Research Paper

US Intelligence Support to Decision Making

by

STEVEN W. PETERSON
FELLOW, WEATHERHEAD CENTER FOR INTERNATIONAL AFFAIRS

WEATHERHEAD CENTER FOR INTERNATIONAL AFFAIRS
HARVARD UNIVERSITY
CAMBRIDGE, MA

ABSTRACT

AUTHOR: Steven W. Peterson

TITLE: US Intelligence Support to Decision Making

FORMAT: Research Paper

DATE: 1 July 2009

Pages: 35

The thesis of this paper is that the intelligence reforms undertaken following the intelligence failures of 9/11 and Iraqi WMD, although useful, will not solve significant problems inherent to the US intelligence system.   The paper argues that the requirements driven intelligence process the United States follows hinders the development of new insights critical to decision making under uncertainty in a changing global environment.

TABLE OF CONTENTS

US Intelligence Support to Decision Making

The United States spends approximately $60 billion a year on intelligence.[1] To put that in perspective, consider the fact that only four of the world's nations (the US, China, France, and UK) spend more than that on their *entire* defense budgets.[2] In a time of fiscal crisis and exploding deficits, it is fair for Americans to ask whether or not they are getting their money's worth from the US intelligence system. Can they expect more failures like 9/11 and Iraqi WMD or will recent reforms lead to better results in the future? Will our intelligence system give our leaders what they need in dealing with challenges like North Korean or Iranian nuclear and missile developments, terrorist threats against the United States, or cyber warfare against our public and private infrastructure?

The goal of this paper is three fold – introduce the reader to the US intelligence system, take a look at reforms stemming from two recent intelligence failures (9/11 and Iraqi WMD), and make recommendations for better intelligence support in the future.

In Part I, I will provide an overview of the US intelligence system – what it is comprised of and how it functions in support of national decision making. In Part II, I will introduce the commonly accepted conclusions about intelligence drawn from analysis of the intelligence failures of 9/11 and Iraqi WMD and the reforms resulting from them. In Part III, I'll address what is wrong with our intelligence support to decision making and discuss why these reforms, though necessary and helpful in improving our intelligence system, are not sufficient to correct the most fundamental problems. I will argue that our requirements-driven system focuses on feeding decision makers' interests stemming from old insights while neglecting its critical role in shaping our leaders' interests toward new insights. Finally, in Part IV I will make

recommendations for improving intelligence support by changing our understanding of the proper roles of intelligence. Rather than continuing to seek certainty in a world of inevitable uncertainty, we must recognize that our intelligence system cannot provide the unambiguous clarity that our decision makers seek. Instead, we must equip them to make better decisions under uncertainty and help them avoid the pitfall of delaying decision while seeking certainty that intelligence cannot provide.

Part I: The US Intelligence System

No nation in the history of man has ever assembled a more capable intelligence system than that of the United States today. The global US intelligence community consists of elements of 16 offices and agencies as follows:[3]

Office of the Director of National Intelligence
- Central Intelligence Agency (CIA)
- Federal Bureau of Investigation (FBI) National Security Branch
- Drug Enforcement Agency (DEA) Office of National Security Intelligence
- Department of Treasury Office of Intelligence and Analysis
- Department of State Bureau of Intelligence and Research
- Department of Energy Office of Intelligence and Counterintelligence
- Department of Homeland Security Office of Intelligence and Analysis
- Coast Guard Intelligence

Department of Defense (Under Secretary of Defense for Intelligence)
- Air Force Intelligence
- Army Intelligence
- Navy Intelligence
- Marine Corps Intelligence
- Defense Intelligence Agency (DIA)
- National Geospatial Intelligence Agency (NGA)
- National Reconnaissance Office (NRO)
- National Security Agency (NSA)

Looking at this list, one can quickly understand the difficulty of managing such a diverse collection of entities. It is easy to see that each would naturally have a different focus driven by

the differing missions and interests of their parent organizations. Each has different policies, different personnel systems, different networks and technologies, different legal restrictions and authorities, and different requirements and cultures driving their intelligence collection and analysis activities.   In fact, prior to 9/11 each organization operated substantially independent of the others with only minor community oversight and coordination. The Director of Central Intelligence was the principal intelligence advisor to the President and the nominal head of the US intelligence community but in reality exercised little effective management control over these diverse entities.

After 9/11, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA) aimed at overcoming the stove-piped independence of the members of the intelligence community. IRTPA created the Director of National Intelligence (DNI). The intent was to overcome agency parochialism and improve coordination, information sharing, and coherency of US intelligence efforts by putting them under a single authority. IRTPA gives the DNI budgetary authority over all of the intelligence community's disparate agencies and the responsibility to manage them as a coherent, mutually reinforcing enterprise in support of national decision making.   Because bureaucracies yield turf with great reluctance, the degree to which the DNI has accomplished this remains a subject of much debate well beyond the scope of this paper. For our purposes here, it is sufficient to understand that the DNI is now the statutory head of the intelligence community and the principal advisor to the President with responsibility for oversight and execution of the nation's intelligence activities.

Note that all but two of the intelligence community members (Office of the DNI and the CIA) belong to Cabinet Departments and as a result serve at least two masters – their parent cabinet head and the DNI. In fact, most US intelligence capabilities reside in the Department of

Defense and report to the Under Secretary of Defense for Intelligence (USDI). Obviously, the

relationship between the DNI and the USDI is critical to the effective functioning of the

intelligence system. In recognition of that, the DNI must work closely with the USDI to ensure

effective integration of DoD intelligence components in the national intelligence effort. The

DNI is also working in other areas to bring coherence to the intelligence system; for example, by

formulating standards for information sharing, by exercising more effective budget oversight, by

beginning initiatives to rotate intelligence officials between agencies as part of their professional

development, by seeking to standardize community processes for identifying requirements and

producing coordinated National Intelligence Estimates to name a few.

The Intelligence Cycle

To understand the way the diverse entities of the intelligence community function in

support of decision making, it is first important to understand the broad outlines of the

intelligence process – how intelligence is gathered, evaluated and presented.   This is done

through the intelligence cycle consisting of five steps: 1) planning and direction, 2) collection,

3) processing, 4) analysis and production, and 5) dissemination.[4] Each step feeds the following

step as intelligence community members work to transform raw information into finished

intelligence useful in meeting decision maker needs throughout the government.

Intelligence Cycle -- Step 1: Planning and Direction.

It is important to understand that the US intelligence community is *requirements driven*.

Intelligence consumers (e.g. the President, executive branch decision makers, cabinet secretaries,

armed services leadership, etc) define what intelligence is needed to support their decision

making and those requirements then drive the intelligence process. In other words, decision

makers identify what they believe to be important and then the intelligence community sets out to find it. This makes sense in that even in an intelligence system as large as that of the US, resources are constrained and must be focused on those issues of greatest importance in the eyes of our leadership.

The DNI communicates intelligence priorities to the intelligence community through the use of a system known as the National Intelligence Priorities Framework (NIPF). The NIPF is:

"the DNI's sole mechanism for establishing national intelligence priorities. [It consists of]:

- Intelligence topics reviewed be the National Security Council Principals Committee and approved by the President.
- A process for assigning priorities to countries and non-state actors relevant to the approved intelligence topics.
- A matrix showing these priorities. The NIPF matrix reflects consumer's priorities for intelligence support and ensures that long-term intelligence issues are addressed."[5]

The NIPF is used to allocate collection and analytic resources and is updated twice a year based on inputs from the National Intelligence Council[6], IC elements, and the ODNI. IC members use the NIPF to report to the DNI on their coverage of national priorities and intelligence consumers provide feedback on the effectiveness of intelligence reporting with reference to requirements articulated in the NIPF. Thus, the NIPF is critical to the planning and direction of intelligence activities and the DNI's management oversight of the intelligence community. It is the first order document in setting priorities for the next step in the intelligence cycle – collection.

Intelligence Cycle -- Step 2: Collection

Working from defined requirements, the intelligence community sets out to gather raw information for analysis. This may include open source information (readily available to the

public) or sensitive sources including agents or technical means (e.g. communications intercepts, satellite imagery, clandestine operations, etc). This is the step in which specific data is identified for collection and the means of obtaining it are deployed to do so. Once data is collected, it enters the next phase of the intelligence cycle – processing.

Intelligence Cycle -- Step 3: Processing

Processing is the conversion of raw data into useful forms for analysis. Examples of processing include the translation of foreign language communications, the expert interpretation of imagery, the decoding of encrypted signals, or the scientific testing of collected samples or materials. Processed information is then passed on for expert evaluation in the next step of the intelligence cycle – analysis and production.

Intelligence Cycle -- Step 4: Analysis and Production

During this step, expert analysts evaluate information for importance and context. They draw not only from current reporting, but also from extensive historical knowledge bases to determine the reliability and significance of newly collected information. They work to piece together fragmentary information to produce analyses that resolve information conflicts, answer questions, and make predictions to fill gaps in what is known about subjects of interest to our decision makers. This is an imperfect art, dependent upon human experience, judgment, imagination, and ability to sift through thousands of data points and determine what is reliable and important in constructing an accurate picture predicting an adversary's actions or intent. The analytical process often raises more questions and feeds new requirements for collection back into the intelligence cycle beginning the process again. The reports, studies, and estimates

produced during this phase are then provided to decision makers in the final step of the

intelligence cycle – dissemination.

Intelligence Cycle -- Step 5: Dissemination

Dissemination is the process of providing intelligence to decision makers. Analytical

products may be tailored to very specific requirements and provided to the specific consumer

who requested them. They are often also more broadly disseminated to decision makers and

staff throughout the intelligence and analytic community where they inform further iterations of

the intelligence cycle.

How Intelligence Works in Support of Decision Makers

So in a nutshell, here is how the intelligence system in the US works. First, decision

makers identify intelligence requirements – things that they want to know more about. The

National Intelligence Priorities Framework (NIPF) is used as a catalyst for capturing these

requirements from across the government and setting priorities upon which to allocate

intelligence resources. Guided by the NIPF and following the intelligence cycle, members of the

intelligence community plan and direct collection operations. Data is then processed and

analyzed to produce intelligence reports, studies and other products disseminated to inform

decision making. In the course of this cycle, further collection requirements are identified and

the process begins again.   Requirements are continuously reviewed and changing international

circumstances may result in ad hoc adjustments.

Throughout the process, national capabilities are also evaluated to identify the need to

develop new collection systems or analytical resources. This in turn generates program and

funding requirements introduced to the budgeting process. The intelligence community leadership evaluates these needs and adjusts budget requests and resourcing accordingly. Overall, the system is adaptable and strives to be responsive to national policy makers needs.

The conduct of US intelligence activities is continually subject to scrutiny – not only for evaluations of effectiveness, but also for compliance with law and policy. Therefore, to understand the US intelligence system, it is also important to consider the oversight mechanisms which apply to it.

Oversight of the US Intelligence System

Because of past abuses and the fact that the intelligence system functions behind a wall of secrecy, US intelligence activities are subject to many layers of oversight to ensure compliance with law and policy and to protect the rights of US citizens.[7] Within each organization there are internal controls, reporting procedures, and inspector general oversight as a first line of defense. Beyond those controls, the DNI exercises oversight over the entire community and Cabinet heads are responsible for ensuring their agencies comply with the law. Additionally, the National Security Council and the Homeland Security Council review US intelligence initiatives and formulate Presidential directives that guide IC activities. The President's Intelligence Advisory Board (PIAB) and its subcommittee the Intelligence Oversight Board (IOB) exercise an additional level of oversight. The PIAB provides independent advice and evaluation of the effectiveness of the intelligence effort and the IOB is charged with identifying any intelligence activity it believes unlawful or in violation of executive orders or presidential directives.

Outside the executive branch, the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) provide direct legislative oversight of US intelligence activities. Senate confirmation of key intelligence appointments

11

provides a further level of legislative accountability as do the appropriations and authorization committees of both chambers in reviewing and approving the budgets of US intelligence programs. Finally, the attorney general and the courts play a role in the authorization and execution of certain intelligence activities (e.g. surveillance authorizations) and offer recourse through civil and criminal action in the event of violations of the law. Legal reviews are an extensive part of the planning and execution of all US intelligence activities and provide yet another measure of accountability in the intelligence cycle.

One need only look to recent events to see evidence of the effectiveness of the many layers of the oversight system. Questions raised by a whistle blower concerning the National Security Agency's (NSA) surveillance of domestic communications following 9/11 became the subject of political debate, legislative action, court review, and the revision of intelligence collection procedures. This is clear evidence of an oversight system that is fully engaged in protecting the rights of the American populace while balancing the nation's intelligence interests to safeguard our security.

So, in summary, the US intelligence system is well-funded, vast, diverse, rationally driven by decision maker requirements, and overseen by multiple levels of legal review and oversight. It is in continuous operation worldwide and seeks to adapt its operations to changing national priorities. Yet, it was not effective in characterizing the threat before 9/11 and was wrong about Iraqi WMD. So, we will now take a closer look at these intelligence failures.

Part II: Lessons Learned from the 9/11 and Iraqi WMD intelligence Failures

In Part I, we provided a broad overview of the structure and functioning of the US intelligence system as it exists today. As we turn our attention to lessons learned from the

intelligence failures of 9/11 and Iraqi WMD, it is important to remember that those failures

occurred under a slightly different system. There was no DNI and the Director of Central

Intelligence ((DCI) did not have budgetary authority or other effective means to exercise

coherent control of the nation's diverse intelligence activities. Although the DCI had nominal

community management responsibilities, cross community coordination, information sharing,

and collaboration were found to be largely ineffective.

In order to learn what went wrong in each of these cases, the nation undertook extensive

investigations and produced multiple reports and studies.[8] For the purposes of this paper, we

will draw principally from two of those efforts – *The 9/11 Commission Report* (9/11 Report) and

the *Comprehensive Report of the Special Advisor to the DCI on Iraqi WMD* (commonly referred

to as the Duelfer Report). We will begin with the intelligence failures of 9/11.

Intelligence Failure in the 9/11 Attacks

On September 11th, 2001 Islamic terrorists under the direction of Al Qaeda's Osama Bin

Laden hijacked four commercial aircraft and used them to hit both towers of the World Trade

Center in New York, to attack the Pentagon, and to destroy a fourth aircraft in a foiled attempt to

attack the Capitol or the White House. In all, 2974 people were killed in the attacks.[9] The

intelligence community failed to identify the plot despite abundant information within the

intelligence system before it was carried out. The nearly 600 pages of the 9/11 Commission

Report examine in detail how the US government failed to understand and respond to the Al-

Qaeda threat and give many specific examples of how intelligence agencies failed to recognize

the significance of clear indicators, failed to share vital information, and failed to move decision

makers to action. The discussion which follows is based on information found in the Executive

Summary of the 9/11 Commission Report, Lawrence Wright's The Looming Tower, and James

Risen's State of War.

For example, Islamist terrorists, Al-Qaeda and Osama Bin Laden were known to US

intelligence as hostile to the United States and intent on carrying out attacks against Americans

at home and abroad. As the 9/11 Report put it "The 9/11 attacks were a shock, but they should

not have come as a surprise."[10] There was an extensive history of terrorist attacks by Islamist

extremists which should have made the threat clear to our intelligence community and decision

makers.

 In Februrary1993, Ramzi Yousef attacked the World Trade Center with a truck bomb

killing eight people and injuring a thousand. Omar Abdel Rahman and other plotters planning

attacks against the Holland and Lincoln tunnels and other New York City landmarks were

arrested and in October Somali tribesmen with links to Al-Qaeda attacked US soldiers in

Mogadishu. In 1995, a plot was uncovered in the Philippines to bomb multiple US airliners over

the Pacific and a car bomb attack took place against Americans working with the Saudi National

Guard in Riyadh. In 1996, a truck bomber killed 19 servicemen and wounded hundreds at

Khobar Towers in Dharan, Saudi Arabia. This collection of attacks should have left little doubt

about the terrorist threat; yet, terrorism remained fairly low among US intelligence priorities.

In February 1998, Osama Bin Laden and others publically issued a fatwa declaring war

on the United States and charging every Muslim with the duty to attack and kill Americans

wherever they might be found. If that left any doubt concerning Osama Bin Laden's intent to

harm America it should have been cleared away by the deadly August 1998 truck bombings of

the US embassies in Kenya and Tanzania in which 224 people were killed and thousands were

wounded by Al-Qaeda operatives. In December 1999, Jordanian officials stopped a plot to bomb

sites frequented by Americans and an extremist was stopped by US customs officials at the Canadian border en route to bomb the Los Angeles airport. The following year saw the bombing of the USS Cole in the harbor of Aden, Yemen by an Al-Qaeda team.

Thus, by 2000, there was little doubt that Al-Qaeda represented a serious threat to the United States. However, it was seen mostly as a law enforcement matter and intelligence linking al-Qaeda to these events was seen as circumstantial and not as direct evidence against Bin Laden himself. President Clinton and his advisors wanted concrete evidence of his involvement before taking decisive action. Although the CIA issued a "preliminary judgment" of Bin Laden's responsibility for the *Cole* attack, the administration saw it as insufficient to drive direct military action against him.[11] The President and his advisors wanted to wait for conclusive evidence before acting. Consequently, other than ineffectual cruise missile attacks following the embassy attacks and half hearted diplomatic efforts with the Taliban, nothing was done directly against Bin Laden. CIA plans to use surrogate forces to capture him and turn him over to the US were rejected because of a risk of killing him in the process.[12] A clear threat to the US was allowed to persist in an effort to seek certainty in the case against him. Consequently, al-Qaeda remained free to put in motion the planning and execution of the 9/11 attacks.

We now know that by late 1998 or early 1999 Osama Bin Laden had accepted a proposal by Khalid Sheik Mohammed for a terrorist attack using hijacked aircraft called the "planes operation." Shortly thereafter Al-Qaeda began to put it into operation. Operatives began training and in January 2000 US intelligence "glimpsed and then lost sight of two operatives" who were spotted in Kuala Lumpur and then passed through Bangkok to arrive in Los Angeles on 15 January 2000 where they proceeded to live openly under their true names.[13] Later that summer, operatives from a Hamburg, Germany Al-Qaeda cell arrived in the United States and

began pilot training. These operatives lived openly in the United States and freely used US banks spending over a quarter of a million dollars in the process.[14] Despite an FBI agent's memo asserting the threat of Islamist terrorists training at US flight schools, nothing was done to investigate the threat or even identify who might be involved in such training.[15] Had this thinking been followed up with effective intelligence work, it is possible that the 9/11 plot could have been disrupted.

When the Clinton Administration left office and the Bush administration took over, the matter of what to do about the *Cole* bombing remained unresolved. Evidence had accumulated, but not to a degree sufficient for immediate action. The Bush administration accepted Al-Qaeda responsibility but was proceeding slowly and deliberately in developing a three to five year plan for dealing with Al-Qaeda. Frustration was high among those responsible for anti-terrorism policy on the National Security Council. Richard Clarke who had enjoyed a higher profile under the Clinton administration was convinced the Bush administration was not properly prioritizing the terrorist threat.[16] As a consequence, a strategy directive for dealing with Al-Qaeda (including plans to arm the Predator aircraft for possible use in killing Bin Laden or his lieutenants) was not an approved draft until the 4th of September and was awaiting the President's review and approval when the attacks occurred on September 11th.[17]

Throughout the spring and summer of 2001, the US intelligence community was receiving multiple warnings that Al-Qaeda was planning "something very, very, very big" and the DCI, George Tenet described it as "the system was blinking red."[18] The problem was that there was nothing specific in the reporting and the greatest threat was thought to be to American interests overseas. Consequently, although precautions were taken abroad, little was done within the United States. In late summer, many of the terrorists' final preparations for the 9/11 attacks

were vulnerable to detection and disruption as operatives dropped out of the operation, were denied entry to the US, or were known to US intelligence to have entered the country months before. Unfortunately, these vulnerabilities were only clear in post attack analysis. Much of the information was buried in the intelligence, law enforcement, and immigration systems and had not been shared with the proper counter-terrorist organizations and analysts. The commission found that the US counterterrorism effort was fragmented within and among organizations, that counterterrorism was not a clear priority, and that information was not routinely shared or managed effectively across the government. By policy, practice, ineffectiveness, and in some cases misunderstanding of the law, information was often withheld by one agency or organization from another. There was no coherent, mutually informed effort across the government to deal with the clear threat of Islamist terrorism.

As the 9/11 Commission considered what the government knew and didn't know and what its agencies did and didn't do in response, it concluded that the United States needed a different way of organizing its efforts with the principle goal of developing unity of effort across the government. Of the five areas that the commission recommended for action, three were directly concerned with intelligence system shortfalls.[19] The commission found that there had been no unity of effort in the counter-terror intelligence and operational planning effort and that there was a foreign-domestic intelligence divide that hampered information sharing and collaborative analysis. Law enforcement elements of the FBI did not even share information with foreign intelligence elements of the FBI let alone across the broader intelligence community. Furthermore, there was no effective link to operational planning for counter-terror actions across the government. Policies hindering the sharing of intelligence information outside parent agencies were the norm across the intelligence community and even specific requests to

share information were frequently rebuffed, in some cases because of misunderstanding of the law and in other cases due to interagency mistrust and personality conflict. Information dissemination was restricted under a principle called "need to know" in which the norm was not to share information broadly but rather to limit sharing to only the smallest subset of people with a demonstrated need for closely classified information. This approach kept key analysts from even being aware of critical information already held by the government. The commission singled out this culture as a significant hindrance to effective collaboration and called for transition to a culture of "responsibility to share" in which intelligence collaboration and information sharing should be valued above limitations stemming from a desire to protect critical sources and methods.[20] The commission believed that the only way to overcome the problem of diverse intelligence agencies operating in isolation would be to unify the intelligence community under an effective National Intelligence Director wielding real authority over budgets, personnel, and activities.

These recommendations led to IRTPA's establishment of the Director of National Intelligence and efforts to improve intelligence sharing and collaboration across the intelligence community. A principal conclusion concerning the intelligence failures of 9/11 was that a failure to share information prevented the national intelligence community from putting together the pieces of the puzzle that the government already had to form an effective picture of the threat. The fundamental assumption of the post-9/11 reforms is that coherent, enterprise-wide management of the intelligence community will improve intelligence sharing and create effective collaboration to prevent similar failures in the future. Thus, the nation is staking its hopes on the ODNI – that it will be able to overcome agency independence and create a culture of cooperation. Although much progress has been made toward that end, it remains to be seen

whether the result will be substantially more effective than in the past. As I will argue later in this paper, these assumptions largely miss the point because in reality our intelligence failures stem from larger flaws in our intelligence and decision making dynamic than simply the inability to effectively collaborate. Even if perfect collaboration and flawless analysis of all data available to the intelligence community were to be achieved, it is unlikely that the degree of certainty would be sufficient for our decision makers to act proactively in response to ambiguous threats. Quite simply put, the intelligence community cannot produce the certain predictions of the future that our decision makers desire. There will always be great uncertainty.

It is now useful to turn our attention to intelligence errors in assessing Iraq's WMD capabilities – problems different from those noted in 9/11. As Mark M. Lowenthal, an intelligence officer of over thirty years experience and retired Assistant Director of Central Intelligence for Analysis and Production noted in a Washington Post op-ed: "In 9/11, intelligence was excoriated for 'failing to connect the dots' . . . but in Iraq, intelligence was blamed for connecting too many dots." [21]

Intelligence Failures in Iraqi WMD

Political discourse often obscures the facts. A popular narrative is that the Bush administration "cooked the books" to fake an Iraqi WMD threat in order to justify an invasion that key neo-cons were intent upon long before 9/11. This widely accepted contention reduces the intelligence failure with respect to Iraq to a problem of politicizing intelligence for nefarious motives.[22] As Chief of Intelligence Plans for the land component in the invasion of Iraq, I was quite well versed in the assessments of Iraqi WMD and the intelligence on which they were based. Contrary to wide belief, the Iraqi WMD assessments were not a Bush-Cheney-Rumsfeld-

19

Wolfowitz fiction, they were assessments broadly held throughout the intelligence community originating from the first Gulf War and well established and accepted during the Clinton administration. [23]   The assessments of Iraqi WMD were firmly held intelligence beliefs and the natural result of some fundamental flaws in our intelligence and national policy making systems. In order to understand whether similar mistakes can be avoided in the future, we need to examine how we got it so wrong with respect to Iraqi WMD.

During the Iran-Iraq War, Saddam Hussein responded to Iranian human wave attacks through the extensive use of chemical weapons. Their success solidified his conviction that they should be an essential part of the Iraqi arsenal. Similarly, his pursuit of nuclear capabilities in the development of the Tuwaitha reactor (bombed by the Israeli's in 1981) and his use of poison gas against his own population (against the Kurds in Halabja) made it clear to the international community that WMD capabilities were a key part of the Iraqi security regime.[24]

So, at the outset of the first Gulf War, we clearly understood that Saddam possessed those capabilities and that they posed a concrete threat to coalition forces. Nevertheless, the United States was surprised by the extent of what it found in Iraq at the end of that war. Iraq's chemical stockpiles were far more extensive than originally believed. Iraq was much further along in nuclear and missile development than previously assessed and it was pursuing biological weapons as well.[25] These findings were the basis for the punitive cease fire provisions requiring Iraq to disarm its WMD and missile capabilities. However, perhaps more significantly, these findings concerned the US intelligence community. Decision makers asked why we had it wrong – why had we been unaware of the extent of the Iraqi WMD programs?

We left the first Gulf War seeing that we had misunderstood the state of Iraqi WMD and we were determined not to repeat that failing. The view from the US was that Iraq had

successfully hidden the extent of its WMD programs and that we had missed it. As a result, Iraqi

WMD became a high priority requirement for the US intelligence system.   This highlights a

problem with a requirements-driven intelligence system like that of the US – you tend to focus

all your resources to find what you are looking for and practically none of your resources to

question long held assumptions. In the case of Iraq, we were determined to find WMD and

consequently we "did".

The invasion of Iraq provided us a very unique opportunity to assess our intelligence

analysis and national policy making. After the invasion, when WMD could not be found, the

administration dispatched a task force to determine how we could have been so wrong about the

state of Iraq's WMD programs. The Iraqi Study Group was headed by Charles Duelfer, who was

uniquely well qualified for the task.[26] He was a State Department official who had been the

Deputy Chief of the UNSCOM mission – the UN organization charged with monitoring Iraqi

compliance with the UN resolutions enforcing the first Gulf War cease fire. In that capacity

from 1993 to 2000, he had continuing contact with key leaders in the Iraqi regime and had

overseen UN weapons inspections within Iraq.   Since Iraq had been under years of sanctions and

US diplomatic contact had been severely limited during that time, he was the only US official

who had first hand relationships with, and insights to, members of the Iraqi regime. As a result,

he was well prepared to lead an unprecedented analysis of Iraqi decision making in response to

US actions through the years leading up to American occupation.

Indeed, this was a unique opportunity for the US to interview former regime members

and sift through the regime's records to reconstruct what the Iraqis were thinking in response to

US actions and what they had done in light of them. What Duelfer found was that we did not

understand Iraq and Iraq did not understand us in the years following the first Gulf War. Saddam

had perpetuated the fiction of Iraqi WMD in order to deter Iran at the same time that he was dismantling his WMD capabilities in an effort to escape continued sanctions. Duelfer found that Saddam dismantled his existing WMD in an effort to convince the UN that he had given up his WMD designs in the hopes that the sanctions would be lifted. However, at the same time he had every intention of restarting his WMD programs as soon as UN inspections were curtailed and for that purpose did not fully disclose his activities. As a result, the UN often found inconsistencies in his reporting and these disconnects fed US suspicions.[27]

When programs and capabilities which Iraq had denied were discovered, this convinced the UN inspectors, and even more so the US, that Saddam could not be trusted and that our intelligence was continuing to be deceived and mislead. The effect was to convince us that the absence of evidence meant we were being effectively deceived. It led us to accept defector reporting that was later found unreliable and to believe that fragmentary indicators should be seen as proof of a well-hidden WMD program.

Perhaps, the most well publicized failure of Iraqi WMD intelligence was the heavy reliance on a single human source codenamed "Curveball".[28] This was a third country intelligence source that was the origin of much of the case for Iraqi WMD. By the time it was clear that he was unreliable, his perspectives had permeated US intelligence analysis. As a result, post-Iraq intelligence reform initiatives have placed high importance on ensuring that the credibility of intelligence reporting underlying analytic products is clearly identified so that decision makers do not confuse conclusions based on fragmentary reporting with established fact. The net effect of many of the reforms has been to put great value in an "evidentiary" approach to intelligence. Reports and assessments now go to great lengths to identify the "evidence" on which analysis is based and make clear its assessed credibility.

When Saddam became frustrated that UN inspectors would not accept the fact that he had dismantled his programs, he sought leverage by decreasing cooperation and resisting inspection efforts. This, ironically, further convinced us that he had something to hide and we began making analytical judgments that went something like this – Saddam had been assessed as having a certain number of missiles. His records could not account for the destruction of all of them, yet they insisted they no longer had them. Although we could not find them anywhere in Iraq, we concluded they must exist and be well hidden. When he insisted he did not have them, we assumed he was being disingenuous and defiant and used our inability to find them as further evidence of the effectiveness of his deception programs and Iraqi non-compliance with sanctions.[29] After all, we had missed things in the past. Surely, we were being deceived yet again.

Since our previous experience convinced us our own intelligence was fallible, we dismissed the absence of evidence and continued in our faulty assessments. Since Saddam wanted strategic ambiguity about WMD with respect to Iran, he was hampered in his ability to persuade us. It was hard for him to foster the notion that WMD existed on the one hand for the benefit of deterring the Iranians while on the other hand trying to convince the UN that he had disarmed. This was a flawed, self-contradicting strategy that ultimately cost Saddam his life.

When analysts look through the lens of hindsight at the intelligence we relied on in making our assessments of Iraqi WMD, the case for WMD appears weak and flawed. It is impossible to go back and see the intelligence the same way now that we know the reality. Analytical reasoning that was persuasive under uncertainty, now looks illogical in light of the known reality. It is therefore tempting to dismiss our failures as an effort by a weak-willed intelligence community to conform analysis to political desires. The problem was not that

simple. The system *believed* its evaluations and decision makers were widely convinced. This leaves us with the question of how we could have drawn so many flawed conclusions and how we can avoid repeating those mistakes in the future. Let's look at this in more detail.

When the intelligence community is given a requirement (uncover the Iraqi WMD program) and when it knows it has been deceived and missed things in the past, it becomes determined to find evidence of what it is looking for. In intelligence, it is never safe to assume that because you have not seen something it is not there. After all, adversaries give their greatest effort to hiding from you those things that are most important to them. WMD was important to Saddam. It had kept the Iranians at bay. It had worked for him in the past. He wanted to keep it. After the first Gulf War, we had seen first hand how much we had missed. As a result, we were determined that no clue, no matter how small, should be overlooked.

The intelligence system is graded on how well it meets requirements. The requirement was to find Iraqi WMD. Analysts who pieced together convincing narratives from fragmentary evidence found their efforts rewarded. They did not set out to deceive, they were only determined to uncover WMD that our earlier experiences gave us substantial reason to believe existed. Thus, for example, when it could be plausibly argued that imagery showed a building had attributes of a biological weapons facility and when defectors reported such facilities existed, it was well intentioned analysis that "connected the dots" and made one 'evidence' of the other. In this way, we put together puzzle pieces that appeared to fit; that is, until we had the real picture in front of us after we invaded. So, in contrast to 9/11 in which we failed to recognize the threat in the face of ample evidence, in the case of Iraqi WMD we interpreted fragmentary evidence through the lens of long-held beliefs and put together a picture of WMD that did not exist.

As a result, our reforms have taken two general forms. In response to 9/11, we created a DNI to bring coherence to a fragmented enterprise and undertook initiatives to foster real intelligence sharing and collaboration across the government. In response to the flawed assessment of Iraqi WMD, we changed our analytic approach to ensure consideration of competing hypotheses. We now state explicitly in our intelligence products assessments of the credibility of reporting that supports our analytic conclusions. We are taking a much more evidentiary approach insisting that supposition be supported with concrete facts. These reforms combined with efforts to improve professionalization and diversity of the intelligence workforce, expand human intelligence capabilities, and bring greater rigor and external scrutiny to our analysis undoubtedly improve the effectiveness our intelligence processes. Unfortunately, I believe they do little to address more fundamental flaws in our approach to intelligence in support of national decision making.

Part III: What's Wrong with our Intelligence Support to Decision Making

As we have discussed above, our intelligence system failed us in different ways with respect to 9/11 and Iraqi WMD. On the one hand, the intelligence system does not do a good job of piecing together unfamiliar data and convincing decision makers of an emerging threat (9/11). On the other hand, the system is likely to stay wedded to long held conclusions about well established threats even long after new evidence should prompt reconsideration (Iraqi WMD).   I contend that both of these problems are an unintended consequence of the way we have structured our intelligence support to decision making and that we have inadvertently "trained" decision makers to expect certainty that it is not possible for intelligence to provide.

The central role we give to requirements to drive our collection and analysis creates a circumstance in which we put the vast majority of our effort into filling gaps in existing perspectives rather than challenging assumptions and developing new insights. Using requirements to organize our intelligence effort and ensure we are providing decision makers what they need is a strength of our intelligence system. However, it is also the system's Achilles heel.

In the beginning, when little is known about an adversary or issue, we gather information to characterize the problem for the decision maker. We start by shaping the leader's interest – identifying issues for consideration and questions to be answered. This shaping of the leader's perspective is an appropriate function of intelligence. We review what is known and make assumptions to fill in the gaps. We paint a plausible picture based on those assumptions and we brief the decision maker. The decision maker reasons from that view to decide what is important and begins to shape our policy responses. This generates intelligence requirements to fill the gaps – not from a neutral perspective in assessing objective reality – but from a subjective perspective through the lens of our own plans and policies and our initial insights to the problem set.

Although we do develop intelligence requirements designed to test assumptions, those very quickly lose emphasis as decisions are made to allocate scarce intelligence resources. As policy planning moves forward and resources are committed, there is a natural tendency to restrain second guessing. We become more and more bound to initial assumptions. The weight of the intelligence effort shifts from shaping the leader's interest, to feeding his interest. Our primary effort becomes answering the leader's most important questions. This is an appropriate

function of intelligence and in a perfect system would be balanced with the function of shaping and reshaping the leader's interest as circumstances change.

However, in practice, our requirements driven system leads us to progressively neglect the first function (shaping interest) while concentrating more, and more exclusively on the second (feeding it). In this way, we fall victim to shifting environments. We mobilize the intelligence system to seek greater and greater clarity based on old insights and fail to develop new insights that reflect changing circumstances. We begin to seek information that helps us execute our chosen courses of action while ignoring information that suggests flaws in our original assumptions. We never pause to ask – is it possible that there is no Iraqi WMD – rather we continue to look for evidence of it. Why? Because that is what the requirements told us to look for and that is where the inertia of the system drives us.

We formulate our policies and then set out to uncover those things the decision maker states are most important to executing it. Very quickly that becomes our sole focus -- how do we find what is important to our plan? This is a significant pitfall because it anchors us to past insights while failing to recognize or develop new ones. The result is that we become reactive as circumstances change. We tend to cling to initial assessments even in the face of countering inputs because our decision making occurs through the lens of our own plans and initial assessments. If there has been no crisis to elevate a subject to a priority in the decision makers' eyes, it is very hard for the intelligence system to thoroughly investigate it. There is little incentive to do so under the existing system.

Decision makers' requirements are based on their *known* interests and the intelligence system is optimized to find out more about what decision makers are already interested in. It is not very effective in introducing new interests for consideration or action. It is hard to change

the system's focus and analytic conclusions when the customer is not asking for that. Many analysts who saw clearly the terrorist threat before 9/11 or who doubted the continued existence of Iraqi WMD, found they could not even interest the intelligence system, let alone the decision makers, in examining the cases they made.[30] This is due to an inherent flaw in our requirements driven approach and will be little affected by the reforms to improve intelligence sharing or more clearly articulate the credibility of reporting sources that came out of the 9/11 and Iraqi WMD failures.

Critics of this line of thinking will point to any number of long term assessments and large scale intelligence projects designed to envision the future and claim that these efforts interject requirements for the system to investigate changes in the environment and challenge existing assumptions. The theory is that these requirements drive the system just as effectively as the decision makers' demands that gaps be filled. In practice, this rarely happens. The immediacy of the present consumes the vast majority of resources as decision makers seek greater and greater certainty for crisis decision making. Exploring new insights and challenging existing assumptions becomes a little appreciated, under resourced sideshow in the process.

Because additional information is being gathered as a function of our decision making requirements, little attention is paid to changes in the environment. Further intelligence work reinforces the original assessment by "filling gaps" while missing fundamental changes that are not being looked for. Consequently, as all effort is shifted into feeding the leaders' interest the intelligence responsibility of shaping the decision makers' interest is neglected. The result is that we operate off old insights long after changing circumstances have rendered them obsolete. As a consequence, we tend to be reactive and surprised when the enemy does not conform to our predictions. Our requirements-driven intelligence system guarantees that we will be slow to

recognize changed circumstances and unlikely to question original assumptions until forced to do so by strategic surprise, mission failure or unacceptable progress.

A second problem with our intelligence support to decision making, is that our system is so good at gathering concrete data that our decision makers erroneously believe that the proper response to uncertainty is to gather more data. Even though we were confident of Al-Qaeda's responsibility for the *Cole* bombing and the bombings of our embassies in Africa, we were unwilling to act against Bin Laden himself because we didn't have direct evidence of his personal involvement. We adopted a law enforcement approach that is evidence based and asked our intelligence system to provide evidence before we would act. Consequently, we delayed action while seeking certainty that was unlikely to ever come.

We persist in the belief that if only we are good enough at collection and analysis and information sharing we can produce certainty from our intelligence system. We focus our efforts and our reforms on improving effectiveness in building evidentiary cases. We look at our Iraqi WMD failure and decide we only needed to be more careful about what we accepted as evidence. We insist that we will be more certain before we act in the future. But in doing so, we miss a fundamental truth about intelligence. We will never be able to develop certainty about those things most important to our adversaries and most dangerous to us. Why? Because these are the things that they will invest the most effort in hiding from us or deceiving us about. Nevertheless, our decision makers proceed as if certainty should be expected from the intelligence system. This is a very consequential flaw.

Consider this observation: *familiarity often falsely suggests certainty while novelty often magnifies uncertainty.* I contend that this characteristic of how decision makers process information does much to explain both the 9/11 intelligence failure and the flawed Iraqi WMD

assessment.   In the case of 9/11, the terrorist threat from non-state actors was more unfamiliar and ambiguous than the familiar problem of WMD in Iraq. Consequently, in the case of 9/11 our leadership delayed decision making while seeking greater certainty while in the case of Iraq familiarity contributed to our acceptance of flawed intelligence as "certain". Both errors stemmed from a desire for certainty and a belief that intelligence can provide it.

The desire for concrete evidence also skews what we look for in our collection effort and even the types of collection we most rely on. Since it is easier to observe what an enemy is doing than it is to understand what he is thinking, we structure our intelligence system to try to see what is being done in order to predict intent instead of working to gain insight into intent in order to predict what adversary leaders or groups will do.   It is much easier to evaluate satellite imagery or communications intercepts than it is to figure out what is going on inside the head of an adversary leader or understand the group dynamics of a foreign government or population. Consequently, we expend far more resources in technical collection (pictures, intercepts, material samples, seismic readings, etc) than we do in assessing the human dynamics and decision making interests of our adversaries.[31]

As we prepared to invade Iraq in 2003, I saw this first hand. There were over 200 personnel dedicated to intelligence in the land component headquarters. As war approached we briefed the commander daily on our collection planning and the status of filling his priority intelligence requirements. Our focus was exclusively through the lens of our plan. We were spending our entire effort on refining our understanding of enemy defenses, force deployments, command and control networks, tracking of major weapons systems, target refinement, and other concrete aspects of the enemy force. By comparison we were spending virtually no effort on intangibles of enemy leadership or tribal and government personalities and dynamics that would

be critical to how different sectors would behave in post-Saddam Iraq. No more than four

intelligence personnel in the headquarters were dedicated to this task as we prepared to invade

(and even those four were diverted to current intelligence shortly after the invasion began).

Efforts to draw this information from the broader national intelligence system also failed. This

information was not critical to the immediate "fight"; so, it was not a priority for the intelligence

system. Consequently, we were ill-prepared for the challenge of governing in the wake of

combat operations. This was a specific result of the requirements driven approach of our

intelligence system and our quest for certainty in answering the commander's current questions

rather than developing insights to support critical future decision making.

To summarize: the problems with our intelligence support to decision making are not

likely to be resolved by the creation of the DNI, improved information sharing and collaboration,

or a more evidentiary approach to intelligence. Greater problems stem from our requirements-

driven approach that focuses almost entirely on filling gaps based on old insights while

neglecting efforts to understand the changing environment or develop new insights to shape our

leaders' interests. Lessons learned from 9/11 and Iraqi WMD have strengthened our

commitment to finding better "evidence" and have added to our decision makers' quest for

certainty from the intelligence system. This is a fundamental mistake; however, there is hope for

overcoming it. The final section of this paper makes recommendations on how we can improve

our intelligence system's support to decision making.

Part IV: Recommendations for a Better Approach

Improving our intelligence system does not require total rejection of the requirements

driven approach. It does require a better application of it. The solution begins with our decision

makers. We must help them understand that their primary challenge is to make timely decisions

under uncertainty, not to delay decision making while seeking certainty that will never come.

Intelligence officials must understand that they not only have a responsibility to answer decision

makers' questions and fill gaps important to execution of our plans and policies, but that they

also have a more important responsibility to continuously challenge initial assumptions and seek

to build new insights as circumstances change. We must recognize that spending all of our effort

in tracking what the enemy is doing sets us up to be victims of deception in the worst case and

continuously forfeiting the initiative in the best case. Instead, we should dedicate substantial

intelligence resources to studying our adversary's motives, interests, sources of power, regime

preservation structures, and group dynamics affecting decision making. In short, we need to

develop insight into adversary intent to predict what they will do, rather than looking at what

they are doing to predict what they intend.

To do this effectively, requires broad first hand contact with those we seek to understand.

For that reason, we must reject the habit of isolating ourselves from interaction with adversaries.

It is folly to forbid diplomatic contact, to limit official and unofficial travel, to cut off business

and student exchanges as we often do in an effort to create diplomatic isolation or economic

pressure through sanctions.   Our intelligence system cannot develop accurate insights into the

inner workings of a target entity without the most extensive contact possible with as many

adversary elements as possible. We need to augment first hand contact with the development of

more effective human intelligence networks and leverage partner intelligence capabilities from

within regions and cultures of interest. We must use academia, the diplomatic corps, allies, and

the business community for alternative views and continuously revisit our operating

assumptions. The intelligence community and decision makers must mutually understand that

the principal goal of intelligence should be to equip decision makers with insights for decision making under uncertainty. It must be understood that we are least likely to have clarity in those areas that are most important to us. It is much easier to hide and deceive than it is to discover that which is most closely guarded.[32] Consequently, we must be prepared to make assessments in the absence of evidence that are based on a thorough understanding of our adversaries' intent.

Conclusion

At the outset of this paper, we asked whether or not we could expect more intelligence failures like 9/11 and Iraq WMD in the future. The answer is far from certain. If we limit our intelligence reforms to the widely accepted lessons learned -- improved intelligence sharing, a coherent enterprise under the DNI, better discipline in evaluating the credibility of information and evidence upon which we base our analysis, then it is likely we will continue to fail. On the other hand, if our decision makers accept that intelligence cannot provide certainty and our intelligence community gives priority to equipping them with insights necessary to support decision making under uncertainty, then we will be much more capable of anticipating events, avoiding surprise, and maintaining the strategic initiative in an ever changing world.

ENDNOTES

[1]Spending on intelligence includes both the National Intelligence Program (NIP) and the Military Intelligence Program (MIP). The DNI released the 2008 NIP budget figure as $47.5 billion. The MIP budget for 2008 was estimated by the Federation of American Scientists to be at least $10 billion making the total US intelligence budget nearly $60 billion dollars for 2008.

[2] According to Wikipedia ,<http://en.wikipedia.org/wiki/ List_of_countries_by_military_ expenditures>. Only the US ($651B), China ($70B), France ($67B) and the UK ($64B) spent more on their entire defense budgets.

[3] National Intelligence: A Consumer's Guide, Washington, DC: ODNI, 2009, <www.fas.org/irp/dni/consumer.pdf >, 9.

[4] The intelligence cycle is found in many intelligence studies and references. The discussion included here was prepared with reference to the ODNI's National Intelligence Consumer's Guide, pp. 17-19.

[5] National Intelligence: A Consumer's Guide, 20.

[6] National Intelligence: A Consumer's Guide, 27. The National Intelligence Council is an analytic entity of the ODNI that serves as a bridge between the intelligence community and policy makers. It provides inputs to national intelligence priorities and provides collection and analysis guidance. It facilitates collaboration across the intelligence community and conducts liaison with private sector and academic experts. Most significantly, it produces National Intelligence Estimates – substantive, comprehensive assessments of critical national security subjects that become key drivers of national policy.

[7] This discussion of intelligence oversight mechanisms was prepared with reference to the ODNI's National Intelligence: A Consumer's Guide, pp. 61-68.

[8] In addition to the two studies cited here, there were multiple hearings in Congress, committee reports, intelligence agency analyses, and armed services reviews.

[9] *Wikipedia*, "September 11th Attacks", <http://en.wikipedia.org/wiki/September_11_attacks>.

[10] "Executive Summary." The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. <www.9-11commission.gov/report/ 911Report_Exec.htm> (archive), 2.

[11] 9/11 EXSUM, 4.

[12] James Risen, State of War, New York, Free press, 2006, 182-184.

[13] 9/11 EXSUM, 17.

[14] 9/11 EXSUM, 10.

[15] For a good discussion of the FBI's failure to act on suspicions of terrorist participation in flight training see "Coleen Rowley's Memo to FBI Director Robert Mueller", Time Magazine, May 21, 2002, <http://www.time.com/time/covers/1101020603/memo.html>.

[16] Richard Clarke was very unhappy with the new administration's pace in addressing terrorism. Beginning in January, he sent a memo to Condoleezza Rice describing Al-Qaeda as a first order threat and just a week before 9/11 issued a blistering memo complaining of foot dragging at the Pentagon and CIA. The 9/11 Commission Report, 343.

[17] 9/11 EXSUM, 5.

[18] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. <www.9-11commission.gov/report/ 911Report_Exec.htm> (archive), 254-277 and 9/11 EXSUM, 5.

[19] "Executive Summary." The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. <www.9-11commission.gov/report/ 911Report_Exec.htm> (archive), 14. The report specifically called for "unity of effort in five areas, beginning with unity of effort on the challenge of counterterrorism itself:
- unifying strategic intelligence and operational planning against Islamist terrorists across the foreign-domestic divide with a National Counterterrorism Center;
- unifying the intelligence community with a new National Intelligence Director
- unifying the many participants in the counterterrorism effort and their knowledge in a network-based information sharing system that transcends traditional government boundaries;
- unifying and strengthening congressional oversight to improve quality and accountability; and strengthening the FBI and homeland defenders."

[20] 9/11 EXSUM, 15-16.

[21] Lowenthal, Mark M. "Behind U.S. Intelligence Failures." Washington Post 25 May 2008, B01.

[22] Charges of politicization of intelligence are common and not limited to the case of the Bush Administration and Iraq. Gregory F. Treverton's article "Intelligence Analysis: Between "Politicization" and Irrelevance." Offers a detailed look at the difficulty analysts have in balancing responsiveness to policy makers' requests with effective intelligence analysis.

[23] In his book, the Threatening Storm, Richard Pollack an analyst for the CIA and the Clinton Administration National Security Council, details the case against Iraq.

[24] Risen, 96 and Charles Deulfer, Hide and Seek: The Search for Truth in Iraq, New York: Public Affairs, 2009, 62.

[25] Iraq's nuclear progress was particularly disturbing. Iraq was successfully using an obsolete technique known as electromagnetic isotope separation to enrich uranium. Since is it was an outmoded technique the US was not looking for evidence of it and consequently had no idea that Iraq was pursuing it. In fact, at the time of the first Gulf War Iraq had been pursuing it for six years without anyone outside the regime discovering it. Even though accidental bombing had led to the principal enrichment site's destruction, the fact that the US had not discovered it gave US intelligence good reason to doubt its ability to discern Iraqi WMD activities. Risen, 96-100.

[26] Charles Duelfer's book, Hide and Seek offers superb insight into how the US and Iraq misunderstood each other over time and why our intelligence assessments were so dramatically wrong. His perspective is unique and worth careful reading as he had both unprecedented contacts with Iraqi leadership in the years before the war during his role in the UN and his candid interviews with the leadership after Iraq fell.

[27] Duelfer, 78-79.

[28] Risen, 115-119.

[29] Duelfer, 88-89.

[30] An example is CIA analyst Tyler Drumheller's futile attempts to interest his leadership in warnings about the unreliability of Curveball's reporting. Risen, 115-116.

[31] In my role as intelligence planner for the ground component for the invasion of Iraq, I found CIA psychological assessments of Saddam some of the most useful materials in understanding his regime. However, I also found references to such studies were not compelling to the general officers leading the land forces. They were looking for concrete, tangible indicators of Iraqi action, not profiles that might offer understanding of the enemy leadership. I believe that the intelligence system would better serve decision makers by helping them gain greater insight into intangible factors of adversary decision making. There are many good works on such subjects to include David Ronfeldt's, Beware the Hubris-Nemesis Complex, Santa Monica, CA; Rand Corporation, 2004, in which he describes attributes of despots who seek WMD.

[32] There are many fine works on denial and deception which make it clear that it is easy to be deceived and that adversaries will employ sophisticated techniques to hide those things they believe most critical. For a good discussion, see James Bruce and Michael Bennett's "Foreign Denial and Deception: Analytical Imperatives," Analyzing Intelligence: Origins, Obstacles, and Innovations, Ed. Roger Z. George and James B. Bruce. Washington, DC: Georgetown University Press, 2008, 122-137.

BIBLIOGRAPHY

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (Authorized Edition). New York: W.W. Norton and Company, 2004.

Bruce, James and Michael Bennett. "Foreign Denial and Deception: Analytcial Imperatives." Analyzing Intelligence: Origins, Obstacles, and Innovations. Ed. Roger Z. George and James B. Bruce. Washington, DC: Georgetown University Press, 2008.

Comprehensive Report of the Special Advisor to the DCI on Iraq's Weapons of Mass Destruction.   30 September 2004. <www.cia.gove/library/reports/general-reports-1/iraq_wmd_2004/contents.html>.   28 June 2009.

Davis, Jack. "Strategic Warning: Intelligence Support in a World of Uncertainty and Surprise." Handbook of Intelligence Studies. Ed. Loch K. Johnson. New York: Routledge, 2007.

Duelfer, Charles. Hide and Seek: The Search for Truth in Iraq. New York: Public Affairs, 2009.

"Executive Summary." The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. <www.9-11commission.gov/report/911Report_Exec.htm> (archive) 28 June 2009.

Gannon, John C. "Managing Analysis in the Information Age." Analyzing Intelligence: Origins, Obstacles, and Innovations. Ed. Roger Z. George and James B. Bruce. Washington, DC: Georgetown University Press, 2008.

Grabo, Cynthia M. Anticipating Surprise: Analysis for Strategic Warning. Washington, DC: Joint Military Intelligence College, 2002.

Heuer, Richards J. Jr. Psychology of Intelligence Analysis.   Washington, DC: CIA, 1999.

Lowenthal, Mark M. "Behind U.S. Intelligence Failures." Washington Post 25 May 2008, B01.

McLaughlin, John. "Serving the National Policy Maker." Analyzing Intelligence: Origins, Obstacles, and Innovations. Ed. Roger Z. George and James B. Bruce. Washington, DC: Georgetown University Press, 2008.

Moore, David T. Critical Thinking and Intelligence Analysis.   Washington, DC: Joint Military Intelligence College, 2006.

National Intelligence: A Consumer's Guide. Washington, DC: ODNI, 2009. <www.fas.org/irp/dni/consumer.pdf >.   28 June 2009.

Pollack, Kenneth M. The Threatening Storm: The Case for Invading Iraq. New York: Random House, 2002.

Risen, James. State of War: The Secret History of the CIA and the Bush Administration. New York: Free Press, 2006.

Ronfeldt, David. Beware the Hubris-Nemesis Complex. Santa Monica, CA; Rand Corporation, 2004.

Schwartz, Peter and Doug Randall. "Ahead of the Curve: Anticipating Strategic Surprises." How to Anticipate Forcing Events and Wild Cards in Global Politics. Ed. Francis Fukuyama. Washington, DC: Brookings Institution Press, 2007.

Steinberg, James B. "The Policy Maker's Perspective: Transparency and Partnership." Analyzing Intelligence: Origins, Obstacles, and Innovations. Ed. Roger Z. George and James B. Bruce. Washington, DC: Georgetown University Press, 2008.

Teitelbaum, Lorne. The Impact of the Information Revolution on Policymakers' Use of Intelligence Analysis. Santa Monica, CA: Rand Corporation, 2005.

Treverton, Gregory F. "Intelligence Analysis: Between "Politicization" and Irrelevance." Analyzing Intelligence: Origins, Obstacles, and Innovations. Ed. Roger Z. George and James B. Bruce. Washington, DC: Georgetown University Press, 2008.

Treverton, Gregory F. and C. Bryan Gabbard. Assessing the Tradecraft of Intelligence Analysis. Santa Monica, CA: Rand Corporation, 2008.

Wright, Lawrence. The Looming Tower: Al-Qaeda and the Road to 9/11. New York: Alfred A. Knopf, 2006