A Look at Intelligence Analysis

by Stéphane J. Lefebvre, CD

PRELIMINARY DRAFT

Comments are welcome and should be sent to the following e-mail address:
Stephane.Lefebvre@rogers.com

POSTER Presentation TC99, Thursday, February 27, 2003 (1:45-3:30 PM)
International Studies Association (ISA)
44th Annual International Convention
Portland, Oregon, February 25-March 1, 2003

Biography: Mr. Stéphane Lefebvre has had a long and varied experience as a Canadian government strategic and intelligence analyst. He has worked as a Defence Scientist (strategic analysis) at the Department of National Defence, and briefly served at NATO Headquarters and the then North Atlantic Assembly. In 1992-1993, he was the *Marcel Cadieux Policy Planning Fellow* at the Department of Foreign Affairs and International Trade. He has also lectured for the Canadian Forces Military College, and served as an army reserve intelligence officer from 1987 until 2001. Mr. Lefebvre has published several book chapters and scholarly articles on security-related issues over the years and currently serves on the editorial board of the *Journal of Slavic Military Studies*. In 2002, he was awarded the *The Commemorative Medal for the Golden Jubilee of Her Majesty Queen Elizabeth II* by the Government of Canada in recognition for his significant contribution to his country.

In the hours, days, and weeks that followed the tragic terrorist attacks against the United States on September 11, 2001 (henceforth 9/11), several students of intelligence and politicians were quick to assign blame to US intelligence agencies, in particular the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI). That these agencies could not prevent the attacks was considered an immense intelligence failure of the type suffered at Pearl Harbor in December 1941.[1]

Characterizations of this nature were uttered by prominent academics, politicians, and citizens on the spur of the moment, their authors not yet knowing what intelligence on the perpetrators the Administration had or had not gathered, processed, analyzed and distributed, and what actions it had actually taken on any discovered threats. They simply assumed, as John Prados succintly put, that the US 'intelligence community somehow *had* to have known about the terrorists' plans for these events [9/11] and had ignored the information, or worse, misapplied or misanalyzed the intelligence.'[2] It was extremely doubtful, however, that any intelligence analysts or case officers would have sat idle on specific intelligence indicating a concerted terrorist attack on 9/11.[3]

It is easy to blame intelligence agencies for the death of 3,000 innocent people. But by its

---

[1] One typical quote: 'This one is a spectacular intelligence failure. I think it will go down in history as the United States's 21st-century Pear Harbor.' - Professor W. Wark, University of Toronto, quoted by M. Mittelstaedt, 'Spy Cloak Left in Shreds,' *Globe and Mail* (September 12, 2001) A2.

[2] J. Prados, *Lost Crusader: The Secret Wars of CIA Director William Colby* (Oxford: Oxford University Press, 2003) ix.

[3] Acting Defense Intelligence Agency (henceforth DIA) Director Rear Adm. L. E. Jacoby, US Navy, expressed a similar belief: 'I want to emphasize that I do not believe any information "owner" has failed to rapidly share even a shred of information that it deems as conveying either an explicit or implicit threat to United States citizens or activities. I believe the un-shared information falls largely into the categories of background or contextual data, sourcing, seemingly benign activities, and the like. But [...] it is within these categories that the critical "connecting dot" may well be found.' Jacoby, 'Information Sharing of Terrorism-Related Data,' Statement for the Record before the Joint Intelligence Committee of the US Senate and US House of Representatives investigating the events leading to the attacks of September 11, 2001, Public Hearing (Washington, D.C.: October 1, 2002) 5.

very nature intelligence is imperfect. Its targets are often elusive. You can expect terrorists, for instance, to use denial and deception[4] techniques to ensure that any intelligence collected against them will be ambiguous and inconclusive in the eyes of the collectors and analysts. This will be compounded by the difficulty of infiltrating terrorist organizations.[5] Solely blaming the intelligence community for the 9/11 attacks is therefore unfair. The statement made by Congressman Michael N. Castle (R-DE) in the House of Representatives three months after 9/11 reflects this sentiment:

> I do not for one moment blame the attacks in New York, Washington, and Pennsylvania on an intelligence failure. Indeed, that blame can only be assigned to radical fanatics who would see America fall. But I do assign some blame on our collective lack of attention for maintaining a robust, properly resourced, and forward-leaning intelligence community that is not unduly restricted from collecting information on foreign threats to our country.[6]

While many were quick to pronounce the 9/11 attacks a failure for the US intelligence community, very few took the time to explain what they meant exactly by 'intelligence failure.' Did 9/11 happen because: (1) the analysis of intelligence collected was deficient (2) the necessary intelligence could not be collected because intelligence collection planners in Washington or the case

---

[4] '*Denial* refers to the attempt to block information that could be used by an opponent to learm some truth. *Deception*, by contrast, refers to a nation's [or, I would add, a terrorist organization's] effort to cause an adversary to believe something that is not true.' R. Godson and J. J. Wirtz, 'Strategic Denial and Deception,' in *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. by R. Godson and J. J. Wirtz (New Brunswick, NJ: Transaction, 2002) 1-2.

[5] 'Intelligence can rarely be perfect and unambiguous,' especially when it must compose with 'crafty opponents who strategize against it and the alien cultures that are not transparent to American minds.' R. K. Betts, 'Intelligence Test: The Limits of Prevention,' in *How Did This Happen? Terrorism and the New War*, ed. by J. F. Hoge, Jr., and G. Rose (New York, NY: Public Affairs, 2001) 160.

[6] *Congressional Record* 147:172 (December 12, 2001) H9251. CIA Deputy Director J. L. Pavitt also placed the blame squarely on the perpetrators: 'The primary cause of the attacks was not a memo ignored, a message untranslated, or a name left off a watch list. Their primary cause was a man named Osama Bin Laden and a group named al Qaeda.' Quoted by B. Gertz, 'CIA Head Says Agency Not At Fault For 9/11 Lapses,' *Washington Times* (January 24, 2003) 3.

officers on the ground were not aggressive enough and lacked foresight (3) of the inherent bureaucratic impediments preventing the appropriate intelligence to reach the right policy consumers in a timely fashion or (4) of a combination of any of these reasons? The question needs to be answered before blame could be fairly apportioned.[7]

The literature on intelligence is divided on the matter. Some argue that most intelligence failures occur either because policy consumers disregard or misinterpret the intelligence reporting they receive (as a result of bureaucratic, organizational or psychological pathologies),[8] whereas others argue that they are essentially the result of faulty analysis and/or inadequate intelligence collection.[9] With respect to the CIA, John Gentry has argued in a highly provocative book that analytical errors are in a sense inevitable when 'intelligence organizations have the institutional courage to tackle difficult issues when the facts are few, intentions obscure and developing, fog

---

[7] As S. Aftergood of the Federation of American Scientists aptly noted, 'before the United States spends more money on intelligence, officials need to understand where intelligence failed.' D. Davidson, 'Lawmakers To Assess Intelligence First, Spend Later,' *Defense News*, 16:36 (September 17-23, 2001) 4.

[8] See, inter alia, W. C. Matthias, *America's Strategic Blunders: Intelligence Analysis and National Security Policy, 1936-1991* (University Park, PA: Penn State Press, 2001); Paper by J. Sims in *What Is Intelligence?*, by A. Shulsky and J. Sims with discussion (Washington, D.C.: Consortium for the Study of Intelligence, Working Group on Intelligence Reform, April 29, 1992) 6.; A. Kovacs, 'The Nonuse of Intelligence,' *International Journal of Intelligence and CounterIntellience* 10:4 (1997-1998) 383; L. K. Johnson, *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security* (New York: NY University Press, 2000) 191; Rear Adm. (Ret.) T. A. Brooks, 'The Importance of Understanding the Enemy,' *Washington Times* (February 13, 2002) 20.

[9] See, inter alia, R. J.Heuer, Jr. *Psychology of Intelligence Analysis* (Washington, D.C.: CIA, Center for the Study of Intelligence, 1999) 65. The literature on strategic suprise and intelligence failure is quite interesting in this regard. Key texts include E. Kam, *Surprise Attack: The Victim's Perspectice* (Cambridge, MA: Harvard University Press, 1988); A. Levite, *Intelligence and Strategic Surprises* (New York, NY: Columbia University Press, 1987); J. J. Wirtz, *The Tet Offensive: Intelligence Failure in War* Ithaca, NY: Colombia University Press, 1991); R. Betts, *Surprise Attack: Lessons for Defense Planning* (Washington, D.C.:Brookings Institution, 1982); and R. Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962).

thick, and noise levels high.'[10] According to him, analytical deficiencies within the CIA are numerous, but are primarily the result of an incompetent management more interested in its self-promotion than putting forward sound but unwelcome judgments to the next level in the review process. In other words, Gentry laments 'the power of management to control ideas.'[11]

With respect to 9/11, US Congressmen also alluded to a bureaucratic rather than an intelligence collection or analytic failure. The difference with Gentry, however, is that theirs was not a look at the problem of failure from within, but from without. In their 2002 intelligence authorization proposal, they put forward the notion that for several years the US government had placed too much emphasis on tactical requirements and not enough on predictive, strategic intelligence. This situation contributed, in their opinion, 'to shortfalls such as the lack of warning of recent nuclear tests, the lack of information on the New York and Washington D.C. terrorist attacks, the inability to monitor key facilities suspected of producing weapons of mass destruction, the bombing of the Chinese Embassy in Belgrade...'[12] Consistent with this judgment, they refused to blame the intelligence community for 9/11 and instead faulted the government as a whole for not fully understanding nor wanting 'to appreciate the significance of new threats to our national

---

[10] J. A. Gentry, *Lost Promise. How CIA Analysis Misserves the Nation: An Intelligence Assessment* (Lanham: University Press of America, 1993) 208. The notion of 'noise' versus 'signals' was developed by Wohlstetter in *Pearl Harbor*. K. Wheaton colorfully commented along the same line of thinking, essentially saying that no matter how good an analyst is, he must deal with his chain of command and sometimes see his work massacred because 'the boss is an idiot.' Wheaton, *The Warning Solution: Intelligent Analysis In The Age Of Information Overload* (Fairfax, VA: AFCEA International Press, April 2001) 10.

[11] Gentry, *Lost Promise*, 211.

[12] US Congress. *Intelligence Authorization Act for Fiscal Year 2002*, House Report 107-219 (henceforth HR 107-219) (Washington, D.C.: 107th Congress, 1st Session, September 26, 2001) 11-12.

security, despite the warnings offered by the Intelligence Community.'[13]

Intelligence failures, however, are rarely unidimensional in scope. Intelligence analysis, for example, is not done in a vacuum; it needs a bureaucratic structure to hire analysts, support their work, and channel their judgments to policy consumers. After looking at a series of apparent analytic failures to foresee events such as the Aum Shinrikyo nerve gas attack in 1995, the Indian nuclear test in 1998, North Korea's ballistic missile test in 1999, and the bombing of the USS Cole in 2000, Bruce Berkowitz concluded that these cases shared similar problems, namely, that the intelligence analytical community had showed 'organizational rigidity, poor planning, insufficient use of outside sources, and isolation of intelligence providers and consumers.'[14] The specialized literature on intelligence has paid particular attention to the analyst's mind and work environment in trying to explain analytic failures of the kind noted by Berkowitz. Frequently cited are the 'intelligence-to-please' syndrome, which amounts to analysts telling policy consumers what they think the latter expect to hear,[15] the 'unavailability of information when and where needed'[16] (because of impediments such overly stringent security regulations, bureaucratic jealousies, power struggles, compartmentalization of analysis, and analysts failing to master the retrieval tools at their disposal), the ready acceptance of 'conventional wisdom' (or the unwillingness to think outside of the box) so

---

[13] HR 107-219, 17-18.

[14] B. Berkowitz, 'Better Ways to Fix U.S. Intelligence,' *Orbis* 45:4 (Fall 2001), from the Internet version posted at http://wwwfindarticles.com.

[15] A. N. Shulsky and G. J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, Third Edition (Washington, D.C.: Brassey's Inc, 2002 [1991, 1993]) 64. For a concrete illustration of the 'intelligence to please syndrome,' see H. Billings, *Vietnam Follies: A Memoir of an Intelligence Officer* (1st Book Library, 2002); and the interesting comment in Wirtz, *The Tet Offensive*, 273-274.

[16] Shulsky and Schmitt, *Silent Warfare*, 65.

as not to upset the hierarchy, and 'mirror-imaging' (the process of judging and foreseeing the behaviors and decision processes of others as our own).[17] Given the ease with which any of these faults could occur, it should not come as a surprise that they would resurface in any in-depth look at whether or not, in the case of 9/11, relevant intelligence was 'discounted, misinterpreted, ignored, rejected, or overlooked because it fails to fit a prevailing mental model or mind-set.'[18] To wit, according to the Joint Inquiry Staff statement of September 18, 2002, there were no indications that: prior to September 11, analysts in the Intelligence Community were:

- cataloguing information regarding the use of airplanes as weapons as a terrorist tactic;
- sending requirements to collectors to look for additional information on this threat; or
- considering the likelihood that Usama Bin Ladin, al-Qa'ida, or any other terrorist group, would attack the United States or U.S. interests in this way.[19]

Regarding the much reported electronic communication from the FBI's Phoenix office discussing flight training and the investigation of Zacarias Massaoui (arrested in August 2001 and indicted four months later on six counts of conspiring to commit acts of international terrorism), the Joint Inquiry Staff added to its criticism the fact that these and other events were seen in isolation

---

[17] Shulsky and Schmitt, *Silent Warfare*, 65-67. One recent case of mirror-imaging is the assessment by US intelligence analysts that Iraq would not invade Kuweit in 1990 because of their belief that Iraq would instead rebuild after its major war with Iran just as the United States would do in similar circumstances. R. L. Russell, 'CIA's Strategic Intelligence in Iraq,' *Political Science Quarterly* 117:2 (202) 196. With respect to conventional wisdom, R. Peters has complained that the US 'intelligence community is, above all, a massive bureaucracy—and bureaucracies discourage risk-taking or excellence that does not match the models of the past. The motto of our vast intelligence establishment is "Play it safe."' Peters, *Beyond Terror: Strategy in a Changing World* (Mechanicsburg, PA: Stackpole Book, 2002) 197.

[18] Heuer, *Psychology of Intelligence Analysis*, 65.

[19] E. Hill, Joint Inquiry Staff Statement before the Joint Intelligence Committee of the US Senate and US House of Representatives investigating the events leading to the attacks of September 11, 2001, Public Hearing (Washington, D.C.: September 18, 2002).

from each other, preventing terrorism analysts and investigators from developing 'a comprehensive and current understanding of the overall context in which terrorist networks like al-Qa'ida operate.'[20] The Joint Inquiry Staff's Final Report was scathing in its discussion of the intelligence community's analytic performance. It reads:

> Prior to September 11, the Intelligence Community's understanding of al-Qa'ida was hampered by insufficient analytic focus and quality, particularly in terms of strategic analysis. Analysis and analysts were not always used effectively because of the perception in some quarters of the Intelligence Community that they were less important to agency counterterrorism missions than were operations personnel. The quality of counterterrorism analysis was inconsistent, and many analysts were inexperienced, unqualified, under-trained, and without access to critical information. As a result, there was a dearth of creative, aggressive analysis targeting Bin Ladin and a persistent inability to comprehend the collective significance of individual pieces of intelligence. These analytic deficiencies seriously undercut the ability of U.S. policymakers to understand the full nature of the threat, and to make fully informed decisions.[21]

The kernel of the problem with respect to intelligence analysis, therefore, seems to reside in the analyst's mind—in his thought processes—and with his hierarchy. Although, as Shulsky explains, 'it may not be possible to lay down rules that will inevitably guide us to analyze intelligence information correctly, it is nevertheless useful to try to identify intellectual errors or deficiencies that may be characteristic of the analytical process.'[22] It is to that task that the rest of this paper is devoted. The following sections examine the nature of intelligence analysis, the analyst's

---

[20] E. Hill, 'The FBI's Handling of the Phoenix Electronic Communication and Investigation of Zacarias Moussaoui Prior to September 11, 2001,' Statement before the Joint Intelligence Committee of the U.S. Senate and U.S. House of Representatives investigating the events leading to the attacks of September 11, 2001, Public Hearing (Washington, D.C.: September 24, 2002).

[21] Joint Inquiry Staff, *Final Report: The Context. Part I: Findings and Conclusions* (Washington, D.C.: December 10, 2002) 7.

[22] Shulsky and Schmitt, *Silent Warfare*, 72-73.

mind at work, the analysis of terrorism, how analysts deal with uncertainty, the use of technology in analysis, and suggestions on the way ahead. In doing so, this paper aims at providing readers with a better general appreciation of what intelligence analysis is all about.

What is Intelligence Analysis?

The literature on intelligence analysis offers a rather mixed account of the discipline. For Mark Lowenthal, 'the literature on analysis is rich,'[23] whereas John Gentry describes it as small, 'filled with judgments and assertions at variance with [...] reality,' containing factual errors, showing ignorance, and missing key aspects of the discipline.[24]

The bulk of the writing on the subject is descriptive in nature, and generally limits its examination at how the bureaucracy manages analysis as a deliverable, while briefly mentioning key errors of logic or fallacies. It is dominated by a wide collection of book chapters, with infrequent articles in leading intelligence journals (e.g., *Intelligence and National Security* and the *International Journal of Intelligence and CounterIntelligence*) and an even fewer number of books. I share Gentry's view that breath and depth is often lacking, but recognize that serious, useful work has been undertaken in this area by scholars and practitioners.[25] Arthur Hulnick aptly captured, I think, how intelligence analysis fares in the field of intelligence studies when he quipped that 'intelligence analysis is the most fascinating and yet the least understood or recognized part of the intelligence

[23] M. M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2000) 96.

[24] Gentry, *Lost Promise*, 207.

[25] The work cited in this paper are indicative of the richness and quality of this literature, if not its size.

process.'[26]

There seems to be a general consensus that analysis is important to intelligence. Why would intelligence agencies collect mountains of intelligence data if not to make sense of them and provide policymakers with their best judgments as to their meaning and implications? There is simply no point in collecting data to sit idle, untouched, and unanalyzed forever. Analysis, therefore, is central to the mission of any intelligence community

Broadly understood, intelligence analysis is the process of evaluating and transforming raw data acquired covertly into descriptions, explanations, and judgments for policy consumers. It involves assessing the reliability and credibility of the data and comparing it to the knowledge base available to the analyst to separate fact from error and uncover deception. Each collected item is then examined to determine its nature, proportion, function, relevancy, and interrelationships. Related items will be grouped together and the extent to which they confirm, supplement, or contradict each other will be determined. Once done, the relevant information will be synthesized in order for the analyst to make predictions, gain insight, identify information gaps, or explain a complex set of facts and relationships. Analysts add value to this process by using their substantive knowledge of the issue at hand and adding, where appropriate, relevant open information. The reverse also holds. Analysis may start from a review and assessment of the relevant open sources, to which would be added 'the special knowledge that cannot be obtained without utilizing intelligence sources and methods.'[27]

---

[26] A. S. Hulnick, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century* (Westport, Connecticut: Praeger, 1999) 13.

[27] J. H. Hedley, 'Checklist for the Future of Intelligence,' ISD Occasional Paper (Washington, D.C.: Georgetown University, Institute for the Study of Diplomacy, March 1995), Internet version accessed at

Most intelligence analysis is predictive in nature and follows a simple pattern: it describes what is known ➜ it highlights the interrelationships that form the basis for the judgments ➜ it offers a forecast. Of course, accurate estimates depend at least as much upon the mental model used by the analyst as upon the accuracy and completeness of the information itself. Potential developments are based on the analysis of factors (e.g., intent and capabilities) that together would logically bring about a certain future. If one or more of the factors should change or be wrong, the basis of the forecast would no longer hold. The basis of the forecast should be clear: is it supported by the facts at hand or not, and are the assumptions upon which it is based stem from past practice(s) or logical extensions of what is known? The simplest definition that describes this process best is Andrew Ilachinski's: 'Conventional intelligence analysis consists of first assessing the information describing a situation and then predicting its future development.'[28]

In practice, many analysts follow a simple two-step methodology to do that. As Stephen Marrin explains, 'they use intuitive "pattern and trend analysis"—consisting of the identification of repeated behavior over time and increases or decreases in that behavior—to uncover changes in some aspect of international behavior that could have national security implications.'[29] The significance of the pattern uncovered is then determined in an ad hoc fashion on the basis of each analyst's mental models (derived largely from the academic discipline(s) in which they were educated), which

---

http://sfswww.georgetown.edu/sfs/programs/isd/files/intell.hrm on January 28, 2003.

[28] A. Ilachinski, *Land Warfare and Complexity, Part II: An Assessment of the Applicability of Nonlinear Dynamics and Complex systems Theory to the Study of Land Warfare* (Alexandria, VA: Center for Naval Analyses, CRM 96-68, July 1996) 58.

[29] S. Marrin, *Homeland Security and the Analysis of Foreign Intelligence*, paper written for the Markle Foundation Task Force on National Security in the Information Age (July 15, 2002) 8. M. V. Kauppi qualifies this approach as 'a time-honored element of intelligence analysis.' Kauppi, 'Counterterrorism Analysis 101,' *Defense Intelligence Journal* 11:1 (2002) 47.

presupposes depth of knowledge. When using this two-step approach, anticipating the future in a linear form of thinking from the past must be avoided.[30] Forecasts in which 'the past is prologue, and forecasting amounts to linear extrapolation of the past trend into the future,' explains Charles Doran, 'ultimately fail because no technique has been developed that allows the forecaster to predict, prior to the event itself, when a nonlinearity will occur.'[31] In other words, as John Lukacs reminds us, 'historical causality is not mechanical, mostly because of free will. Also: what happens is not separable from what people think happens.'[32] While the use of history cannot be avoided to fully understand an issue, analysts must remain cautious not to poison the well by using it selectively to bolster their judgments for political, partisan or personal benefit.[33]

To determine how a situation will develop, analysts must nevertheless start somewhere and look at recent behavior as the most realistic starting point. Rather than thinking linearly, however, analysts must remain mindful of the distinction between possibilities and probabilities, and 'speculate about the full theoretical range of possible developments.'[34] What is possible would be rated against the relative capabilities of the actors involved and what is probable against the actors'

---

[30] D. F. Hayes, 'Whence the Terrorist Threat to OSCE States?' paper presented to the OSCE Forum for Security Cooperation's Terrorism Experts Meeting (Vienna: May 14-15, 2002) 2.

[31] See C. Doran, 'Why Forecasts Fail: The Limits and Potential of Forecasting in International Relations and Economics,' *International Studies Review* 1:2 (1999) 11-41.

[32] J. Lukacs, *At the End of an Age* (New Haven, CT: Yale University Press, 2002) 187.

[33] On this, see W. C. Burris, 'The Uses of History in Intelligence Analysis,' *International Journal of Intelligence and CounterIntelligence* 6:3 (1993) 297-301. As Burris wrote, historians study what has happened and intelligence analysts 'what whill happen next.' Ralph Peters also cautions not to 'look for answers in recent history, which is still unclear and subject to personal emotion.' Peters, *Beyond Terror*, 65.

[34] K. Booth, 'Military Power, Military Force, and Soviet Foreign Policy,' in *Soviet Naval Developments: Capability and Context* ed. by M. MccGwire (New York, NY: Praeger, 1973) 33.

known intentions, capabilities and behavioral constraints shaped by their environment. Another way to escape the linear thinking trap when looking at an actor's past behavior is to undertake counterfactual analysis, that is, using 'what if' statements about the past to determine if history could have taken a different course or its effects have been explained by different variables. A counterfactual analysis of the Aldrich Ames's espionage case was conducted by the CIA.[35] Counterfactual analysis implies, though, that the past is fixed and certain, but not its interpretation, a matter hotly contested by constructionists who argue that the past is uncertain and 'wholly dependent upon one's interpretative stance [...].'[36]

The references in the preceding paragraph to academic disciplines and counterfactual analysis suggest common ground between academic work and intelligence analysis. Just as in the academic world, there are many intelligence analytical disciplines. They range from highly technical and specialized ones such as medical intelligence (MEDINT),[37] imagery intelligence (IMINT), signals intelligence (SIGINT), measurements and signature intelligence (MASINT), and human intelligence

---

[35] The CIA 'imagined a series of procedures that might have been in place and asked which, if any of them, might have tripped up Ames.' R. N. Lebow, 'What's So Different About a Counterfactual?' *World Politics* 52 (July 2000) 552.

[36] R. Hassig, 'Counterfactuals and Revisionism in Historical Explanation,' *Anthropological Theory* 1:1 (March 2001) 58.

[37] 'Medical intelligence is described in Department of Defence Joint Pub 1-02 as 'That category of intelligence resulting from the collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information which is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting force and formation of assessments of foreign medical capabilities in both military and civilian sectors.' See D. C. Kaufman, *Medical Intelligence: A Theater Engagement Tool*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, February 21, 2001) 1.

(HUMINT),[38] primarily concerned with the transformation of 'highly specialized data, totally or virtually incomprehensible to everyone but the specialist, into data that other intelligence analysts can use,'[39] to less technical social sciences disciplines such as political science, international relations, comparative politics and area studies, sociology, and economics. The scholar and the all-source intelligence analyst would also have a similar sense of purpose. As Reg Whitaker describes it,

> Intelligence and academia are both in a sense the same business: the systematic and organized collection, analysis, and interpretation of information—and the construction of theories to explain the facts thus processed. [...] Both [...] tend to labor within frameworks that structure and sometimes limit their capacity to understand changing or disconsonant reality.[40]

On several points, however, they differ as to how they go about their business. The intelligence analyst has access to secret information not available to the scholar, while the scholar makes his work accessible to all. The work of the intelligence analyst is intended only for a small, selected number of policy consumers, while the scholar seeks the broadest possible audience. The intelligence analyst deals with problems whose consequences could be dire, while the scholar works simply for the cooperative pursuit of knowledge. The intelligence analyst works under considerable

---

[38] In the 1999 *Director of Central Intelligence Annual Report for the United States Intelligence Community* (Washington, D.C. May 1999), IMINT is defined as 'the collection, processing, and analysis of imagery for intelligence reasons;' SIGINT as 'intelligence information derived from all communications intelligence, electronics intelligence and foreign instrumentation signals intelligence, however transmitted or collected;' MASINT as 'technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and moving targets;' and HUMINT as 'a category of intelligence information derived from human sources.'

[39] Shulsky and Schmitt, *Silent Warfare*, 41.

[40] R. Whitaker, *The End of Privacy: How Total Surveillance Is Becoming A Reality* (New York, NY: The New Press, 1999) 9.

time constraints on topics required by policy consumers, while the scholar typically selects his subject matter and sets his research, analysis and production schedule at his own discretion.[41]

With respect to the disciplines that are common to both scholars and intelligence analysts, the analytic techniques employed by intelligence analysts may not be very different than those in use in the 'corresponding social sciences.'[42] While reporting indicates that intelligence analysts prefer the two-step approach to analysis described above, the argument that the overall quality of their analysis would be enhanced by a solid grounding in social sciences methodologies is, I think, valid.[43] Causal models, and Delphi, formulaic (or Bayesian), psycho-linguistic, pattern (e.g., link analysis, association and activities matrices) and other analytical techniques could be used to profit by an intelligence analyst faced with a large amount of raw data on a particular issue or individuals.[44]

Intelligence analysis, however, is not focused on producing methodologically complex and long documents. Nor does it try to compete with other sources of information easily available to policy consumers. It should excel, however, at being able to advise a consumer of a new or lingering situation and of its meaning and implications for him. Many different vehicles can be used to provide

---

[41] Whitaker, *The End of Privacy*, 10; Shulsky and Schmitt, *Silent Warfare*, 55-56.

[42] Shulsky and Schmitt, *Silent Warfare*, 52.

[43] Intelligence analysts should therefore be very familar with works such as G. King, R. O. Keohane and S. Verba, *Designing Social Inquiry: Scientific Inference in Qualitative Research* (Princeton, NJ: Princeton University Press, 1994); G. K. Huysamen, *Methodology for the Social and Behavioral Sciences* (Johannesburg: International Thompson Publishing, 1994); S. Van Evera, *Guide to Methods for Students of Political Science* (Ithaca, NY: Cornell University Press, 1997); J. Best, *Damned Lies and Statistics: Untangling Numbers from the Media, Politicians, and Activists* (Berkeley: University of California Press, 2001); C. Hay, *Political Analysis: A Critical Introduction* (Houndmills: Palgrave, 2002); and many more.

[44] The analysis conducted by think-tank such as the Rand Corporation and the Center for Naval Analyses serves as an excellent model of analytical work employing a full range of methodologies to address complex issues and forecast their development.

intelligence insight. While the written product still carries a lot of weight, especially for the analysts concerned with quantity rather than quality (the well-known 'publish or perish' dilemma), oral briefings and analyses in the form of graphics are not uncommon. Current intelligence products, concerned with what has just happened or is happening now, dominate the flow of intelligence from the producers to the consumers. The amount of analysis required for these products is usually minimal and often consists of a comment on an item and a short-term forecast. They can easily be tailored to the needs of the day, and are disseminated in a timely fashion. More difficult to do are those assessments or estimates requiring a deeper and wider look at issues of national importance. They take longer to construct, coordinate and disseminate, and are more subject, because of their focus on the longer-term, to be proven wrong. While they can be tremendously useful for mid- to long-range policy planning exercises, many policy consumers have admitted over the years that they have no or little time to read them. Intelligence analysts also produce basic intelligence documents, which are generally concerned with large amount of verified data, such as the CIA's *World Factbook* and the *Chiefs of State and Cabinet Members of Foreign Governments*.[45] Having provided some markers on what intelligence analysis is, we will now examine what the intelligence analyst does.

What Is the Analyst's Job?

Intelligence analysts do not try to predict the future with any measure of accuracy; they simply cannot. Instead, they assign odds to different courses of action, such as the most dangerous, the most

[45] J. S. Nye, Jr., 'Peering into the Future,' *Foreign Affairs* 73:4 (1994) 82. See also Shulsky and Schmitt, *Silent Warfare*, 57-61.

likely and the least likely courses.[46] Their daily routine is one of searching 'for insights into the meaning of "raw" or unevaluated data.'[47] According to the US Director of Central Intelligence's 1999 Annual Report,

> all source analysts examine and interpret both the raw data from the intelligence disciplines of IMINT, HUMINT, SIGINT, and MASINT, as well as the expert commentary of both single source analysts and HUMINT collectors. Each all source analyst also develops a unique personal preferences for other valuable data sources. These may include industry and academic contacts, allied intelligence services, non-governmental agencies (NGOs), and counterintelligence data. The all-source analyst synthesizes all such data through the prism of their academic training, language skills, foreign travel, and personal experience.[48]

The analyst's mental/intellectual processes are his key assets since he is required to draw judgments of intelligence value to the policy consumers. To do so, an intelligence analyst must be highly proficient at synthesizing a wide body of literature and deriving meaning from it; classifying and integrating a disparate range of all-source information, comparing it with previously acquired information, and drawing conclusions. An analyst must be alert to analytical pitfalls and able to employ different analytical techniques (inductive, deductive, abductive, scenario-based, contingency-based, high-impact/low-probability, Team A-Team B, etc.). The analyst should also be prepared to

---

[46] Lowenthal, *Intelligence: From Secrets to Policy*, 88. The development of enemy possible courses of action is an important part of the US and Canadian military's 'intelligence preparation of the battlefield process. See US Army Field Manual 34-130/Fleet Marine Force Manual 3-20-1, *Intelligence Preparation of the Battlefield* (Washington, D.C.: Headquarters, Department of the Army, July 8, 1994); and *Land Force Information Operations: Field Manual Intelligence*, B-GL-357-001/FP-001 (Ottawa: Department of National Defence, Chief of Land Staff, January 30, 2001). See also J. J. Medby and R. W. Glenn, *Street Smart: Intelligence Preparation of the Battlefield for Urban Operations*, Report MR-1287-A (Santa Monica, CA: Rand Corporation, 2002).

[47] L. K. Johnson, 'A Framework for a Theory of Strategic Intelligence,' paper presented at the 43rd Annual Convention of the International Studies Association (New Orleans, LO: March 23-27, 2002) 12.

[48] *Director of Central Intelligence Annual Report for the United States Intelligence Community* (Washington, D.C. May 1999).

deliver intelligence in writing, verbally or graphically, and brief with very little warning.

To better understand what goes on in an analyst's mind, a cognitive model based upon a review of the applicable cognitive psychology literature, 117 detailed interviews, and field observations, was developed nearly 25 years ago for the Army Research Institute for the Behavioral and Social Sciences (ARI) and the US Army Intelligence and Security Command (INSCOM) by Operating Systems Inc. It is the most complete, empirically-grounded piece of research, along with Richards J. Heuer's *Psychology of Intelligence Analysis*, I have seen on this subject.

To devise a model that would cut across single-source and multi-source intelligence disciplines, the research team studied SIGINT and IMINT task processes that were judged (on the basis of five criteria—analytical orientation, generality, interpretive complexity and level of aggregation) to have 'high analytical and judgmental content,' so that the findings could be equally applicable to the multi-source analytical environment. One of the key conclusion of the study was that 'intelligence analysis is conceptually driven as opposed to data driven. What is critical is not just the data collected, but also what is added to those data in interpreting them via conceptual models in the analyst's store of knowledge.'[49]

The research team also developed a generic intelligence production model, which integrated resource management and adaptation functions, because both were judged to have an impact on the quality of the analysis and interpretation. With respect to resource management, this model recognizes that managers and analysts both have a say on the planning of the analytical work and its

[49] R. V. Katter, C. A. Montgomery and J. R. Thompson, 'Human Processes in Intelligence Analysis: Phase I Overview,' Research Report 1237 (Woodland Hills, CA: Operating Systems, Inc., December 1979) 1—10. A conceptual model was defined as 'a pattern of generalizations about a given category or range of experience, which depicts a relation or relations between two or more entities, where an *entity* may be an object, an individual, or an event.' Ibid, 2—2.

prioritization, as well as the allocation of resources to respond to consumer requirements. Time management is judged by this model to be a critical management issue affecting all analysts. While the latter may have different projects underway for different consumers, they are also expected to find sufficient time to maintain and enhance their skills and improve their knowledge base.

With respect to adaptation functions, the model indicates that 'both the organization and the analysts examine the quality of products and use whatever means are available to correct deficiencies.'[50] This would include analysts being self-critical about the appraisal of their performance and seeking feedback, and organizations reallocating resources and the re-assignment of analysts where there would be a better fit for their expertise and experience.

This relationship between analysts and their managers, noted in te previous section, was fully explored, discussed and dissected by former CIA intelligence analyst John A Gentry with respect to the CIA's Directorate of Intelligence (henceforth DI). Gentry, who focused on problems apparent to him within the DI from the early 1980s to the early 1990s, concluded that up to the 1980s, problems between analysts and managers were primarily due to personality clashes. From that time on, however, the problems between the two groups became rooted in practices and policies. The latter prescribed unity of review and management, which meant that senior supervisors could enforce the inclusion of their preferences in analyses. Consequently, many analysts tried to please their bosses by writing what they think their bosses would like to see and began to focus on quantity rather than quality of production, although lip service was paid to the latter. Because quality was judged by the immediate supervisors, it became a subjective exercise with a great impact on the future career of an analyst. Supervisors and senior managers, no longer experts in their areas of

[50] Katter, Montgomery and Thompson, 'Human Processes in Intelligence Analysis,' 3—2.

responsibility, in turn, fell prey to the politicization of intelligence by trying to fill the analysis to 'the perceived ideological, political or bureaucratic preferences of key consumers,' in the anticipation of kudos that would reflect well on them. Shallow analysis and packaging therefore became more important than sound analytical judgment. Supervisors and managers were no longer in their respective position to facilitate publication of the analysts' work as in the past. In the end, Gentry concludes, 'whatever their specifics, intelligence agencies develop institutional practises that affect their performance.'[51]

The key to the research team's general model, however, is interpretation, the core function of an analyst. This, they break down into three tasks: '(1) receiving incomplete or sparse data, (2) interpreting the data, and (3) formulating the intelligence product [...].' The data received is filtered (selected and evaluated) usually according to 'memory-stored conceptual models of the types of real-world objects or events thought to have generated the data being interpreted.'[52] From their observations of the analyses produced by intelligence analysts, the team noted 'that often a large proportion of the information in the products has been added from memory,' leading to its central conclusion that 'the interpretive process is often more concept-driven than data-driven.'[53] In other words, analysts never have a perfect information situation and 'information from memory provides

---

[51] J. A. Gentry, 'Intelligence Analyst/Manager Relations at CIA,' paper presented the Annual Conference of the Canadian Association for Security and Intelligence Studies (Ottawa, October 27-29, 1994); for a detailed explanation of his argument, see Gentry, *Lost Promise.* There are also empirically supported arguments that peer review is as 'unreliable [as an] indicator of a paper's quality, accuracy, or its integrity' than hierarchically-imposed review processes. See, inter alia, R. W. Hahn, 'Disclosing Conflicts of Interest: Some Personal Reflections,' Working Paper 02-2 (Washington, D.C.: AEI-Brookings Joint Center for Regulatory Studies, February 2002).

[52] Katter, Montgomery and Thompson, 'Human Processes in Intelligence Analysis,' 3—5.

[53] Katter, Montgomery and Thompson, 'Human Processes in Intelligence Analysis,' 3—9.

the sole basis for hypothesizing relationships among data available for interpretation and for classifying various date as relevant, redundant, present, absent, or crucial for the interpretive task.'[54] By 'added from memory,' the research team meant that each analyst has an internal memory comprising his acquired knowledge of events/situations, of the procedural intricacies of intelligence analysis (e.g., how to resolve problem-solving situations), of accepted judgmental and analytical criteria, of how to get additional information, and of collection assets' capabilities.[55]

The cognitive model therefore focuses on how an analyst processes information and interprets it. Three mechanisms are described by the research team: sensory information filtering (selectivity—'Which aspects of the raw sensory information pattern are significant?'—and generalization—'How much and what kind of similarities are required to recognize things as the same?'), memory contents consolidation and memory access interference. As the team explains, memory access interference is brought about by extended exposure to data inputs that are difficult to distinguish: 'Thus an analyst processing many messages of very similar contents from the same domain, under constant conditions and over an extended period of time, is unlikely to be able to

[54] Katter, Montgomery and Thompson, 'Human Processes in Intelligence Analysis,' 7—1. Recent psychological studies have reaffirmed the validity of this observation. D. Halpern notes, for example, that 'when a pattern of events triggers the need to understand what is happening, people retrieve an explanation in a highly automatic manner. The stored information is applied to the present situation without considering possible differences between the event we are trying to explain and those that led to the memory of the explanation.' Halpern, 'Sex, Lies, and Audiotapes,' in *Why Smart People Can Be So Stupid*, ed. by R. J. Steinberg (New Haven, CT: Yale University Press, 2002) 117.

[55] Katter, Montgomery and Thompson, 'Human Processes in Intelligence Analysis,' 5—3- 5—4. The team notes later that 'it is worth recalling that the cognitive model indicates that the individual is not free to choose what will be recalled in a given situation: memory access functions are mostly automatic and outside of awareness. What will emerge first from memory is what has been processed most frequently and deeply.' Ibid., 8—3.

recognize the specific messages processed during a certain period of time.'[56]

The problem of decision pressure was also well explained by the research team:

> Most centrally, the analyst must repeatedly decide when the point has been reached where the results of each analytic endeavor are sufficiently clear to warrant no further expenditure of analytic resources under the current conditions of resource availability. Situational variables that focus pressure on such decisions include: Amount of ambiguity and uncertainty in the date and in memory; Possible losses or penalties associated with a serious error of interpretation; Amount of error reduction possible if more data and analytic resources could be applied to the interpretation; Limitations on applying more analytic resources, including time, to the interpretation. Analytic situations involving great ambiguity, large possible penalties from error, great potential for error reduction with more processing, but severe limits on more processing can cause great decision pressure.[57]

Although worded very differently, this explanation of decision pressure closely matches the findings of the Joint Inquiry Staff with respect to 9/11 analytic deficiencies.

If we accept the cognitive model developed by Operating Systems, Inc. as valid, then it becomes clear why analysts must be trained and encouraged to develop the necessary skills to think critically and innovatively. Objectivity is, as Michael Herman argues, an 'elusive ideal.'[58] This is important if intelligence analysts are to produce estimates that are as unbiased and free of logical fallacies as possible. To wit,

> If anything should be taken for granted it is the centrality of critical reflection, or boundary exploration and critique, to all forms of analysis. It is perhaps a poor reflection on the current analytical culture that critical thinking as an activity has to

---

[56] Katter, Montgomery and Thompson, 'Human Processes in Intelligence Analysis,' 6—7.

[57] Katter, Montgomery and Thompson, 'Human Processes in Intelligence Analysis,' 7—3.

[58] M. Herman, '11 September: Legitimizing Intelligence?' paper presented at the 43rd Annual Convention of the International Studies Association (New Orleans, LO: March 23-27, 2002) 5.

be made explicit.[59]

Critical thinking is particularly important, as analysts use human source testimony to determine the intentions and plans of an adversary. The intelligence analyst must decide into which of mathematician Pierre Simon Laplace's four categories his testimonial evidence falls into: '(1) the witness does not deceive and is not mistaken, (2) the witness does not deceive and is in fact mistaken, (3) the witness does deceive and is not mistaken, and (4) the witness does deceive and is in fact mistaken[60].' When the testimony is 'incomplete, inconclusive, and lacks credibility to some degree,'[61] it must be corroborated or graded (in terms of its force or weight). To be of any use, it must have credibility, probative force, and be relevant to the requirement at hand, bearing in mind that experience and intuition may have a role to play.[62]

Just as intelligence analysts must be conversant with the social sciences methodologies applicable to their areas of responsibility, I contend that they and their supervisers/managers must also be able to easily recognize and deal with one-sided arguments (organizational, personal and

---

[59] K. A. Richardson, P. Cilliers and M. Lissack, 'Complexity Science: A "Grey" Science for the "Stuff in Between",' paper presented at the *1st International Conference on Systems Thinking in Management*, Proceedings (2000) 536.

[60] Hunt and Schum, 'Probabilistic Reasoning Using Incomplete and Singular or Unique Evidence.'

[61] Hunt and Schum, 'Probabilistic Reasoning Using Incomplete and Singular or Unique Evidence.'

[62] Hunt and Schum, 'Probabilistic Reasoning Using Incomplete and Singular or Unique Evidence.'

cognitive biases),[63] intuitive principles,[64] and fallacies of omission and assumption (oversimplification, hasty generalizations, fallacies of composition and division, special pleading, post-hoc, false dilemma, begging the question, hypotheses contrary to fact, misused analogies, and *ad hominem* attacks).[65] They must also understand the distinctions between facts, opinions, and inferences,[66]. Where and when applicable, they must avoid linear thinking and think abductively, rather than inductively or deductively. Abduction requires that we integrate our own thoughts and intuitions into our reasoning. Philosopher Charles Saunders defines abduction as an instinct for guessing right. If so, David Schum argues, 'new ideas emerge as we combine, marshal or organize thoughts and evidence in different ways.'[67] Complex systems theory is often argued an excellent abductive approach because of its 'emphasis on pattern recognition and its general openness-of-mind

---

[63] '[W]hile we may not be able to avoid bias in argumentation, there seems to be a consensus of opinion in modern textbooks that one of the most important skills of critical thinking is the ability to recognize bias in argumentation and to be able to deal in a critical manner with cases where bias is a problem.' D. Walton, *One-Sided Arguments: A Dialectical Analysis of Bias* (Albany, NY: State University of New York Press, 1999) xvii.

[64] See Jonathan Baron, *Judgment Misguided: Intuition and Error in Public Decision Making* (New York, NY: Oxford University Press, 1998).

[65] See, inter alia, A. Thomson, *Critical Reasoning: A Practical Introduction*, 2nd Edition (London: Routledge, 2002); T. Bowell and G. Kemp, *Critical Thinking: A Concise Guide* (London: Routledge: 2002); B. S. Thornton, *Plagues of the Mind: The New Epidemic of False Knowledge* (Wilmington, DE: ISI Books, 1999); and Jonathan Baron, *Thinking and Deciding*, 3rd Edition (Cambridge: Cambridge University Press, 2000).

[66] A fact is a statement that has been demonstrated to be true; an opinion is what someones believes to be true; and inferences are conclusions drawn by logic from facts, opinions, or other inferences. Army Field Manual 34-3, *Intelligence Analysis: Initial Draft* (Fort Huachuca, AZ: US Army Intelligence Center and Fort Huachuca, January 2000) 3—6-3—7. The key text is D. A. Schum, *Evidence and Inference for the Intelligence Analyst*, 2 volumes (Lanham, MD: University Press of America, 1987).

[67] C. W. Hunt and D. A. Schum, 'Probabilistic Reasoning Using Incomplete and Singular or Unique Evidence: Complexity-Based Reasoning Innovation for Commanders,' paper presented at the 1999 Command & Control Research and Technology Symposium (United States Naval War College, Rhode Island, June 30, 1999), Internet version.

when it comes to what variables and/or parameters might be relevant].'[68] As Ilachinski explains,

> complex systems theory persuades an analyst, in general, not to discard information solely on the basis of that information not conforming to a 'conventional wisdom' model of an adversary's pattern of activity. Instead, [...] complex systems theory teaches us to recognize the fact that apparently irrelevant pieces of information may contain vital clues as to an adversary's real intentions.[69]

To remain effective over a long period of time and minimize the effect of clientelism,[70] intelligence analysts should be expected to continually strive to increase their knowledge, through such means as getting on the ground, close to their subject,[71] and improve their analytical skills through graduate education, professional courses, participation at conferences, and interactions with colleagues in government and the academic sector. Ideally, an analyst should demonstrate every so often that he has taken adequate steps to stay abreast of his field of expertise, and honed his ability to think critically and innovatively before being considered for promotion. Intelligence analysts and managers should be cognizant, in this context, that one's current performance is not necessarily indicative of long-term potential. Intellectual flexibility – which is to say, our ability to learn, incorporate and recognize different conceptual models – is not fixed. Through training and practice, our intellectual flexibility can flourish. Left unchallenged, it can simply atrophy. True expertise,

---

[68] Ilachinski, *Land Warfare and Complexity, Part II*, 59.

[69] Ilachinski, *Land Warfare and Complexity, Part II*, 59.

[70] 'Clientelism is a flaw that occurs when analysts become so imbued with their subjects – usually after they have been working on an issue for too long – that they lose their ability to view issues with the necessary criticality.' Lowenthal, *Intelligence: From Secrets to Policy*, 81.

[71] As Lowenthal observes, 'Their distance from the subjects they analyze can occasionally be costly to analysts, in terms of how their policy consumers may have more "in-country" experience and direct contact with foreign leaders than do the intelligence analysts.' Lowenthal, *Intelligence: From Secrets to Policy*, 82.

therefore, can only be developed through sustained motivation, and intense effort at self and directed development over a decade or longer.[72]

Should Terrorism Be Analyzed Differently?

Michael Herman does not see a fundamental difference between foreign intelligence analysis and security intelligence analysis. He says: 'Security intelligence is slightly different; those who seek to detect espionage and terrorism are rather more like detectives than the journalists or researchers who produce accounts of situations and subjects. But the techniques of analysis are similar everywhere.'[73]

It must be acknowledged, however, that contrary to political, economic or social analysis, gathering and analysing intelligence on terrorists and their organizations is inherently more difficult. As Jeffrey Isaacson and Kevin M. O'Connell explain:

> Analyzing terrorism is not like analyzing Russian naval strength or Latin American political systems; such analyses rely upon well-defined indicators and data sources. In contrast, counterrorism analysis must provide structure to information that can be highly fragmentary, lacking in well-defined links, and fraught with deception. It must infer specific strategies and plans from small pieces of information. It must find common threads among seemingly disparate strands. And unlike the terrorist, who needs only a single vulnerability to exploit, the analyst must consider all potential vulnerabilities.[74]

Terrorists can hide easily, attempt to deceive at every opportunity, and their inner circle is

---

[72] See the various contributions by psychologists to Steinberg, ed., *Why Smart People Can Be So Stupid*.

[73] M. Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996) 101.

[74] J. A. Isaacson and K. M. O'Connell, 'Beyond Sharing Intelligence, We Must Generate Knowledge,' *Rand Review* 26:2 (Summer 2002) 49.

very hard to infiltrate. Analysts who are unfamiliar with the language and culture of the terrorists for whom they must assess the intent and capabilities therefore face a higher degree of uncertainty and information scarcity. Since it takes a long time to develop the required expertise, there is a somewhat compelling argument to develop one in most if not all areas of the world, in case future unforeseen contingencies eventually require it.[75] The need is for intelligence analysts who can extract '"meaning" from incomplete evidence [observed, reported facts/activities], using knowledge, experience, expertise and insight to compensate for absent evidence and ever-present ambiguity.'[76] A difficult task indeed, but one which counterterrorism analysts are reported to have performed well overall at the strategic level.[77] The problem, of course, has to do with the exact who, where, when and how a terrorist attack will materialize. No amount of expertise can supply that information. However, should it be supplied, trained and experienced analysts will need to be in place and

[75] While the argument to develop expertise for yet unforeseen contingencies has some currency in a country as large and resourceful as the United States, it is doubtful that other countries' intelligence communities would take a similar approach. It is more likely that they will favor expertise in some key areas while covering everything else with generalists with good analytical skills, but no long-term expertise in any specific area. An interesting explanation for this approach with respect to foreign ministries was developed by J. W. Moses and T. Knutsen: 'First, we can expect an increase in the pace and scope of international events affecting nations. The shrinking importance of time and space means that it will be increasingly difficult for states to prioritize certain areas, at the expense of others. Far-away flashpoints (e.g., the Maldives, East Timor, Sudan) can require immediate action; rapid technical, social, political and economic developments make it more difficult to focus and institutionalize issue-area expertise. States that sink their human and economic investments into specific areas of permanent expertise can risk bankruptcy in a rapidly changing global environment. The quicksilver-like liquidity (or flexibility) of human and intellectual capital is the new name of the game. Thus, we should expect states in a global context to rely less on permanent area-study specialists; area expertise might be sub-contracted on a need-to-know basis. With the possible exception of just a few large states, it does not make sense to maintain encompassing area-specialist teams: "relevant" areas of the world are increasingly difficult to define.' Moses and Knutsen, 'Globalization and the Reorganization of Foreign Affairs' Ministries,' *Discussion Papers in Diplomacy* (Netherlands Institute of International Relations 'Clingendael', n.d.) 14.

[76] Jacoby, 'Information Sharing of Terrorism-Related Data,' 3.

[77] According to P. Pillar, 'Fighting International Terrorism: Beyond September 11th,' *Defense Intelligence Journal* 11:1 (2002) 19.

linguists and collection assets available to capitalize on the intelligence.

Potentially useful to intelligence analysts looking at terrorism is the paper of Ted Robert Gurr on 'Methodologies and Data for the Analysis of Oppositional Terrorism,'[78] in which he lays out a framework to start making sense of the threat. He divided his framework into five levels (global, national, group, incident, and individual), each raising its own set of research questions and methods. At the global level, Gurr looks at trends (in terms of time, space, and tactics), diffusion processes, and terrorism as an outgrowth of interstate conflict, and suggests that trend analysis graphically presented is an adequate methodology. At the national level, he examines where terrorism is more prevalent, the trends and diffusion patterns of terrorist activities, national policies to fight terrorism, the political context giving rise to terrorism, and the effects of terrorist campaigns. The main objective at this level of analysis is to identify causes of terrorism. At the terrorist group level, Gurr is interested in looking at their socioeconomic origins, ideologies, organization, international linkages, and their rise and decline. At the incident analysis level, he suggests studies of the vulnerability of targets, incident outcomes, negotiation strategies, and the effect of the media. Finally, at the individual level of analysis, he pays attention to recruitment and training, motivations, and the impact of terrorist actions on hostages. What Gurr offers is a strategic analysis approach to the study of terrorism that would help analysts situate the problem in its various contexts and dimensions. While it may not provide answers to tactical questions of the what, where, who, when, and how type, Gurr's framework should focus one's analytical work, reduce the information gap, and provide sufficient value-added to assist policy planners in their task of finding solutions to terrorism.

---

[78] T. R. Gurr, 'Methodologies and Data for the Analysis of Oppositional Terrorism,' paper prepared for the Symposium on International Terrorism (Washington, D.C.: Defense Intelligence College, December 2-3, 1985).

Since Gurr presented his paper in 1985, the US Defense Intelligence College has put together a Terrorist Intelligence Analysis Course package, which includes sections on pre-incident indicators, database design and development, analytical tools, time event charting, and case studies. This is an excellent tool for any intelligence analyst on his initial assignment to a counterterrorism desk.[79]

How Do Intelligence Analysts Deal With Uncertainty?[80]

Analysts face uncertainty every time they attempt to project current trends into the future or determine the likelihood of a particular event or chain of events. This is particularly acute when looking at terrorism. We talk of uncertainty because of information gaps, possible deception, and the unique character of contexts. If they were not unique,

> then past experience would always be sufficient when confronting any situation. This uniqueness means that attempts to associate existing understanding with particular contexts is problematic. This would imply that the recognition of contexts is a black and white exercise.[81]

In other words, the analysis of past events and outcomes cannot apply in cases which are unique or happen only rarely. In such cases, 'there may be no accumulations of past outcomes to

---

[79] The course package is available on the Internet at http://www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm

[80] '"But where would we be if we could speak only of things we know with certainty?" asked the sixteenth-century French historian Henri Voisin de La Popelinière.' Quoted by Lukacs, *At the End of an Age*, 56.

[81] Richardson, Cilliers and Lissack, 'Complexity Science,' 537.

analyze.'[82]In addition to the mental models they have developed, analysts also rely on theoretical frameworks learned in graduate schools to deal with uncertainty. A word of caution, however, is in order when using such frameworks:

> [...] we must accept that frameworks are essential in providing at least a focus or starting point to analysis. What we must be strongly aware of is that the theoretical insights offered by any framework should not be used to *determine* our explorations, but considered as an offering of *direction*, or simply as a source of creativity to fuel the exploration process.[83]

Within the US intelligence community, intelligence analysts build their judgments following five key standards:

- quantify the certainty level of its key judgments by using percentages or "betters' odds," where feasible, and avoid overstating the certainty of judgments;
- identify explicitly its assumptions and judgments;
- develop and explore "alternative futures:" less likely (but not impossible) scenarios that would dramatically change the estimate if they occurred;
- allow dissenting views on predictions or interpretations; and
- note explicitly what the IC [intelligence community] does not know when the information gaps could have significant consequences for the issues under consideration.[84]

These principles applied, a policy consumer has a better appreciation of what exactly is at stake and clear parameters to better understand the value of the analysis.

One assumption that has been attracting interest outside the intelligence community for the last couple of years is referred to as the precautionary principle. This principle essentially states that

---

[82] Hunt and Schum, 'Probabilistic Reasoning Using Incomplete and Singular or Unique Evidence,' Internet version.

[83] Richardson, Cilliers and Lissack, 'Complexity Science,' 536.

[84] US General Accounting Office, *Foreign Missile Threats: Analytic Soundness of Certain National Intelligence Estimates*, Report to the Chairman, Committe on National Security, House of Representatives, GAO/NSIAD-96-225 (Washington, D.C.: August 1996) 2. See also Nye, 'Peering into the Future,' 82-93.

'when an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically.'[85] The principle is gaining prominence in several European countries where it is inscribed in legal statutes. Over the last two years it has also made giant strides in the world of politics. It is indeed easy to use this principle within different contexts. For example, it theoretically would allow a country such as the United States to preempt any attacks against it— even if there are no cause to effect relationships in the intentions and capabilities of an identified threat—by taking offensive actions first. The implications stemming from the application of the precautionary principle are evidently serious in such a context. Knowing where the political wind blows, analysts who want to avoid being fingered for a potentially costly mistake may be tempted not to try to fully resolve the inherent uncertainty attached to their analysis and rely on the precautionary principle to draw their judgments.

Another way to deal with uncertainty and equivocal data is to compare one's analysis and judgments with the same work done by a different analyst, ideally someone with a different background and viewpoint. This is called disparity analysis.[86] The evaluation of the two interpretations would lead to necessary adjustments or reinforce the positions initially taken. In the same line of thought, community-wide assessments could be useful in identifying gaps, errors, and disagreements. However, they have severely criticized because they are usually 'time-consuming exercises in compromise, resulting in watered-down judgments and overly long documents lacking

[85] D. Appell, 'The New Uncertainty Principle,' *Scientific American*, 284:1 (January 2001) 18.

[86] Katter, Montgomery and Thompson, 'Human Processes in Intelligence Analysis,' 7—5- 7—6.

both timeliness and relevance.'[87]

There are several other assumptions, methods, and models to deal with uncertainty. The point I would like to get across is that no matter what tool or set of assumptions an analyst chooses to build solid judgments, it must be transparent to the policy consumer. If it is not, the latter may make a decision leading to disastrous consequences because he misunderstood or misinterpreted what he read. Uncertainty will always be a key feature of intelligence, but it can be reduced with the use of logic, relevant methodologies, analytic techniques, and better collection.

Is Technology an Analytical Enabler?

It has been argued often that 'intelligence hardware is high-tech and glamorous, but is ultimately less important than the ability of trained analysts to interpret intelligently what they are seeing.'[88] While true, there is no denying that technology is an enabler and that analysts must be technologically proficient and able to muster the resources offered by databases and data management software.

More specifically, analysts access intelligence by pushing, pulling or observing. In the 'push' dimension, the analyst receives intelligence without asking for it. This intelligence takes two forms: non-record traffic products (e.g., e-mail) which the analyst could use to populate or add to a database, or official records being added to a databases by data analysts and forwarded to the analyst as a matter of interest or pre-established requirements. In the 'pull' dimension, analysts retrieve what they need from secure web pages or established databases. If analysts work in a 'pull' dimension

---

[87] Hedley, 'Checklist for the Future of Intelligence,' Internet version.

[88] K. Schake, 'Constructive Duplication: Reducing EU reliance on US military assets,' *Working Paper* (London: Centre for European Reform, January 2002) 21.

only, they have no choice but to search for what they need, otherwise they would not know what is available to them. Although working in this sole dimension would appear to be rather exceptional, it has been noted that more and more intelligence organizations only post their information and no longer 'manually' distribute it to lists of selected addressees. The third dimension, 'observe,' is more akin to the military and involves near-real time displays such as that provided by IMINT, HUMINT and other collection assets.[89]

Intelligence analysts must master information retrieval and access techniques if only because the flow of intelligence reporting is now too large to handle without technical assistance. According to statistician Leo Breiman, the amount of data stored electronically follows Moore's Law and, like CPU power, doubles every 18 months.[90] At a military tactical level, intelligence analysts may receive over 17,000 reports per hour from sensors alone.[91] So much data, however, is useless, unless what is valuable can be identified and retrieved.

The intelligence collected by the single-source intelligence disciplines is stored in databases. Most modern, computerized intelligence agencies have millions of documents in their databases. To be useful, these databases must be able to accommodate refined searches which would answer very specific requirements (for instance, what intelligence is available on terrorist organizations in Norway?). To do so and avoid potentially costly mistakes, these databases require algorithms that

---

[89] See LTC S. K. Iwicki, 'Synchronized Chaos: Visualization, Integration, and Dynamic Thinking,' *Military Intelligence Professional Bulletin*, 29:1 (January-March 2003) 5-6.

[90] L. Braiman, 'Data Avalanches, Smart Algorithms, Human Intelligence,' talk on data mining delivered to the Rand Graduate School (2002), Internet version.

[91] Iwicki, 'Synchronized Chaos,' 7.

are fast and accurate.[92] There are also speech recognition programs available to assist analysts, but these have on average a 5 percent error rate, a margin that has not improved over the last 15 years.[93] Although these tools can save the analysts an incredible amount of search time and organize a wide range of data for them, they are not a substitute for human intelligence. As Braiman explains:

> Smart algorithms are a tool for human intelligence – not a replacement. Their function is to reduce the human burden of extracting information from large data bases. Humans are the best class recognisers in existence. Their ability seems built into the brain. It's usually difficult to construct an algorith that will do nearly as well.[94]

To assist the manipulation of large amounts of disparate data by terrorism analysts, the Defense Advanced Research Projects Agency's (DARPA) Information Awareness Office manages the development of several programs which would 'analyze and extract data, allow the identification of individuals by their characteristic body movements, or automatically translate Arab, Persian and other languages into English.'[95] One of the IAO's key programs, Total Information Awareness (TIA), has raised privacy concerns because of its perceived potential to bring together all manner of private and public information on every American citizen (such as passport and visa applications, driver's license information, airline-ticket and firearms purchases, arrest records, etc). According to the government, TIA is 'an experimental prototype in the works that will determine the feasibility of

---

[92] Braiman, 'Data Avalanches, Smart Algorithms, Human Intelligence,' Internet version.

[93] Braiman, 'Data Avalanches, Smart Algorithms, Human Intelligence,' Internet version.

[94] Braiman, 'Data Avalanches, Smart Algorithms, Human Intelligence,' Internet version.

[95] A. Mayle and A. Knott, 'Outsourcing Big Brother: Office of Total Information Awareness Relies on Private Sector to Track Americans,' Special Report of the Center for Public Integrity (Washington, D.C.: December 17, 2002), Internet version.

searching vast quantities of data to determine links and patterns indicating terrorist activity.'[96]

Another DARPA program of potential to intelligence analysts is the Evidence Extraction and Link Discovery (EELD) software. It would assist in the analysis of 'the more than ten thousand messages a day that intelligence analysts receive from classified and non-classified sources' by extracting 'relevant data and relationships about people, organizations, and activities from message traffic and open source data.' Another related project, Genoa, would allow for the rapid location and grouping of 'relevant information from a wide assortment of classified and open multimedia data sources (e.g. real-time commercial video source (CNN) and geographic (map) information.).'[97] Genoa is currently being tested by government agencies.[98]

All these DARPA programs would be useful to the analysis of 'pre-incident behavior and activity.' As DIA Acting Director Jacoby explains:

> There are scores - in some cases hundreds - of discrete steps taken by terrorists as they choose, plan, and move in on a target. For the most part, each step, when observed in isolation, may appear to be everyday, routine activity. For example, the purchase or forgery of travel documents, "accidental" intrusions in secure areas, or movement of cash may have innocent explanations and benign implications. But maybe not. [...] We need to do a much better job of incorporating this type of information into our analytic equation. While ninety-nine percent of it will likely turn out to be "noise," we cannot afford to miss the one percent that is not.[99]

---

[96] J. Michael Waller, 'Fears Mount Over "Total" Spy System,' *Insight Magazine* (December 24, 2002).

[97] H. Stephens, 'DARPA Developing a Range of Technologies to Counter "Asymmetric Threat",' *Defense Information and Electronics Report* (September 21, 2001) 1.

[98] R. Scarborough, 'Pentagon Delivers Software to Assess Data on Terrorists,' *Washington Times* (December 18, 2002) 3.

[99] Rear Adm. L. E. Jacoby, US Navy. 'DIA Response to Jont 9/11 Letter of Invitation,' Statement for the Record before the Joint Intelligence Committee of the U.S. Senate and U.S. House of Representatives investigating the events leading to the attacks of September 11, 2001, Public Hearing (Washington, D.C.: October 17, 2002) 4.

Senator Richard C. Shelby also sees the potential TIA has for all-source analysis. He explains:

> TIA aspires to create 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. 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.[100]

Current and future technological developments will assist the work of the intelligence analysts in so many new ways. Technologies act as enablers and should be embraced by analysts when they simplify their life and allow then to retrieve and manipulate information in a timely effortless manner.

Who Is the Analyst?

A lot of emphasis is publicly placed on the necessity for intelligence analysts to be highly educated, multilingual, and possessing relevant experience (through employment or foreign travel). Jobs

---

[100] R. C. Shelby, *September 11 and the Imperative of Reform in the U.S. Intelligence Community*, Additional Views to the Joint Inquiry Staff's Final Report (Washington, D.C.: December 10, 2002) 41.

advertisement posted by the CIA often ask for individuals with graduate degrees and relevant languages. It also happens that a number of intelligence analysts exceed these requirements. Yet, complaints are routinely heard that the best and brightest do not necessarily join intelligence agencies, that there is a lack of talent throughout the community, etc. Congressmen noted two weeks after 9/11 that there was still a tendency within the community to develop intelligence generalists rather than intelligence professionals (i.e., experts). These intelligence generalists are assigned and reassigned at will, according to current priorities.[101] This reportedly holds true for both civilian and military intelligence analysts. In the military, the standard three-year assignment rotation system is not enough for military intelligence analysts to become experts in any given subject. Analyst Jeffrey White noted that in 'every crisis, it always comes down to a few recognized experts providing the core knowledge to decision makers. The generalists do general things, and the experts provide what decision makers and war fighters need.'[102]

Ex-US Army intelligence officer Ralph Peters has long argued that good analysts are born that way. He also offers interesting suggestions about how to groom the best analysts:

> Intelligence analysis, done well, requires not only rigorous training and much practical experience, but innate talent, a predisposition. [...] Yet, we assume that anyone with a moderately high IQ can be trained in a few months to grasp an enemy's mentality, character, fears, intentions, hopes, beliefs, vulnerabilities, and individuality– without even speaking his language.
> But we need to try to understand that a good analyst's mind is wired a bit differently – he or she need not go into a trance and speak in tongues but had better have a richer, cannier vision of the world than that possessed by the average Washingtonian

---

[101] US Congress. *Intelligence Authorization Act for Fiscal Year 2002*, House Report 107-219, Washington, D.C.: 107th Congress, 1st Session, September 26, 2001, p. 19.

[102] J. B. White, *Some Thoughts on Irregular Warfare*, NWC 3060 reprint, in *Studies in Intelligence* 39:5 (1996) 58, quoted by Jean MacIntyre, *Operational Intelligence in a Changing World* (Newport, RI: Naval War College, Joint Military Operations Department, February 5, 2001) 18.

> bureaucrat. [...] But good analysts – the truly good ones – are rare and, sometimes, irreplaceable.
> Talented people are difficult, from start to finish. They require special care and feeding - not consistently, but often unexpectedly. Brilliant analysts may be a chronic annoyance in the otherwise collegial staff meeting; they're often priggishly self-righteous and sometimes obsessive [...]. analysts need to be valued, with the most talented identified, protected, and groomed. [...] have to be rewarded.[103]

The literature on intelligence has several anecdotal references to intelligence analysts. The majority of them are somehow similar to Peter's in that the truly dedicated and best analysts are described as peculiar, even weird, but very efficient in their own way. To find, hire, and retain the best analysts is a full-time, continuous task. You simply never have enough of them. Once they are in, however, it is important that they be given opportunities to grow further as individuals and analysts. In this regard, the opening in the United States on May 4, 2000 of the CIA's Sherman Kent School for Intelligence Analysis and in 2002 of the FBI's College of Analytical Studies (CAS) are two very positive developments. The Kent School offers four programs: a 26-week analysis course for new analysts, a managing and teaching analysis program, a seminar series for intelligence managers, and an academic outreach and intelligence analysis studies program.[104] The CAS provides 'training for all FBI analytical support personnel' and 'is intended to become a featured component of training at the FBI Academy, along with New Agents Training and the FBI National Academy.'[105]

---

[103] Peters, *Beyond Terror*, 194-195, 199, 205-206.

[104] 'Tenet Dedicates New School for Intelligence Analysis,' Press Release (Washington, D.C.: Central Intelligence Agency, May 4, 2000). See also S. Marrin, 'CIA's Kent School: A Step in the Right Direction,' paper presented at the 43rd Annual Convention of the International Studies Association (New Orleans, LO: March 23-27, 2002).

[105] R. S. Mueller, III. Testimony of the Director, Federal Bureau of Investigation, before the Joint Intelligence Committee of the U.S. Senate and U.S. House of Representatives investigating the events leading to the attacks of September 11, 2001, Public Hearing (Washington, D.C.: October 17, 2002) 8.

Could Intelligence Analysis Be Improved?

This paper was not intended to be an assessment of the analytic performance of the US intelligence community. However, given the United States-centric nature of the literature in this field and that country's professionalization of its intelligence analysts, references to the US intelligence community cannot be avoided. The discussion, however, should be no less relevant to smaller intelligence communities that also face significant analytic challenges.

While intelligence analysis as a discipline with its own methodologies, concepts and principles is slowly evolving, there are perhaps a few steps that could be implemented to enhance the quality of analysis.

Network the Analysts

If one agrees with the notion that 'good intelligence, comes from a team effort,'[106] then one would also agree with increasing interactions between intelligence analysts, other government officials and outside experts in academia or the private sector. This would alleviate the isolation sometimes felt by analysts who also 'tend to be marginalized in policy and public debate.'[107] Better networking between analysts involves breaking down 'hierarchies and stovepipes' that 'restrict the flow of information, impede interaction among intelligence specialists, and inhibit exchanges between the intelligence community and the outside world.'[108] While the benefits are tangible, caution should be

[106] Argued by A. Campbell, former Executive Director of the Intelligence Assessment Secretariat in Canada's Privy Council Office, and J. Gannon, former CIA deputy director. D. Jacobs, 'Security Analysts Issue Wake-Up Call,' *Ottawa Citizen* (October 4, 2001).

[107] A. Campbell quoted by Jacobs, 'Security Analysts Issue Wake-Up Call.'

[108] Berkowitz, 'Better Ways to Fix U.S. Intelligence,' Internet version.

excercised. Networking can mean many things and may not always be beneficial. For example, a strict network may not be to anyone's taste and actually counterproductive. Too loose a network and security flags would be raised as sensitive intelligence will be perceived to be flowing between analysts outside authorized and supervised channels. This is something applicable to all countries and assuredly worth developing further.

Give Ownership of the Information to Analysts

Admiral Jacoby suggested to the Joint Inquiry that 'ownership of information belonged with the analysts and not the collectors.'[109] This is a bold proposal to intelligence agencies where the situation is the other way around. Its implementation would require changes in mentalities and in ways of doing things. The advantage is that analysts would no longer be prevented from accessing and using intelligence vital to their project. This is a proposal, though, that needs further refinement, perhaps through a comparison of services from different countries with different intelligence ownership systems.

Involve the Analysts More

Jennifer Sims suggests that intelligence analysts personally brief the result of their assessments to policy consumers. This will balance the iterative production process with more individualistic work and give analysts 'greater exposure to policymakers' requirements, while helping the latter to

[109] Jacoby, 'Information Sharing of Terrorism-Related Data,' 6.

develop contacts in the Intelligence Community.'[110] Bruce Berkowitz also argues for more direct contacts between analysts and consumers. Such contacts, he added, should not automatically imply that analysts would loose their objectivity.[111] However, by getting closer to the policy consumers, analysts will have to be careful not to adopt their 'mind-sets and misperceptions.'[112] To be of use, intelligence must be made available to policy consumers, who in turn must be convinced that there is something that will help them. The proposal thus has merit. It needs, however, to be accompanied by greater detail. How much time, for instance, should an analyst spend on the road and away to do this? What would be reasonable?

Empower the Analyst

Bruce Berkowitz has argued that analysts should speak for themselves. Rather than focusing on internal coordination, quality assurance should instead be placed on hiring and promotions, not on products. In other words, 'instead of trying to guarantee that each product is perfect, they [intelligence agencies] should ensure that any analyst in the intelligence community has met certain standards and can speak as an authority. Peer review, especially on matters that depend on judgment more than fact, is much overrated.'[113] Berkowitz speaks from personal experience. I cannot disagree

---

[110] Sims in *What Is Intelligence?*, 15. Amb. R. D. Blackwill went even farther by suggesting to: 'Place the best and most promising analysts on tours in the policy world. [...] Intelligence officers can learn something about how to use intelligence resources effectively by reading about policymaking. You can learn some more by periodic visits to a policymaker's office. Blackwill, in response to a question from Jack Davis in 'Insightful Interviews: A Policymaker's Perspective On Intelligence Analysis,' *Studies in Intelligence* 38:5 (1995) 14.

[111] Berkowitz, 'Better Ways to Fix U.S. Intelligence,' Internet version.

[112] Herman, *Intelligence Power in Peace and War*, 110.

[113] Berkowitz, 'Better Ways to Fix U.S. Intelligence,' Internet version.

with this approach.

Have Your Analysts Travel to Gain First-Hand Knowledge

Arthur Hulnick argued that 'analysts have to spend a fair part of their formative years in the area in which they are supposed to be expert.'[114] Bureaucratic hurdles (costs, vacancies, career progression, etc) does not make this a very attractive proposal to most managers. If considered essential to develop the required expertise (and I think it is in many respects), the implementation of a program similar to the US Army's Foreign Area Officer (FAO) could be an attractive option. FAOs are trained in a foreign language, sent to complete a graduate degree in area studies and international relations, and given in-country training opportunities, 'which are essentially internships to permit the officer to learn about his assigned region through service abroad in a US embassy or military group.'[115] While very attractive, it is unrealistic to expect such a program to accommodate large numbers of intelligence analysts. However, this idea deserves further exploration.

This paper touches on only a few of the many proposals floating around to improve the analytic performance of the intelligence community. Intelligence analysis is a vibrant, multifaceted discipline that has received a surprisingly scant share of academic attention. Given its critical role in national security, a role highlighted in the Joint Inquiry Staff's Final Report, this is an element of intelligence studies that merit further study.

* * * * * * * * *

[114] Hulnick, *Fixing the Spy Machine*, 60.

[115] CPT J. B. King, "Foreign Area Officers and Special Forces: Synergy in Combined Peacekeeping Operations," *News from the Front* (September-October 1998).