough of the information in its possession to understand the potential threat posed by terrorists at U.S. flight schools, might also conceivably have led the Bureau to Hani Hanjour – one of the September 11 hijackers who trained at flight school in Arizona with one of the individuals identified in the EC as having links to Al-Qa'ida.[131]

The Bureau was unable to connect these "dots," however, in large part because

> "[t]he FBI's focus at the time Moussaoui was taken into custody appears . . . to have been almost entirely on investigating specific crimes and not on identifying linkages between separate investigations or on sharing information with other U.S. Government agencies with counterterrorist responsibilities."[132]

Approaching issues of intelligence fusion with a law enforcement "casefile" mindset and organizational structure left the FBI unprepared for the national security challenges of modern terrorism.

Moreover, because the FBI is fundamentally a "casefile" organization, it has been very poor at *disseminating* any intelligence information it might happen to acquire or analytical products it might happen to produce. The Bureau disseminated extraordinarily few intelligence reports before September 11, 2001, even with respect to what is arguably its most unique and powerful domestic intelligence-collection tool: collection under the Foreign Intelligence

---

131 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 10.

132 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 19.

Surveillance Act (FISA).[133] The FBI's problems in counterterrorist intelligence before September 11 were thus threefold: the Bureau did not know what information it possessed, it did not approach this information with an intelligence analysis mindset, and it too often neglected to inform other agencies of what it *did* know or believe.

Even when the FBI did see fit to *try* to notify the rest of the Intelligence Community about the potential threat represented by the Moussaoui situation not long before the September 11 attacks, it was unable to place the Moussaoui case in the analytical context that would have made this information useful to analysts and intelligence consumers. On September 4, the FBI's Radical Fundamentalist Unit (RFU) sent out a teletype that did no more than merely recount the investigative steps the FBI was undertaking in its Moussaoui investigation. The author apparently did not find it worthy of comment that Al-Qa'ida threat warnings were at a fever pitch when Moussaoui had come to the Bureau's attention.[134] (Given the FBI's poor record of internal information-sharing, it is conceivable that the author was not even *aware* of the broader analytical context, even though he worked in the office at FBI Headquarters nominally responsible for having such awareness. At any rate, the RFU teletype certainly provided no such context.) Despite Moussaoui's specific focus upon aviation training, the RFU's teletype to the FAA on that same day also contained no analytical context that would have helped a reader understand Moussaoui's potential significance.[135]

(b) *Analysis versus Investigations*

(i) *Disinterest in Analysis*

Fundamentally, the FBI consistently prized investigations and operations in its national security work and neglected long-term analysis of the sort that might have permitted agents to understand more about the pre-September 11 threat of terrorists using civil aviation. According

---

133 At a joint SSCI/HPSCI hearing on July 18, 2002, Senator Feinstein read into the record the number of reports sent from the FBI to the CIA on terrorism issues. These figures have not been declassified, but there were essentially *no* FISA-derived "dissems" issued by the FBI in calendar year 2001. (The number of "disseminations" issued by the FBI to other members of the IC – mostly in connection with FISA surveillance or searches – *since* October 2001 is much higher.)

134 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 18.

135 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 21.

to FBI Counterterrorism Division chief Dale Watson, counterterrorism work was "a relatively low-priority program" at the Bureau for many years. He has testified that it received more emphasis beginning in late 1998, but even this new emphasis grew out of the FBI's *investigations* into the 1996 Khobar Towers bombing and the 1998 East African embassy attacks.[136] This emphasis does *not* seem to have changed the FBI's disinterest in long-term strategic analytical work in support of the Bureau's national security responsibilities.

As the Joint Inquiry Staff put it,

> "At the FBI, our review found that, prior to September 11, 2001, support for ongoing investigations and operations was favored, in terms of allocating resources, over long-term, strategic analysis. We were told, during the course of our FBI interviews, that prevention occurs in the operational units, not through strategic analysis, and that, prior to September 11, the FBI had insufficient resources to do both."[137]

These problems were, in large part, an outgrowth of the "casefile" mentality that prevailed at the Bureau. According to the JIS,

> "the case-driven, law enforcement approach, while important and extremely productive in terms of the FBI's traditional mission, does not generally 'incentivize' attention to big-picture, preventive analysis and strategy. This is particularly true when there is no direct and immediate impact on an ongoing criminal prosecution."[138]

Counterterrorism (CT) and counterintelligence (CI) work were for years considered less prestigious career fields for FBI agents. CT and CI investigations could last for years and often produced no defendants at all, and analytic work almost *never* produced easily-quantifiable career

---

136 Dale Watson, written statement presented to SSCI/HPSCI joint hearing (September 26, 2002), at 3.

137 JIS, written statement presented to SSCI/HPSCI joint hearing (September 18, 2002), at 28-29.

138 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 2-3.

trophies. Particularly after the collapse of the Soviet Empire, managers de-emphasized the FBI's CI mission, assignments to national security billets became less and less attractive within an organization focused upon criminal cases. The reluctance of agents to "homestead" in national security work – instead of working CT and CI issues merely on a rotational basis, which was much more common – helped preclude any possibility of breaking the hegemony of the "casefile" mindset within the organizaztion's national security components.

On top of a general lack of emphasis upon national security work within the organization as a whole, the FBI suffered in particular from a positive aversion to long-term strategic analysis of the sort routinely expected of intelligence agencies. CT investigations, after all, were at least *investigations* – and bore at least some resemblance to ordinary law enforcement work. Analysis, however, was apparently anathema. Even as the FBI received ever-greater amounts of CT money and personnel during the late 1990s, therefore, it showed little interest in devoting more effort to strategic intelligence or to analytical efforts aimed at Al-Qa'ida cells in the United States.

According to the JIS, the FBI's disinterest in analysis work led managers systematically to reassign good analysts from doing strategic analysis to supporting operational (*i.e.*, investigative) units. JIS investigators were "told that the FBI's al-Qa'ida-related analytic expertise had been 'gutted' by transfers to operational units and that, as a result, the FBI's [international terrorism] analytic unit had only one individual working on al-Qa'ida at the time of the September 11 attacks."[139] Indeed, the FBI seems to have regarded "intelligence analysts" as little more than a pool of disposable personnel assets to be redeployed as needed to other responsibilities – which perhaps explains the Bureau's longstanding failure to insist upon clear standards for adjudging intelligence "analyst" qualifications in the first place.[140]

---

[139] JIS, written statement presented to SSCI/HPSCI joint hearing (September 18, 2002), at 28-29; *see also id.* at 18.

[140] The SSCI became so concerned about the fuzziness of these standards that it enacted specific provisions in the Fiscal Year 2003 Intelligence Authorization Bill (Public Law 107-306) to encourage the Director of Central Intelligence to promulgate Community-wide standards for individuals performing intelligence functions. As the Senate Report put it,

> "the Committee has become concerned that, particularly in the area of analysis, elements of the Intelligence Community are denominating individuals as 'analysts' or 'intelligence analysts' without adherence to a meaningful common definition of that word."

U.S. Senate Select Committee on Intelligence, S.Rep. 107-149, *Report to Accompany S. 2506*, 107th Cong., 2d Sess. (May 13, 2002), at 12.

Discouragingly, all of the problems found by the JIS with the FBI's chronic inability to perform serious intelligence analysis occurred despite a major reorganization of the FBI announced in late 1999 *in order to improve the Bureau's ability to do analysis.* In November 1999, FBI Director Louis Freeh announced that he was creating a new "Investigative Services Division" within the FBI to "coordinate the FBI's international activities, integrate and substantially strengthen its analytic capabilities, and oversee the Bureau's crisis management functions." This reorganization was the result of Director Freeh's 1998 "Strategic Plan," which allegedly "focuse[d] on the need to improve the FBI's capacity for information analysis."[141] According to Attorney General Reno, this new organizational scheme would "help enable the Bureau to face the challenges of the next millennium."[142] The Bureau's failures leading up to September 11 thus suggest the possibility that *no* internal FBI reorganizations will prove able to effect real reform.

(ii) *Problems Illustrated by the Phoenix EC*

According to the JIS, the FBI's handling of the Phoenix EC was "symptomatic of a focus on short-term operational priorities, often at the expense of long-term, strategic analysis. . . . [W]e have found that the FBI's ability to handle strategic analytic products, such as the Phoenix EC, was, at best, limited prior to September 11, 2001." [143]

> "The manner in which the Phoenix EC was handled demonstrated how strategic analysis took a back seat to operational priorities prior to September 11. * * * Even the analytic unit responsible for strategic analysis was largely producing tactical products to satisfy the operational section. In fact there was no requirement [at the time] to handle projects with nationwide impact, such as Phoenix, any different[ly] than any other project."[144]

Due to "[i]nadequate information sharing within the FBI, particularly between the operational and

---

141 Federal Bureau of Investigation, press release (November 19, 1999), at 1-2.

142 *Id.* at 1.

143 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 2.

144 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 8.

analytic units,"[145] the recipients of the Phoenix EC lacked any knowledge of information – already within the FBI's possession, but lost or ignored in a myriad of disaggregated casefiles – that would have put the EC into a broader context of longstanding concern with terrorism threats related to Middle Eastern flight school students training in the United States.[146]

As it was, even those FBI "Intelligence Operations Specialists" (IOSs) – the name itself reveals the Bureau's preference for "operations" over "analysis" – who *did* see the Phoenix EC decided *against* sending it to the FBI's lone analytic unit concerned with terrorism.[147] Nor is it clear that it would have done much good to pass the EC to that unit, as it had been effectively crippled by personnel poaching and bureaucratic infighting.

> "[T]he capability to conduct strategic analysis on al-Qa'ida was limited because five of the unit's analysts had transferred into operational units. The Joint Inquiry Staff has been told that every time a competent new analyst arrived, the UBLU or RFU would either try to recruit them as IOS or would refuse to share information. This allowed the ULBU and RFU to control the information flow. The end result, unfortunately, is that there is no one left whose role is to perform strategic analysis."[148]

Against this deep background of analytical and organizational dysfunction and mismanagement in the national security arena, it is hard to imagine that real CT and CI analytical reform within the FBI is really possible.

(2) *The FBI's Inability to Know what it Knows*

(a) *Technological Dysfunction*

---

145 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 2.

146 For a summary of information relating to this context, *see* JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 3.

147 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 7.

148 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 8.

In addition to these cultural and organizational problems – or perhaps in large part *because* of them – the FBI has never taken information technology (IT) very seriously, and has found itself left with an entirely obsolete IT infrastructure that is wholly inadequate to the FBI's current operational needs, much less to the task of supporting sophisticated all-source intelligence fusion and analysis. Fundamentally, the FBI's IT system has changed surprisingly little since the late 1980s or early 1990s, a decade during which the rest of the computer world moved at extraordinary speed.

The handling of the Phoenix EC demonstrates some of these technological deficiencies, highlighting the "limitations in the electronic dissemination system" that kept FBI supervisors from seeing the document *even when it was addressed to them.*[149] According to the JIS, the problems with the Phoenix EC "are consistent with the complaints we have repeatedly heard throughout this inquiry about the FBI's technology problems."[150] The Bureau's electronic system for disseminating messages such as the Phoenix EC was itself "considered so unreliable that many FBI personnel, both at the field offices and at FBI headquarters, use e-mail instead."[151] Since most offices at the FBI *lack* a classified e-mail capability, this represents a fundamental obstacle to information-sharing of even the most rudimentary sort. Moreover, as users have fled the dysfunctional case-tracking system, the Bureau appears to have lost any ability to track leads entered into it. The JIS, for instance, was told that "there are 68,000 outstanding and unassigned leads assigned to the counterterrorism division dating back to 1995." At the time of our Inquiry, the FBI had no idea whether any of these leads had been assigned and dealt with outside the electronic system.[152]

This disastrous information-management system compares unfavorably with the systems developed elsewhere in the Intelligence Community for sharing data and providing analysts with the information they need to conduct intelligence "fusion." In this respect, it is useful to compare the IT capabilities of the CIA with those at FBI.

"At CIA, the DCI's CTC maintains a massive database of terrorist

---

149 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 9.

150 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 2.

151 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 9.

152 JIS, written statement presented to SSCI/HPSCI joint hearing (September 24, 2002), at 9.

> related information going back at least two decades. Within this database are analytic papers, messages between CIA headquarters and CIA stations and bases around the world, signals intelligence reports from the National Security Agency (NSA), and various briefings, memoranda, and working notes."[153]

At the most generous, the FBI is years away from having such IT capabilities, even if the Bureau's organizational structure and institutional culture permitted such tools to be used appropriately.

The FBI's TRILOGY project seeks to improve the Bureau's IT infrastructure in order to bring it up to IC standards, but this project was only begun at the very end of the tenure of Director Louis Freeh – who himself apparently did not even use a personal computer – and remains a very long way from completion. Moreover, as suggested above, even if TRILOGY *succeeds* in bringing the FBI up to "Community standards" in the IT realm, those standards are themselves inadequate to the challenges of 21st-century intelligence analysis.

(b) *A Pattern of Failures*

Unfortunately, this combination of organizational, cultural, and technological impediments has led the FBI into a recurring pattern of information dysfunction. Time after time during the past few years, the Bureau has distinguished itself by its inability to assess what is in its own files – much less to make productive analytical use of such information. This occurred, for instance, in 1997 when the FBI misplaced vital information in its own files linking the People's Republic of China to illicit political influence operations during the 1996 U.S. Presidential campaign.[154] It happened with the belated discovery of thousands of pages of documents related to convicted Oklahoma City bomber Timothy McVeigh – just days before his execution.[155] It happened on several occasions during the FBI's botched handling of the Wen-Ho Lee nuclear espionage

---

153 JIS, written statement presented to SSCI/HPSCI joint hearing (September 20, 2002), at 3.

154 *See* U.S. Department of Justice, Office of the Inspector General, *The Handling of FBI Intellience Information Related to the Justice Department's Campaign Finance Investigation* (July 1999) [unclassified Executive Summary], *available at* http://www.usdoj.gov:80/oig/fbicfi/fbicfi.1htm.

155 *See, e.g.*, David Johnson, "Citing FBI Lapse, Ashcroft Delays McVeigh Execution," *New York Times* (May 12, 2001), at A1.

investigation, when agents in the Albuquerque field office or at FBI Headquarters misplaced or failed to pass along crucial information that might have permitted agents to discover Lee's unlawful removal of nuclear secrets from the Los Alamos National Laboratory months or years before they finally did.[156]

As detailed by the JIS in the present inquiry, the same thing happened with the Phoenix EC and the many tidbits of information in the FBI's possession relating to terrorists' interest in U.S. flight schools. It also happened in the FBI's belated revelation to the Joint Inquiry in the late summer of 2002 of certain information relating to the activities of September 11 hijackers Khalid al-Mihdhar and Nawaf al-Hazmi.

Being able to know what one knows is the fundamental prerequisite for any organization that seeks to undertake even the most rudimentary intelligence analysis. The FBI, however, has repeatedly shown that it is unable to do this. It does not know what it knows, it has enormous difficulty analyzing information when it *can* find it, and it refuses to disseminate whatever analytical products its analysts might, nonetheless, happen to produce. The Bureau's repeated failures in this regard – despite successive efforts to reorganize its national security components – have led many observers to conclude that "mixing law enforcement with counterintelligence" simply cannot work. As one former director of the National Security Agency has suggested, "cops" cannot do the work of "spies."[157] This insight, in turn, has led to widespread public debate over the need for radical structural reform – including removing the CI and CT functions from the FBI entirely.

B. *The Need to Consider Radical Reform*

For all of these reasons, I believe that a very strong argument can be made for removing the CI and CT portfolios from the FBI. Despite repeated reorganizations, the FBI has simply performed too poorly for the American people to have much faith in its ability to meet current and future challenges no matter *how* many aggressive "reform" plans are announced by FBI management. Even a year after September 11, in fact, the FBI's deputy director sent angry e-mail messages to Bureau field offices declaring that he was "amazed and astounded" that the Special Agents in Charge (SACs) *still* refused to commit essential resources to the fight against terrorism

---

156 *See* Thompson & Lieberman, *supra*,at 3-4 & 11.

157 Gen. William Odom, USA (ret.), written statement presented to JIS hearing (October 3, 2002), at 4.

and *still* refused to share information properly with Headquarters. "You need to instil a sense of urgency," he told them, insisting that the SACs send their agents "out on the street and develop sources" and "demand that information is being sent" to headquarters.[158] If September 11 cannot persuade the existing FBI to focus properly upon terrorism, perhaps nothing can.

Some observers have thus suggested placing the Bureau's CI and CT functions within their own separate agency, a stand-alone member of the Intelligence Community that would be responsible for domestic intelligence collection and analysis but would have no law enforcement powers or responsibilities. This would be, in effect, an American analogue to the British Security Service (a.k.a. MI-5) or the Australian Security Intelligence Organization (ASIO).

There is much to recommend such an approach. The FBI today performs the domestic intelligence role within the U.S. Intelligence Community. Its problem, however, is that it performs this task poorly – and arguably *cannot* be made to perform it well given the cultural and organizational chasm that exists between a "casefile" organization and a true intelligence organization. An MI-5 analogue would allow our domestic intelligence collection and analytical functions to be performed by a "pure-knowledge" organization freed from the tyranny of the casefile and thus able properly to perform these functions.

Paradoxically, such a freestanding "domestic spy agency" might offer advantages over our current structure even in terms of civil liberties. Today, domestic intelligence collection is performed by FBI special agents who, in addition to their "pure-knowledge" functions, also have law enforcement powers: they have badges, can carry firearms, and can arrest and detain Americans. I suspect that most Americans, however, would feel safer having such collection performed by intelligence officers who do *not* possess coercive powers – and who can only actually take *action* against someone through a process of formal coordination with law enforcement officials (*e.g.*, an office remaining within the FBI that would function as an analogue to the Special Branch, which performs law enforcement liaison functions with the British Security Service).

Should the creation of a wholly freestanding agency turn out to be, in bureaucratic terms, "a bridge too far," an alternative approach might be to separate the CI and CT functions of the FBI into a semi-autonomous organization. This approach envisions an organization that would

---

[158] Eric Lichtblau, "FBI Officials Say Some Agents Lack a Focus on Terror," *New York Times* (November 21, 2002), at 1 (quoting Deputy Director Bruce J. Gebhardt).

still report to the FBI director for purposes of overall coordination and accountability, but which would in all other respects (*e.g.*, training and promotion pipelines, IT systems, management structures, and chains of command) be entirely separate from the "criminal" components of the FBI. (This approach might be called the "NNSA option," after Congress' effort in 1999 to create a semi-freestanding National Nuclear Security Administration within the Energy Department – though any effort to do this with the FBI would have to avoid the rampant "dual-hatting" that has eroded the effectiveness of our NNSA reforms.)

A third approach might be to move the FBI's CI and CT functions to the new Department of Homeland Security, thereby adding a domestic *collection* element to that organization's soon-to-be-created Undersecretariat for Information Analysis and Infrastructure Protection. This might allow the collection components to take advantage of working within a "national security" culture rather than a "law enforcement" culture, and would give them a broader base of institutional support than they might enjoy as a freestanding "MI-5" within the Intelligence Community. Many Americans, however, might be uncomfortable with combining these functions with the already sweeping security responsibilities of the new Department.

Whatever the best answer turns out to be, I believe some kind of radical reform of the FBI is in order – indeed, is long overdue – and should be a major item on the "intelligence reform" agenda for the 108th Congress. The FBI has, unfortunately, shown that in its present form, it is not capable of successfully performing domestic intelligence collection and analysis against modern CI and CT challenges. The Bush Administration and the 108th Congress should make it a high priority to resolve these issues, and to put the domestic components of our Intelligence Community on a footing that will enable them to meet the challenges of the 21st century.

V. *Human Intelligence*

In an unclassified report such as this one, it is hard to provide much supporting information for a critique of human intelligence (HUMINT) operations against terrorist groups prior to September 11. Suffice it to say, however, that the *status quo* of Intelligence Community approaches in this regard was tested against the Al-Qa'ida threat and found wanting.

CIA officials have publicly boasted that they had operatives in Afghanistan before

September 11,[159] but careful observers should not confuse the periodic infiltration of operatives for brief *liaison* meetings with friendly warlords for a real HUMINT or paramilitary *presence*. Such unfounded braggadocio aside, the distinguishing feature of anti-terrorist HUMINT three years after the embassy bombings and the DCI's "declaration of war" against Al-Qa'ida was our *lack* of HUMINT penetration of the organization, especially of its central operations.

It is well known in the intelligence world that "[c]landestine handling of agents or other covert activity is usually assigned to intelligence officers under diplomatic cover"[160] – that is, to officials operating out of embassies who, while they face greater risks than the average diplomat, are in the final analysis protected from arrest by diplomatic immunity. The CIA's HUMINT collection service, the Directorate of Operations (DO), admits to occasionally using non-official cover (NOC) officers,[161] but such assignments are the rare exception rather than the rule, and NOCs too often suffer career damage because their nonconventional assignments necessarily remove them from the usual network of DO contacts and advancement opportunities.

This balance between diplomatic cover officers and NOCs may have served the CIA tolerably well during the Cold War – though HUMINT was never regarded as our strong suit against the Soviets – but it is patently *unsuited* to HUMINT collection against nontraditional threats such as terrorism or proliferation targets. As former DCI James Woolsey has observed, "[o]ne needs to use non-official cover officers to recruit spies inside terrorist organizations," because "not too many [Al-Qa'ida] supporters and friends attend embassy cocktail parties."[162]

---

159 *See, e.g.*, Drogin, *supra* (quoting CIA Deputy Director for Operations Jim Pavitt that "we were there before the 11th of September").

160 FBI Section Chief Timothy D. Bereznay, statement for the record submitted to the House International Relations Committee (May 11, 2000), at 2.

161 Both DCI Tenet, during his confirmation hearing, and his predecessor John Deutch have discussed CIA policy with respect to the employment of NOCs posing as members of certain professions. As Deutch explained it, the CIA has a policy of generally avoiding "having a U.S. intelligence asset use U.S. journalistic cover." John Deutch, testimony before SSCI hearing (February 22, 1996), *available from* Federal News Service transcripts (February 22, 1996); *see also* George Tenet, testimony before SSCI hearing (May 6, 1997), *available from* Federal News Service transcripts (May 6, 1997).

162 James Woolsey, testimony before Senate Judiciary Committee Subcommittee (September 3, 1998), *available from* Federal News Service transcripts (September 3, 1998).

Especially against Al-Qa'ida – which is known actively to *seek out* Islamic converts such as José Padilla, John Walker Lindh, and Richard Reid, who have "legitimate" papers and can travel and live in the West without raising much suspicion – it is hard to understand why the CIA was not more interested in, and successful at, NOC-based HUMINT operations against Al-Qa'ida before September 11.

The CIA has relied too much, in my view, upon traditional embassy-based HUMINT, and not enough upon NOCs. It has also focused too heavily upon HUMINT operations conducted in collaboration with foreign intelligence services. There is nothing intrinsically wrong with liaison service work, and such collaboration has produced some of the greatest HUMINT successes we have had in the war against terrorism. Liaison operations are also by far the *easiest* sort of HUMINT for CIA officers to conduct against terrorist groups when those officers are operating under diplomatic cover. (Visiting one's liaison counterpart at his office is rather less hazardous than actually developing sources in the *souk*, and "State Department" employees are unlikely to be invited to many radical Islamist meetings anyway.) Liaison work, however, is inherently conducted only on the basis of, and limited by the extent of, the cooperative service's *own* interests – rather than those of the CIA or the United States. They are also of necessarily limited utility in countries in which the host government is, to some extent at least, part of the problem. In the final equation, there is no substitute for mounting our *own* extra-embassy, non-official cover HUMINT operations.

It is far past time for the CIA to recognize the sharp limitations of its traditional Cold War approach to HUMINT, and to begin serious development – in a large-scale, programmatic way, rather than simply on an *ad hoc* or "volunteer" basis – of nontraditional HUMINT "platforms" and the use of NOCs. A greater emphasis upon non-Caucasian NOC officers would also probably pay dividends out of proportion to the investments necessary to recruit and train such individuals. Indeed, it is perhaps in getting undercover agents out (and at risk) amongst the "target" population that the HUMINT operators of the DO perhaps have the most to learn from their law enforcement counterparts. If the Drug Enforcement Administration can put actual, salaried *American* officers undercover in clannish narcotrafficking organizations in foreign countries, surely the CIA can learn to penetrate aggressively proselytizing Islamic fundamentalist organizations. We depend upon them to do just that.

As a final note, it is worth pointing out that I do not believe the language in the Joint Inquiry's "Recommendations" concerning the importance of enhancing "the recruitment of a more ethnically and culturally diverse workforce with the intelligence skills and expertise needed for success in counterterrorism efforts" is meant to represent our collective endorsement of

workplace diversity *for its own sake.* Rather, the Committees believe that the challenges of both understanding and penetrating international terrorist organizations and the milieu in which they move require that the Intelligence Community seek to develop larger numbers of native-speaking translators, culturally-attuned analysts, and HUMINT operators – especially NOC officers – ethnically and culturally indistinguishable from their collection targets. In legal terms, certain specific target-related types of ethnic and cultural diversity should be sought as a bona fide occupational qualification. Without a fundamental shift in the CIA's operational paradigm, diversity for diversity's sake alone will do little to improve the CIA's ability to execute its mission.

VI. *Covert Action*

A. *Clarity and Support*

As with HUMINT operations, there is obviously little one can say here about the lessons that should be learned from the CIA's clearly mixed record of success in offensive operations against Al-Qa'ida before September 11, 2001.[163] One important lesson, however, was suggested by former National Security Advisor Sandy Berger in his testimony before our Joint Inquiry. In giving covert action instructions to the CIA, he said it is incumbent upon the President to convey legal authorities – the limits spelled out in a covert action "finding" or Memorandum of Notification (MON) as to what agents are permitted to do in pursuit of the stated aim – with absolute clarity.[164] Unfortunately, as the committees have heard repeatedly from knowledgeable participants, Berger's injunction was honored more in the breach than in the observance by the very Administration he served.

---

[163] DCI Tenet confirmed the existence of CIA offensive operations against Al-Qa'ida in public testimony before the Joint Inquiry. *See* George Tenet, testimony before joint SSCI/HPSCI hearing (October 17, 2002), *available from* FDCH Political Transcripts (October 17, 2002) (declining to discuss specific legal authorities received by CIA to conduct operations before September 11, 2001 but describing "offensive operations" and a "plan of attack" both "inside Afghanistan and globally" to "render" Al-Qa'ida terrorists [capture and deliver them to appropriate authorities], "disrupt" Usama bin Laden's terrorist infrastructure and finances, and otherwise "degrade his ability to engage in terrorism").

[164] Sandy Berger, testimony before joint SSCI/HPSCI hearing (September 18, 2002), *available from* FDCH Political Transcripts (September 19, 2002) (remarking with respect to covert action authorities that "We certainly would have to have clarity from the President of the United States ....").

Particularly given the unpleasant history of covert action scandals that have affected the CIA, one should not be surprised to find that – ironically, perhaps – the covert action infrastructure is a relatively cautious one. Intelligence officers will often, and with good reason, hesitate to take operational risks or to push aggressively to accomplish their missions if they are operating under ambiguous or convoluted legal authorities and always suspect that they may be prosecuted or hauled before a hostile inquiry for any actual or perceived missteps. This admonition clearly applies to both Executive Branch and Congressional leaders: whatever the merits or demerits of the policies they are asked by the President to execute, our intelligence operators risking their lives in the field need to know that their own government will make clear to them what their job is and protect them when they do it. Neither assurance, unfortunately, could be had by the DO's covert action staffs working against terrorism in the late 1990s.

As far as the anti-terrorism efforts of the Intelligence Community *since* September 11 are concerned, I believe it is important that the record reflect that we on the oversight committees of Congress *have* been kept apprised of the new approaches and initiatives adopted by the President as part of our country's war on terrorism. As any perusal of our closed hearing records at the SSCI will show, we have been uniformly supportive. These are challenging times, and they have in some respects demanded unprecedented responses. In the past, Congress has sometimes contributed to cultural and legal problems of risk-aversion within the Intelligence Community by conducting high-profile investigations into intelligence activities. Congress can and must continue to assert its prerogatives in undertaking careful oversight of IC activities and conducting investigations wherever necessary. Historians of the United States' war on terrorism, however – and, above all, our intelligence operatives currently in the field – should be aware that our committee Members have forcefully *supported* the IC's current counterterrorist campaign. Far too much is already publicly known about this campaign, but if and when the full story is actually told, it must be made clear that what has occurred has been undertaken with the knowledge and support of the oversight organs of our national legislature.

B. *Oversight Challenges*

Perhaps in part because of frustrations with the existing covert action system, it has been widely reported that the Defense Department is interested in augmenting a quasi-covert action capability of its own, based upon its highly competent cadre of special operations forces (SOF).[165] If this parallel system works, I wish it well: the covert action side of the war on terrorism could

---

[165] *See, e.g.*, Schmidt & Ricks, *supra*.

certainly use the manpower and expertise. It is worth emphasizing, however, that a greater DOD involvement in the world of covert action could present oversight challenges for Congress.

The oversight mechanism and reporting requirements for covert action contained in 50 U.S.C. §§ 413b, of course, operate in a *functional* basis rather than an agency-specific one. The law does not require that only the CIA conduct covert action: rather, the President can designate any government entity for this purpose if he sees fit. DOD forces conducting covert action-type operations against Al-Qa'ida, however, may be harder for Congress to oversee if the Defense Department decides to treat attacks on Al-Qa'ida and affiliated terrorist networks as part of its "wartime" *operational* responsibilities rather than as part of covert action policy.

Like the rules in Executive Order 12,333 regarding "assassination," some might argue that "covert action" is a conceptual category more appropriate to times of "peace" in which special restrictions and oversight rules are crafted to oversee the government's employment of certain somewhat sinister policy tools. By this argument, operational conduct in attacking "enemy" forces in time of "war" is something else entirely – and is not something into which Congress has traditionally enjoyed any meaningful visibility, let alone had "oversight" responsibilities. In truth, such questions are legal matters of first impression, because the federal laws governing covert action were not yet in place the last time we faced a bitter war of indefinite duration against a global enemy. How exactly the line is drawn between "covert action" oversight and "operational" opacity, therefore, remains to be determined. The 108th Congress should watch these issues carefully, for the oversight committees are the only real "check" our constitutional scheme provides in these areas. We should take care that any alleged covert action "exception" does not swallow its rule.

VII. *Accountability*

The story of September 11 is one replete with failures: to share information, to coordinate with other agencies; to understand the law, follow existing rules and procedures, and use available legal authorities in order to accomplish vital goals; to devote or redirect sufficient resources and personnel to counterterrorism work; to communicate priorities clearly and effectively to IC components; to take seriously the crucial work of strategic counterterrorism analysis; and most importantly, to rise above parochial bureaucratic interests in the name of protecting the American people from terrorist attack.

One of the mandates of this inquiry has been to "lay a basis for assessing the accountability

of institutions and officials of government"[166] by identifying any problems and failings within the Intelligence Community that helped leave us unprepared for the terrorist attacks. The Joint Inquiry's recommendations call for the agency Inspectors General to

> "review the factual findings and the record of this Inquiry and conduct investigations and reviews as necessary to determine whether and to what extent Intelligence Community personnel at all levels should be held accountable for any omission, commission, or failure to meet professional standards in regard to the identification, prevention, or disruption of terrorist attacks, including the events of September 11, 2001."

The DCI has declared us to be at "war" against Al-Qa'ida since 1998, and as the President has declared, we have really been so since at least September 11. Some have suggested that this means that we should postpone holding anyone accountable within the Intelligence Community until this war is over and the threat recedes. I respectfully disagree.

The threat we face today is, unfortunately, in no danger of subsiding any time soon, and the problems our Intelligence Community faces are not ones wisely left unaddressed any longer. Indeed, it is precisely *because* we face a grave and ongoing threat that we must begin reforming the Community immediately. Otherwise we will simply be unable to meet this threat. The metaphor of "war" is instructive in this regard, inasmuch as wise generals should not – and historically do not – hesitate to hold their subordinates accountable while the battle still rages, disciplining or cashiering those who fail to do their duty. So also do wise Presidents dispose of their faltering generals under fire. As the fabric of military law makes clear, failures in wartime are traditionally considered less excusable, and are punished more severely, than failures in times of peace. If we are indeed at war, accountability is more important now than ever, for it is through insisting upon accountability that life-threatening problems may best be fixed.

Nor should we forget that accountability has two sides. It is also a core responsibility of all good leaders to reward those who perform well, and promote them to positions of ever greater responsibility. In urging the Intelligence Community to hold its employees accountable, the IC must therefore both discipline those who fall down on the job and reward those who have excelled. For officials charged with protecting our national security and keeping Americans safe

---

[166] SSCI & HPSCI, "Initial Scope of Joint Inquiry" (June 5, 2002), from the preamble.

from attack, professional advancement should proceed by Darwinian selection.

For these reasons, it is disappointing to me that despite the Joint Inquiry's explicit mandate to "lay a basis for assessing the accountability of institutions and officials of government" and despite its extensive findings documenting recurring and widespread Community shortcomings in the months and years leading up to September 11, the Joint Inquiry has not seen fit to identify *any* of the persons whose decisions left us so unprepared. Careful readers of the Joint Inquiry's findings will be left with little doubt as to the identities of at least some of the officials responsible. It is unfortunate, however, that the Joint Inquiry has shied away from its oversight responsibilities in refusing to provide more of the accountability to which we ask the IC to subject itself. I thus urge President Bush carefully to examine the Joint Inquiry's findings in order to determine the extent to which he has been well served by his "generals" in the Intelligence Community.

Some have argued that we should avoid this issue of accountability lest we encourage the development of a worse climate of intra-Community risk-aversion and legal timorousness than the Committees have already seen during the 1990s. I do not believe this is the case. To begin with, the failings leading up to September 11 were not ones of impetuousness, the punishment for which might indeed discourage the risk-taking inherent in and necessary to good intelligence work. The failures of September 11 were generally ones not of reckless *commission* but rather of nervous *omission*. They were failures to take the necessary steps to rise above petty parochial interests and concerns in the service of the common good. These are not failings that will be exacerbated by accountability. Quite the contrary. And, more importantly, it is clear that without real accountability, these many problems will simply remain unaddressed – leaving us terribly and needlessly vulnerable in the future.

By no means do I advocate a crusade to hold low-level employees accountable for the failures of September 11. There clearly were some individual failings, but for the most part our hard-working and dedicated intelligence professionals did very well, given the limited tools and resources they received and the constricting institutional culture and policy guidance they faced. The IC's rank-and-file deserve no discredit for resource decisions and for creating these policies.

Ultimately, as the findings of the Joint Inquiry make clear – though they carefully stop short of saying so explicitly – accountability must begin with those whose job it was to steer the IC and its constituent agencies through these shoals, and to ensure that all of them cooperated to the best of their abilities in protecting our national security. Responsibility must lie with the leaders who took so little action for so long, to address problems so well known. In this context,

we must not be afraid publicly to name names, and I do so here. The U.S. Intelligence Community would have been far better prepared for September 11 but for the failure of successive agency leaders to work wholeheartedly to overcome the institutional and cultural obstacles to inter-agency cooperation and coordination that bedeviled counterterrorism efforts before the attacks: DCIs George Tenet and John Deutch, FBI Director Louis Freeh, and NSA Directors Michael Hayden and Kenneth Minnihan, and former NSA Deputy Director Barbara McNamara. These individuals are not responsible for the disaster of September 11, of course, for that infamy belongs to Al-Qa'ida's 19 suicide hijackers and the terrorist infrastructure that supported them. As the leaders of the United States Intelligence Community, however, these officials failed in significant ways to ensure that this country was as prepared as it could have been.