Balancing Spending Between Spies, Satellites and Schoolboys

By Arnold E. Donahue

INTRODUCTION

In John Le Carre's wonderful post-Cold War novel - *The Secret Pilgrim*, Smiley addresses the spymaster's latest class of recruits. The recruits are questioning the entire purpose of Smiley's life's work of spying and intelligence.

> *"Nine times out of ten a good journalist can tell quite as much about a situation as the spies can. Very often they're sharing the same sources anyway. So why not scrap the spies and subsidize the newspapers? It's a point that should be answered in these changing times. Why not?"*

Smiley responds:

> *"It is perfectly true that most of our work is either useless, or duplicated by overt sources. The trouble is, that the spies aren't there to enlighten the public, but governments. ... And governments, like everyone else, trust what they pay for, and are suspicious of what they don't. ... Spying is eternal," he announced simply. "If governments could do without it, they never would. They adore it. If the day ever comes when there are no enemies left in the world, governments will invent them for us, so don't worry. Besides - who says we only spy on enemies? All history teaches that today's allies are tomorrow's rivals. ... For as long as rogues become leaders, we shall spy. For as long as there are bullies and liars and madmen in the world, we shall spy. For as long as nations compete, and politicians deceive, and tyrants launch conquests, and consumers need resources, and the homeless look for land, and the hungry for food, and the rich for excess, your chosen profession is perfectly secure, I can assure you.."*

84

Smiley's words are relevant to the topic of my talk today; and they are most pertinent in these closing days of the 20th Century. World military expenditures, reflecting the disappearing threat of a global conflagration and the diminishing prospects of serious regional conflicts, are estimated to have declined by about 50 percent from their Cold War high. In the United States, the recent Quadrennial Review of our Defense strategy and programs struggled mightily to buttress the case for forces and capabilities necessary to conduct two major regional contingencies. They ended up acknowledging that the real threat was of much lesser conflicts - inter-racial or ethnic strife, terrorism, international peacekeeping, complex humanitarian assistance operations - that is, in operations other than war. It is hard to justify carriers, bombers, and tanks for these operations other than war, but a grand leap of faith by military strategists somehow manages to justify the current force as just right for these non-war missions.

Sizing Intelligence in the US and the World

Lest we go too far afield into the 21st Century's evolving military questions, let us reflect on what is happening in US intelligence. CIA, for the first time, in 1997 announced that the United States spends $26.6 billion on foreign intelligence. Let me repeat that - $26.6 billion! Let's reflect on what that means for a moment:

$26.6 billion is about 10 percent of the United States' defense budget and more than what almost all countries spend on their entire military. There are a handful of countries that are exceptions. In total military spending, only Russia, France, Germany, the UK, and Japan exceed that number, such that what the US spends on intelligence equates roughly to what most of these nations spend on their total defense establishment.

Comparisons with what other countries spend on intelligence are impossible because, unfortunately, most other countries do not acknowledge what they spend on intelligence. One could hazard a guess, however, that few, if any, can afford to devote anything like 10 percent of their military budgets to intelligence. So if there is a comparison to the United States, I would hazard a guess that it is more like 3 to 5 percent of their budgets; no more than $2-3 billion in the case of Russia, and more like a billion for other "big" military spenders.

Of equal significance is the trend in US intelligence spending. One might think that the diminishing national security threat would curtail intelligence spending, but it appears there has been only a modest reduction at the margin - maybe 10 to 15 percent less, nothing like the more precipitous decline in military funding. Indeed for five of the post-Cold War years, US intelligence has been led by directors proclaiming the "new, more dangerous world" we live in, even with the absence of a super-power confrontation. The supposed complexity of the lesser potential conflicts around the globe - the non-war threats - the terrorist, the drug cartels, the proliferators - have been used and, I must say, successfully to sustain intelligence funding levels.

So there is a great deal of truth in what Smiley said. The profession of intelligence is perfectly secure, or so it seems. The fragmented states of the old Soviet Union may not all quite fit in the category of allies yet, but most are partners. What height of folly would lead one to argue that, therefore, the numbers of spies should be reduced, the number of spy satellites curtailed, intercept activities curbed, or sensors, sniffers, and spoofers downsized. It is also true that the United States has not been able - despite the best efforts of some - to find a new international villain to supplant the Russian bear. The panda is too cute and cuddly, and besides he has nearly a quarter of the world's population and can produce gobs of cheap consumer goods at unbelievable prices. Saddam Hussein certainly gets under America's skin, but that bully has been beaten up once already. The tried and true - Iran, Cuba, North Korea - are not really contenders for the title of chief villain, at least not for a decade or so.

TODAY'S TOPIC - RESOURCING INTELLIGENCE

But my task today is not to find a villain, but rather to explore the balance among the intelligence disciplines most suited to an era when there is no clear-cut threat of any magnitude. First, let me address what this talk is not about - worthy subjects though they be. It is not about the value of information or intelligence. That is taken as a given. It is not about the organization and management of intelligence in general, nor specifically about the labyrinth that is US intelligence. Nor will we address covert action activities conducted by intelligence agencies. Nor are we to confront the large issues of accountability, oversight, and the ethical dimensions of intelligence. Rather, as the title suggests, the focus will be on providing some sense of the balance in intelligence among the various functions and disciplines: the balance between open and clandestinely-acquired information, the balance between human source or agent collection and technical collection approaches, the balance between use of academic expertise and home-grown intelligence analysts.

So let us try to design intelligence cut to the cloth of the 21st Century. Let's start with the most obvious parameters.

OPEN SOURCE DOMINANCE

First, let's examine some of the characteristics of information that are emerging that will carry into the 21st Century. The vast bulk has been and will continue to be unclassified, so-called open source information. Conventionally that has been sized at about 90 percent - or, as Smiley says - nine times out ten the journalist will know as much. It varies, of course, with the topic. Certainly, much higher when it comes to basic economic, political, and social information. No doubt significantly less when one considers issue like international terrorism, drug trafficking, nuclear proliferation and the like.

I know of no precise test or proof of what percentage of information is openly available, but I think it is fair to argue that it certainly must be increasing. Most of the closed, controlled societies of this century are now part of history, and the number of nations engaged in the more rigid forms of information control appears to be rapidly diminishing. Not only are most societies more open and their information more readily available, but the access of any outsider to it is infinitely better. There is hardly a country in the world that doesn't have its government gaudily displayed on an enticing web pages that lead you to ever more details of the country and its governmental institutions, its policies and its programs, its politics and its personalities. Read its newspapers, visit its universities, sample its other print and non-print media. And if you are not sated by these, join the innumerable chat lines that are often inquisitive and most insightful, if not openly critical, of their own national, regional, or local politics, institutions and cultures.

Look at the lesson of the last year in Asia, where the tiger cub economies of yesterday have become house cats in training in the name of transparency. While Asia's leadership has been spared the fate of the more ideological and politically repressive regimes of Europe, their economies have been given a heavy dose of openness in process and transparency in dealings that is more attune to Western democratic and free market values. They may not yet quite be at the stage of open covenants openly arrived at, but they are certainly moving notably in that direction.

It is hard to imagine that the trends set in motion by the Internet and the worldwide web will not continue to grow and expand. More information, organized in much more accessible hierarchies, or searchable through ever more powerful search engines or knowbots, translatable into languages, formats, and digits that mere mortals, as opposed to the cognoscenti, will be able to acquire, analyze, and report.

WHAT RECENT US STUDIES SAY

This conclusion is shared by a series of reports of recent years that can provide anyone with a pretty clear understanding of the direction of the trends in information technology and intelligence for the future. Let's briefly make mention of these so that any of you with further interest in the topic of this presentation can develop your own confidence in the directions and trends in information and intelligence:

First, there is an excellent small volume done by the prestigious US Council on Foreign Relations and entitled *Making Intelligence Smarter*. Richard Haass, a former National Security Council advisor and frequent television commentator on foreign policy issues, directed this study.

Second, there was the in-depth report of the Commission on the Roles and Capabilities of the United States Intelligence Community, initially directed by the late Les Aspin, former Secretary of Defense, after whose untimely death, was led by another former Defense Secretary, Harold Brown. Its is appropriately titled - *Preparing for the 21st Century: An Appraisal of U. S. Intelligence*.

Third, the US Congress contributed its own detailed staff study, called *IC21* or *Intelligence in the 21st Century*, done by the staff of the Permanent Select Committee on Intelligence. A colleague of Robert Steele's and mine - Mark Lowenthal - had a major role in putting this excellent report together.

Finally, not to be outdone, the Twentieth Century Fund issued a report on *The Future of US Intelligence - In From the Cold.*

I want to emphasize that one need not endorse all or even any of the findings, conclusions, and/or recommendations of this vast array of thoughtful research, analysis, and opinion on US intelligence to appreciate the rich source of wisdom and understanding conveyed by these recent studies.

If one looks at these reports only cursorily, one will quickly come to same conclusions reached above about the future importance of open sources of information. Let's look at a few examples:

The Foreign Relation Council study points to "the abundance of information … now available to policymakers on an immediate basis through telephones, fax machines, the internet and other computer links, radio, and television. …satellite imagery can be purchased, vast amounts of information are compiled and analyzed by universities, think tanks, and businesses. … The result is that policymakers and other actors now have more information at their disposal - the intelligence community now has more competitors in providing information to civilian and military officials and users."

The Presidential Brown Commission report similarly found that "the information obtained from open sources was substantial and on some points more detailed than that provided by the Intelligence Community." It called for "a greater effort … to harness the vast universe of information now available from open sources."

There were similar conclusions in the other studies, such as in the Twentieth Century Fund study, which recommended a major increase in foreign service personnel to increase overt collection.

So one overwhelming conclusion that could be reached on the subject of our discussion today is that the very first scarce dollar in everyone's intelligence resource management handbook should be devoted to collection, integration and analysis, and production of open source information. In a real sense, this is not new. One of the first activities that US and British intelligence supported was the acquisition and analysis of foreign radio broadcasts. The venerable trade of personal open source collection and reporting by foreign service or diplomatic officers is also of long-standing and historic significance. These open sources, even today, account for the vast bulk of both near-real-time and long-range products and analyses by US intelligence. My own personal experiences close to national level policy makers confirm this evidence. They are more likely to be focused in on the latest TV speech of Saddam Hussein or his Foreign Minister than the obscure evidence reported in some highly classified human agent report or technical imaging or sensor system.

This is not to say that US intelligence has done a particularly good job of marshaling its open source collection, integration, and analysis efforts. The

Congressional study cited above, for example, noted that "open source intelligence ... has had a difficult time increasing market share commensurate with its potential." The study identifies "a bias among some in the intelligence and policy communities against open sources, stemming from the erroneous belief that no information that is valuable is likely to be easily accessible or unclassified. This prejudice severely undercuts the utility of open sources. [There is] an under-utilization of open sources ... and the IC ... should devote more resources to them." If you listen carefully, you hear shades of Smiley's world-wise conclusion that governments don't trust what they don't pay for.

It is difficult to put a price tag on the open source effort because so much of it is done for other purposes. CNN is serving a news media purpose, the businessman is attempting to assess his market, and the diplomat is conducting foreign relations in addition to their critically important and highly successful open source collection, analysis, and dissemination functions. In the US case, probably no more than several hundred million are spent on dedicated open source activities. Foreign broadcast monitoring and translation, openly-acquired books, periodical and newspaper collection, and some limited internet surfing account for the bulk of these efforts. If you, as many others have, conclude that that number is too small and misses large opportunities, certainly one could conceive of an effort in the $500 million to a billion range before beginning to exhaust this most lucrative and highest value of sources. Like most things in life, at some point, there almost certainly is diminishing returns where the incremental dollar is not worth the output, but we are so far from this today that it is difficult to imagine when the yield curve begins to flatten out.

THE ENDURANCE OF SPYING

The above is not meant to imply that spying, the second oldest profession, does not have staying power. Spying is alive and well and it should be. But if the world is on an ascending curve of openness with volumes of value readily available, literally for the asking, where does clandestine human source collection - the polite term for spying - fit in. Well, we do know that in the days of closed societies, spying was often one of the only ways to get information of almost any genre - military or technical data, reliable economic statistics, political factions and forces at work, and cultural, social, even ideological information. Characteristically, this spying were categorized as against the so-called "hard targets". Though the number of countries that now fit that category has dwindled dramatically, there are still surviving nations whose ways and means are largely hidden. Burma, North Korea, Iraq, Iran, and some others come to mind. So certainly a clandestine capability should remain in place here.

But, in addition, many of the new major concerns of intelligence in the post-Cold War era center on topics that also may be only readily accessible through clandestine means. Intelligence on many aspects of drug trafficking, terrorism, proliferation of the weapons of mass destruction, human rights abuses, and bribery is not likely to show up front and center in the New York Times or easily found openly on the internet. They clearly fit appropriately into the categories of targets more susceptible to clandestine collection. There sometimes are open source approaches to some of these issues and topics, but the hunger of policymakers and law enforcement officials for information on them are not likely to be fully satisfied by open sources. Robust clandestine capabilities are still needed here.

Finally, there is the perennial argument that spying is one of the best ways to determine intentions, that is, spying alone gives policy and operating officials a heads-up on changing intentions, a warning of things to come. This is a difficult argument to prove or disprove. One need only look at the dismal success of human sources in ferreting out the intentions of the USSR in Hungary or Czechoslovakia, the fall of the Berlin wall, the entry of the USSR into Afghanistan or Iraq into Kuwait, or a host of other surprises where spying provided little insight into intentions or warnings of changes in the status quo. Nonetheless, there are enough cases where human agent intelligence was highly instrumental in signaling intentions that it would be dangerous to ignore this task in designing a human source collection posture. The Cuban missile crisis, some of the Arab-Israeli conflicts, and intentions of the former USSR and China today toward many other countries come to mind as areas particularly acceptable to traditional clandestine collection.

Like the findings on open source intelligence, the anticipated future role of spying is carefully analyzed and well understood in the recent studies mentioned above about US intelligence.

The Twentieth Century Fund report, for example, recommends that "the scope of clandestine efforts should be narrowed to focus on potential foes proximate to deployed US troops, … a small number of potentially destabilizing rogue states, groups … engage[d] in terrorist activities, and countries with nuclear capabilities." The report argues that "the clandestine service should be assigned tasks separate from, and more narrow than, the rest of intelligence ... focus[ed] on high-value secrets that cannot be collected another way."

The Congressional House study phrases the same point in a different way: "Clandestine collection must be focused primarily on select high priority national and military requirements." But this study also argues for "at least a minimal clandestine presence in most countries (a "global" presence) so as to maintain a broader base-line contingency capability and to respond to transnational collection requirements."

The Presidential Brown Commission also argues for a global clandestine presence with emphasis on those "hard" targets that cannot be adequately covered by other means. The Foreign Relations Council supports a similar approach.

If you accept these rationales and roles for clandestine human source collection, it should be able to size that effort rather easily, at least in terms of a rough order of magnitude. It is costly to place a clandestine agent with his family, furniture, car, and housing in the field; the United States uses a rough approximation of $200,000 to $300,000 annually. This is slightly higher than a foreign service or diplomatic officer because of security and supporting tradecraft costs - the miniature camera, the listening or monitoring devices, dedicated communications, specialized identity support, and other costs. Using that estimate and supporting a global presence in, say, 200 countries, may add up to $100 million or so. But, one or two staff per country for high priority tasks such as drugs, terrorism, and proliferation and for more troublesome countries such as North Korea and Iraq quickly doubles or triples that number. Finally, at least in the US experience, this needs to be multiplied by a factor of 3 to support a home base rotation and training cadre. Thus, one can quickly size a worldwide clandestine "spying" presence on the order of a billion dollars also.

This, of course, is based on the US model - a model that is unlikely to apply to most other nations whose key country and topical interests and relationships may be more regional than global, more specifically targeted than those associated with the United States' global preoccupation. You can use your own yardstick to measure your national priorities and concerns and the likely contribution that clandestine collection can make to these efforts.

NATIONAL TECHNICAL MEANS

Let's use the euphemism of "national technical means' to summarize all the technical collection approaches of satellites, U-2s, signal intercept activities, and other technical measurement techniques from imagery to sniffers. It is a huge area to discuss and much of it can not be done openly. But, again, the basic parameters are reasonably easy to define. Let's again refer to the recent intelligence studies identified earlier. What do they tell us?

First, the Presidential Commission report finds, not surprisingly, that "satellite reconnaissance is ... very expensive. ...the large satellite systems developed by the United States and the ground stations needed to operate them require expenditures in the range of several billions of dollars per year." For the non-intelligence Global Positioning System, for example, DOD cited costs of almost $5 billion to develop and launch the initial system; the European Commission here in Brussels forecast similar costs for Europe if it decided to build a stand-alone European system. The highly capable SPOT 4, for example, which was scheduled for launch last Friday, reportedly cost almost $600 million. When one adds launch costs, ground control stations, data processing and analysis costs, the costs quickly escalate to a billion or more for even marginally capable satellite systems.

The Congressional study concludes that "SIGINT (signals intercept) is already the most expensive of the collection disciplines. Balancing the required level of investment in [this] technology with the maintenance of existing core capabilities is the true challenge of the 21st century."

So-called measurement and signals intelligence or MASINT is also addressed in several of the report as an area of growing importance with a high level of technical sophistication required to support it.

It should be obvious that these forms of technical collection and processing do not come cheaply. You are literally talking billions to play in the game. Some individual nations or consortium of nations have the financial resources to commit to some of these national technical means, but the opening ante is often so large that most nations cannot or will not commit to expenditures of this magnitude for the limited gain that they see. There are some options, for example, for small satellites that may be capable of performing a limited aspect viewed as critical to a nation whether for prestige or substantive reasons. A separate US Small Satellite Review Panel concluded that, to the first approximation, satellite cost is linear to weight - a conclusion that can be interpreted to imply that one gets what one pays for. A small satellite may be reasonable to monitor the weather or take a multispectral view of its land cover or vegetation. But the large worldwide reach of these high tech systems comes only with a very heavy financial burden for nations or groups of nations accepting the challenge. The same arithmetic seems to apply to signals intercept activities made the more demanding by the pace of technological advances in areas such as digital communications, fiber optical cables, data compression, and sophisticated encryption and signaling techniques.

One final comment on the subject of technical collection. Most of the US studies in this area point in the direction of international cooperation rather xenophobic nationalism. Even for the US, the heavy costs of these technical means strongly argues for a burden-sharing approach that maximizes joint asset use. This continues to be a policy theme supporting future US technical operations.

CONCLUDING COMMENTS

The balancing of resources among spies, satellites, and schoolboys should proceed in such a fashion as to take advantage, first, of the most cost-effective and, then, proceed to the least cost-effective. Clearly, the open source world has a great and growing appeal as the most advantageous of the approaches examined. A very sizable chunk of any country's initial dollars should be devoted to these endeavors. In the US case, this should be moving upward to a billion dollar range from a current level several times less. This "schoolboy" approach to collection, research, and analysis should be mirrored in the accession of analytic talent as well. Rather than the traditional heavy reliance on home-grown expertise within US intelligence, a wider outreach for analytic expertise appears more appropriate to the information age. Resources devoted to open source solutions could perhaps go higher, but we are below it by such multiples that it is difficult to calculate the eventual optimum crossover point for additional open source resources. For other countries, a similar, perhaps even greater, open source dominance would seem appropriate.

The spying profession should not be relegated to retirement, for as Smiley says, as long as nations compete and scoundrels rule, governments will want to take the step of hiring and paying their own informants. It is an area worthy of the incremental dollar in high priority areas, not only for the US, but for other nations as well.

Finally, there will be targets and areas that will merit some degree of high cost technical collection effort as well. But these will be even more selective than the areas where human source collection is sought for most nations. For the US and a few other nations and international or regional groupings, technical approaches on a massive scale may be possible, but, even here, the push toward cooperation and exchange - even if behind a veil of classification and compartmentation - is likely to be sought.

Arnold E. Donahue is President, Pactrade, Inc., a private consulting and trading company that he helped form after a long career involvement in US intelligence policies, programs, and operations. This included 27 years in the Executive Office of the President, Office of Management and Budget, with responsibilities for US intelligence resources, organization and management, policies, and legislation. He recently has led several major studies at the National Academy of Public Administration - one on the Global Positioning System and another on US geographic information resources. Pactrade is located at 3232 O Street, NW, Washington DC 20007; telephone (202-338-0593) and email: aedonahue@worldnet.att.net.

EuroIntel '98 PROCEEDINGS 1 st Annual Conference & Exhibit European Intelligence & European Electronic Security: Open Source Solu - Link Page

Previous	Belgian Observations on Intelligence Oversight and Strategic Opportunities for Change
Next	Economic Espionage and Open Sources: Legal and Security Implications for Planning

Return to Electronic Index Page