The Intelligence Profession Series

Number SEVEN

INTELLIGENCE:
What It Is And How To Use It

by

John Macartney

6723 Whittier Avenue, Suite 303A
McLean, Virginia 22101
(703) 790-0320

The Association of Former Intelligence Officers (AFIO) was formed in 1975 by former intelligence personnel from the Federal military and civilian intelligence and security agencies. Its purpose is to promote public understanding of, and support for, a strong and responsible national intelligence establishment.

AFIO believes that effective intelligence is the nation's first line of defense against surprise from abroad and subversion at home and is indispensable for our national leaders in the conduct of foreign and defense policy. AFIO therefore holds that reliable intelligence is essential to the cause of peace.

In its first years, AFIO was active in providing expert testimony to committees of Congress which were investigating various aspects in national intelligence. With a lessening of the amount of effort required to provide Congress with objective, expert testimony, AFIO is embarking on an education project designed to provide material which will support the teaching of the subject in American universities and colleges. This series of monographs is one aspect of that project.

AFIO is independent and has no affiliation with the United States Government. Publications of the Association, however, which could divulge sensitive information regarding sources, methodology and techniques, are cleared with the proper element of the intelligence community. Clearance with a government element merely serves to satisfy security requirements and does not constitute substantive approval by that element; In fact, AFIO will not accept substantive direction. Opinions expressed in these monographs are those of the authors, not necessarily those of the Government or of AFIO.

Future editions of this series will address other subjects of current critical interest to the United States intelligence community and the citizenry. These will include secrecy, estimates, the legal and ethical bases for national intelligence, the history of national intelligence in the United States, comparisons with foreign services, collection, policy and the establishment of requirements.

Other pamphlets in this series are:

The Clandestine Service of the Central Intelligence Agency by Hans Moses

National Security and The First Amendment by John S. Warner

The KGB: An Instrument of Soviet Power by Thomas Polgar

Warning Intelligence by Cynthia M. Grabo

The Role of Women in Intelligence by Elizabeth P. McIntosh

The Central Intelligence Agency: An Overview by Lewis Sorley

INTELLIGENCE:
What It Is And How To Use It

John Macartney

Intelligence Profession Series
Number Seven

The Association of Former Intelligence Officers
McLean, Virginia
1991

About the Author

John Macartney is a faculty member at the American University and a past Commandant of the Defense Intelligence College. A former Air Force fighter pilot and planner as well as a former intelligence officer, he has been on both side of the operations-intelligence interface. This paper was written while Colonel Macartney was serving as the DIA Representative at the National War College.

The monograph series, *The Intelligence Profession,* is published by the Association of Former Intelligence Officers, 6723 Whittier Avenue, Suite 303A, McLean, Virginia 22101. Copies are available for classroom use.

Printed at McLean, Virginia

INTELLIGENCE:
What It Is And How To Use It

Contents

INTELLIGENCE:

What It Is And How To Use It[1]

Introduction

Intelligence not only has to train new recruits but also to educate its customers. This is a formidable task... They have to be convinced of what intelligence can, and what it cannot achieve: they must learn that an overload of requests will result in diminishing returns; that intelligence should be taken into the confidence of policy-makers if these wish to obtain relevant information.

Professor Walter Laqueur[2]

This is a consumer's guide. It's intended as a roadmap for those who use intelligence information to do their jobs – US military commanders and government policymakers. They need to understand what intelligence can do for them, what it can't do, and how to use it. But in my experience, many do not.

My goal is to clear away myths, provide a big-picture understanding, and offer practical tips for using intelligence. The emphasis is on military intelligence and Defense Department consumers. That reflects my own background as well as the fact that the overwhelming majority of all the government officials who are concerned with intelligence, producers as well as their customers, are Defense Department employees. Nevertheless, what follows will also be applicable to those who use intelligence at the State Department or elsewhere in the US Government.

WHAT IS INTELLIGENCE?

Spy novels, Hollywood movies and sensational headlines have given us a distorted picture. Stripped of its James Bond/Rogue Elephant mystique, *intelligence is basically a dedicated information support service for government policymakers*. Thus the business of intelligence is really the processing of information. For a more useful image of intelligence, picture a think tank or a news room, rather than James Bond. Like a research institute, intelligence employs vast numbers of experts, including many Phds, and like a think tank or the media, it produces information and analysis. Unlike those others, however, intelligence serves up *tailored* products to a restricted clientele and has its own dedicated and sometimes exotic information sources, including secret agents and elaborate systems of high tech sensors. And of course intelligence focuses primarily on foreign political and military information that governments may conceal and distort. Let's begin with the fundamentals:

- Intelligence is a policy *support* rather than a policy making function
- Intelligence looks at *foreign* information; it is prohibited by law from collecting or maintaining information about this country or its citizens
- Although intelligence makes use of classified sources, most information comes from open sources including books, newspapers, public announcements and the observations of diplomats
- Most classified intelligence information is collected by technical sensors
- Intelligence sources and methods are very fragile and classification is primarily intended to protect those sources.
- There are persistent and sometimes serious strains in the relationship between intelligence and its policy making customers; and breakdowns in that relationship are the cause of most intelligence failures (rather than lack of information)

- Dissemination bottlenecks are another cause of failure; too often information doesn't get *down* to key staff and field units that need it
- Good, objective intelligence will sometimes conflict with policy (and thereby infuriate policy makers)
- Optimized for peace, intelligence would be very vulnerable in war
- Covert action, which gets most of the notoriety and headlines, is **not** really intelligence at all; the President's Executive Order calls it "Special Activities" while Congress refers to "intelligence related activities" – either way, it's policy
- Two important caveats: (1) The future is basically unknowable and thus intelligence estimates are inherently very tenuous; and (2) a surprise attack against the US might well succeed, despite good intelligence

THE INTELLIGENCE COMMUNITY

Intelligence is a *staff* rather than a line function. As a result, the Community is a loose conglomeration of agencies, organizations and staff elements defined by Executive Order[3]

The Director of Central Intelligence (DCI) is also the Director of the CIA as well as the President's Intelligence Advisor. Depicted in the enter of the chart,[4] the DCI has coordination and guidance responsibilities for the entire Intelligence Community. Those responsibilities are exercised through a separate (from CIA) staff called the Intelligence Community, or IC, Staff. In recent years, that staff has been headed by a military officer of 3-star rank. The DCI plays an important coordinating and leadership role for the Community, but, except for the CIA, does not exercise direct command. Indeed, except for the President (and, increasingly, the Congress) no one has direct command over the whole Community, and thus this "organization chart" has no one on top. The coordination, which is quite effective, is managed through a complex web of interagency committees and staffs, rather than through a chain of command.

Why, some ask, are there so *many* intelligence organizations? Because intelligence is a staff support function, and there are a great many headquarters, commanders and senior policymakers to support. Furthermore, the number of intelligence organizations is driven by the diversity of consumers interests – each intelligence staff specializes in what its particular consumers need (or want) to know. Navy intelligence, for example, focuses on maritime matters, a subject that the State Department's intelligence bureau, which specializes in diplomacy and policy, pays little heed.

The Central Intelligence Agency (CIA), located in McLean, Virginia, is unique in the US Intelligence Community because it is an autonomous organization rather than a staff element of a larger government department – the case for all other intelligence entities. A key point! Partly as a result, CIA employees tend to see themselves as the elite of the profession. They sometimes regard their colleagues elsewhere in the Community as soldiers or foreign service officers first, intelligence officers second, and perhaps captives of the larger bureaucracies they inhabit. The Agency has the biggest analytical staff

The Intelligence Community

within the Community and also exercises primary national responsibility for the clandestine collection of human intelligence (HUMINT). Additionally, and uniquely, the CIA is also charged with conducting approved covert action missions.

The National Security Agency (NSA), headquartered at Ft Meade, Maryland, is part of the Defense Department but is nevertheless an agency of unusual autonomy. It is responsible for communications security (COMSEC) as well as collecting, processing and disseminating signals intelligence (SIGINT). Primarily an information gatherer, NSA

is less involved with all-source intelligence analysis and the production of finished intelligence products. Each of the military services also has sizeable SIGINT elements which operate under the coordination and management of NSA.

The Defense Intelligence Agency (DIA), located in the new DIAC Building on Bolling AFB in Washington, DC, is a joint defense agency that serves the foreign intelligence requirements of the Secretary of Defense, the Joint Chiefs of Staff (JCS) and the Unified and Specified Commands. While DIA provides its customers with all types of finished intelligence, its specialty is military intelligence. The Director is double-hatted as the J2, or Intelligence Deputy, for the JCS. In a third hat as "Director of military intelligence,"[5] he is responsible for coordinating the intelligence activities of the four military services. That gives him a measure of control over Service intelligence programs, including budgets, but not over any part of NSA's SIGINT business. DIA also manages the worldwide Defense Attache System and provides a number of "services of common concern" for the larger Intelligence Community including, for example, photo processing and operation of the Defense Intelligence College. Additionally, DIA supplies current intelligence briefings for the Secretary of Defense and the Chairman of the JCS, and operates the intelligence watch at the National Military Command Center in the Pentagon.

The **intelligence elements of the Services** are much more fragmented and scattered than the three Washington-based Agencies. Army intelligence includes the 3-star Deputy chief of Staff for Intelligence (DCSINT) in the Pentagon as well as over 25,000 intelligence personnel assigned not to the DCSINT but to various Army field commanders worldwide, down through corps, divisions, brigades, battalions and companies. There are also separate Army intelligence production centers such as the Missile and Space Intelligence Center at Huntsville, Alabama as well as training centers at Ft Huachuca and Ft Devens. Whereas the Washington based CIA, DIA and NSA are primarily concerned with national-level, *strategic intelligence*, Army intelligence interests are more *tactical* – focused on the weapon systems, battlefield terrain and other threat or target information of immediate concern to Army commanders in the field. Similarly, Air Force, Navy and Marine Intelligence have a tactical focus and a Pentagon staff as well as dispersed elements scattered throughout the operating commands of their services.

Intelligence elements at **State, Treasury** and **Energy** are much smaller than the CIA or the DOD intelligence arms. Primarily doing analysis, along with some open source collection, they concentrate on the special interests of their respective Departments, but also contribute to the national analytical effort. Although small, State's Bureau of Intelligence and Research (INR) is a major player in both current intelligence and national estimates.

The FBI has counterintelligence responsibilities, and its counterintelligence arm is part of the Intelligence Community, unlike its criminal divisions and other law enforcement elements, which are not.

There is a good deal of personnel exchange among the members of the Intelligence Community, and major elements, especially DIA, NSA an the Community Staff, are composed of personnel on detail from other organizations. While many in DIA and NSA are permanent civilian employees, a sizeable portion, including both three-star Agency Directors, are military personnel on temporary loan (usually 3-4 years) from their Services.

INTELLIGENCE COLLECTION

If the different agencies and organizations of the Intelligence Community constitute one type of subdivision, the INT's, or collection disciplines, are another. As noted earlier, most intelligence information comes from open sources – news stories, diplomatic reporting, and common knowledge. But intelligence is distinguished by its classified information and sources, which are not available to everyone. Most of the secrets are collected by high tech sensors, electronic eyes and ears, described below by former DCI, Admiral Stansfield Turner:[6]

> *Now that we have technical systems ranging from satellites travelling in space over the entire globe, to aircraft flying in free airspace, to miniature sensors surreptitiously positioned close to difficult targets, we are approaching a time when we will be able to survey almost any point on the earth's surface with some sensor, and probably with more than one. We can take detailed photographs from very long distances, detect heat sources through infrared devices, pinpoint metal with magnetic detectors, distinguish between barely moving and stationary objects through the use of Doppler radar, use radar to detect objects that are covered or hidden by darkness, eavesdrop on all manner of signals from the human voice to electronic radio waves, detect nuclear radiation with refined Geiger counters, and sense underground explosions at long distances with seismic devices.*

Signals Intelligence. **SIGINT** encompasses many of those sensors. SIGINT'rs, or "crypies", as they are called in the Navy, have a long and distinguished history going back to both World Wars.[7] Not until the mid-1970's was the SIGINT story of World War II made public. The ULTRA secret, the fact that we and our British allies were intercepting and decoding much of the military and diplomatic transmissions of both Germany and Japan, is now recognized to have been a decisive factor in that war.[8]

SIGINT today is basically a continuation of those wartime efforts and embryonic organizations. It is a very sophisticated, high tech business with numerous sensors and antennae scooping up vast quantities of signals. Hundreds of linguists are on duty day and night, while literally acres of computers sift through electronic signals and seek to unravel codes. Not only are communications of interest, but all

manner of electronic emissions. So much is taken in that not all of it can be exploited in real time; much is taped for future use. During World War II, code breaking, or *cryptanalysis*, was the work of geniuses – slide rule equipped mathematicians and linguists. Today they have the world's newest and most powerful computers to assist them.

Even without breaking codes or reading the content of messages, a great deal can be learned from a technique called *traffic analysis*. Much may be gleaned from the number of transmissions, for example, or from observing who is transmitting and at what time of day. Sometimes the message format, or maybe its length, or some other characteristic of the transmission, may give valuable clues. Skillful analysts learn to associate certain patters of message traffic with key events, such as a military headquarters going on alert.

SIGINT produces the greatest volume of new intelligence information, and it is usually the most timely as well. A SIGINT "hit" arrives within seconds and can be passed on to senior policy makers, in some cases, within minutes.

Imagery Intelligence. Policymakers all want to see pictures, and **IMINT** has become the most glamorous of the collection disciplines. The intelligence job is not done when information has been collected, analyzed and disseminated. To be really effective, a good intelligence officer has to make sure his customer, the policymaker, actually gets the message and appreciates its significance. Thus, intelligence also has to be "marketed". And here, as they say, a picture is worth a thousand words.

Imagery comes from a wide variety of sources – hand held cameras as well as reconnaissance aircraft and satellites,[9] and may be a conventional photograph, or perhaps a video, infrared or radar image. Imagery is a wonder of modern science, it certainly enlivens intelligence briefings and products, and it is marvelous for convincing skeptics. But it has limitations that consumers tend to overlook.

To begin with, cameras can't see what's inside a building or under cover. Then there are the matters of clouds and darkness – the Eurasian land mass is cloud covered up to 70 percent of the time. Also, cameras have to be aimed, told where to look. And finally, electronic transmission of imagery consumes extremely large amounts

of transmission capacity – it's not always easy to get imagery into the hands of consumers, especially distant field commanders.

Human Intelligence. HUMINT involves both open and clandestine collection. The open collection includes attache and other diplomatic reporting, as well as systematic debriefing of refugees, emigres, defectors, ex-hostages and so on. The clandestine part of HUMINT generally involves *case officers* and their *agents*, or *assets*. As a former DCI describes it:

> *The case officer is always a CIA person, usually an American, usually overseas. He is the contact between CIA Headquarters an the agents who do the actual spying. Agents generally are foreigners...*[10]

While HUMINT generates smaller quantities of information, compared to the technical sensors, it often supplies the most critically important. In addition to gathering intelligence "in the old fashioned way," case officers or their agents may also be involved in the placing of remote sensing devices, or perhaps the surreptitious acquisition of an item of foreign equipment.[11]

Along with the three main INT's described above, there are a dozen or so lesser ones. Some examples: MASINT (measurements and signature intelligence), MEDINT (medical intelligence), NUCINT (nuclear intelligence).

Readers should also keep in mind that there are various non-intelligence sensors, such as AWACS, the Air Force's airborne radar planes, or the Navy's underwater acoustic systems. These are the business of military *operations* rather than part of the intelligence function. Although the distinction may appear subtle to civilians, it is very real and significant to military personnel. Operations sensors are usually those that feed data to weapon systems in real time – such as a fire control radar. Although military *operations* personnel are responsible for operating such systems, they constitute still another source of information and intelligence helps to exploit it.

INTELLIGENCE PRODUCTS AND SERVICES

Once collected, the information is tested against and combined with other information, both classified and unclassified. Analytical judgment is applied and the information is "produced" as a finished intelligence product, ready for dissemination. Both the large number and the wide diversity of intelligence products are impressive. A review of the product line is probably the best way to appreciate the capabilities of intelligence – to know what support is available. There are at least 15 of these products and services.

Current intelligence	Crisis support
Basic intelligence	Arms control support
Scientific and technical	Exercise support
Indications and warning	Foreign intelligence sharing
Estimates	Special security
Threat assessments	Counterintelligence
Operational intelligence	Covert action
Targeting	

Current Intelligence[12] This is the most readily available and common of all intelligence products. For many consumers, it may be the only product they ever see. Because it is usually based on initial and fragmentary reports about fast breaking events, current intelligence may contain inaccuracies or uncertainties that will be resolved by subsequent reporting and evaluation. Also, current intelligence is by far the most **expensive** of intelligence products, and it's quite perishable.

Current intelligence is basically reporting on current events, or what has changed in the last 24 hours (or what may have been discovered during that time frame). It generally takes the form of morning briefings, particularly in military headquarters, and/or printed summaries, tailored especially for the readership and circulated throughout the staff or agency. In many cases, these daily summaries are produced in two or more edition with different levels of classification. Only very senior consumers with a need-to-know receive the most sensitive versions, while field units and general readers will get a "sanitized" edition. Electronic message versions are also shared with other US intelligence organizations and headquarters worldwide.

Along with last night's "news," current intelligence products may also carry in-depth pieces as well as background items geared to upcoming events. If the headquarters is going to host a visiting foreign VIP, there will probably be an item that provides background for the meeting. And if the CINC (Commander, Secretary, etc) is about to take an overseas trip, there will be updates on the countries to be visited.

In addition to the President's Daily Brief, or PDB, the national-level current intelligence products include the National Intelligence Daily, or NID, which is CIA produced but coordinated with DIA, State and NSA; DIA's Defense Intelligence Summary (DINSUM) as well as its Chairman's Brief; and the Secretary of State's Morning Summary. Similar products emerge from the Service headquarters, every one of the military's Unified and Specified Commands, many of their component commands, and most intelligence organizations.

Current intelligence is busy and exciting work. For intelligence managers, the daily briefings and products present an invaluable opportunity to focus the attention of senior leaders on a particular threat or issue.[13] In that way, intelligence officers are sometimes able to set the policy agenda. Current intelligence also offers an opportunity for intelligence to look good, to occupy center stage. Because of the agenda setting an limelight opportunities, senior intelligence officers are usually inclined to push current intelligence – as much as the market will bear. Policymakers, for their part, often become eager customers. They do need to know what's going on in the world and custom tailored briefings and "read books" are nice to have. And it's quite an ego stroke, after all, to have your own personal and private "news show", complete with the latest and most sensitive secrets, plus the opportunity to directly challenge and question the "anchor person." or briefer.

But the cost is very high; current intelligence products are not cheap. Because they must be produced under very short deadlines, and are tailored and orchestrated for high level audiences (leading to considerable concern for the showmanship of the presentations), they require large teams of workers. And since they have to be done all over again the next day, and every day, and at every headquarters, a sizable portion of the total U.S. intelligence effort is involved.[14]

The scene is much the same in every large headquarters: dozens of intelligence personnel labor in a pre-dawn frenzy to have the morning intelligence report ready when the boss arrives. Bleary eyed analysts come in about midnight to review their message traffic for significant new developments; scriptwriters are in a little later to start putting the multiple analyst inputs into a coherent whole; still later the briefers (sometimes called "talking dogs") arrive and start working with graphics personnel to produce hard-hitting color slides and maybe videotapes to illustrate the briefing. Senior intelligence managers are in by 4 or 5AM to review the effort and preside over dry runs while analysts answer questions and provide details. Still later, the editors and printing plant personnel responsible for the printed "hard copy" edition get busy. By 8 or 9AM, the morning intelligence briefing, in all its multi-screen splendor, is ready to go. Shortly thereafter the electronic version and the printed summary will be "on the street." It's a big effort. The larger and more elaborate presentations cost thousands of dollars apiece.

There are also opportunity costs. The intelligence teams that labor overnight to orchestrate morning briefings are essentially shift workers whose expertise will be unavailable later in the duty day to produce the many other intelligence products described below. Nor will they be able to attend policy and planning meetings, answer questions or otherwise interact with the rest of the headquarters staff.

Basic Intelligence.[15] Sometimes called "research", this is the heart and soul of the intelligence business. It is the continuous effort by legions of analysts who are constantly sifting through reams of incoming data, images, reports and publications. They extract and store away millions of bits an pieces of information in preparation for future needs.

Contrary to what you might expect, very little of this new intelligence information flows directly on to a customer. Instead, most goes into "storage" where it becomes part of the national intelligence data base. Analysts from throughout the Community maintain as well as draw on that data base as they prepare products and respond to customer needs. (Think of a huge archive that is being continually accessed, maintained and used by a worldwide network of U.S. military and civilian intelligence analysts.)

The basic intelligence information that will be needed to support the next foreign policy initiative or international crisis is being collected and stored today, and every day.[16] It includes information of every sort from every source: military order of battle information, weapon systems performance figures, details about transportation and logistics networks, political and economic background data, biographical information on foreign leaders, and so on.

Most of this goes into computerized intelligence files for future reference; some of it is produced and disseminated in a multitude of special reports, usually magazine-sized publications that provide in-depth analysis of a specific topic. They cover subjects such as world oil production, or Soviet Spesnatz troops, or the Philippine insurgency. Many, such as DIA's series on the various Soviet Theatres of Military Operations (TVD studies), are valuable to military planners. Since reports of this type are usually non-recurring (one of a kind) and classified, dissemination is a perennial problem. They don't appear on library shelves or in card files and consumers often have a difficult time finding out what is available.

Scientific and Technical Intelligence. S & T intelligence is part of basic intelligence, but is organizationally distinct because the analysts are scientists and engineers. Their job is to keep track of foreign, especially Soviet, science, military technology and industry.[17] In addition to impressive analytical organizations at CIA and DIA, the military services operate S & T production centers, such as the Air Force's Foreign Technology Division (FTD) at Wright-Patterson AFB. The focus of the service S & T effort, understandably, is on foreign weapon systems, and foreign weapons research. Whenever possible, they physically examine and exploit actual weapons that fall into our hands. (Remember the MIG-25 that defecting Russian fighter pilot, Lt. Belenko, flew to Japan some years back?)[18] More often, they have to make do with fragmentary reports about highly classified foreign weapons development programs.

Indications and Warning[19] I & W is the most crucial of intelligence functions, or products. The goal is to detect and provide advance warning of impending threats – to prevent another Pearl Harbor.

Everyone shares in this function, of course, but there are specialists who do nothing else. The basic approach is to have trained duty officers (watch officers) on 24 hour duty at every major military headquarters and intelligence agency, as well as at the White House and State Department. Their job is to continuously track all incoming information, consult with each other and, when trouble is indicated, sound the alarm. Potential threats or "warning problems", insofar as possible, are identified and studied in advance. Lists of "indicators" are developed that can be the focus of on-going collection efforts and which, it's hoped, will provide advance signals.[20] Indicators might include events such as a call up of military reserves.

There are other provisions in the system: CRITIC's, for example, are highest precedence messages that carry critical intelligence information of urgent importance directly to top officials as well as the watchstander network; NOIWON's are secure telephone conferencing arrangements that allow watch officers from various national level command centers to instantly and simultaneously consult one another.[21] WATCHCONS, or watch conditions, are the intelligence counterpart to DEFCONS – they represent the judgment of a particular military headquarters on the status of potential hotspots and are reviewed daily.

This elaborate indicator based system will probably work best for detecting preparations for invasions or other major attacks; warning of more esoteric threats such as a terrorist attack, a political assassination, or a coup d'etat is a much tougher problem. But even a major attack could come as a surprise. Warning is an issue all senior decision makers and other intelligence consumers really need to understand. Most seem to expect far too much, believing that modern intelligence techniques make surprise attack all but impossible in this day and age.[22]

In my view, that's too optimistic. To be sure, we almost certainly would get *tactical warning*, which is a last minute heads-up. But warning just before the attack is not of much practical use.[23] *Strategic warning*, which comes in enough time to be useful for avoiding the attack altogether, or preempting it, is by no means assured. In addition to various *camouflage*, *concealment* and *deception* techniques that might foil intelligence collection efforts, the real problem is our own skepticism and deeply ingrained perceptions.

Let's be very clear on that point: It's our skepticism and preconceptions, not lack of intelligence information, which makes surprise attack so dangerous. The problem is not with the ability of sensors or agents to detect an enemy's attack preparations, the problem is what we (and our allies) are prepared to believe, and to do about it.

We all expect tomorrow to be very much like today. That is, we don't really believe there will be some momentous event, particularly an attack on the United States. And every day we are proven correct. Sure enough, there is no attack. Which further strengthens our belief that the next day, and the day after that, will likewise be peaceful. Intelligence officers just as much as policymakers are subject to this fallacy.

> *British Foreign Office apocrypha tells of a retiree saying that for fifty years, year in and year out, he had assured Foreign Secretaries that there would be no major European war. In all that time, he boasted, he had only been wrong twice...*[24]

The lessons of history are very instructive and very sobering. Despite multiple indicators that their adversaries were up to no good, in virtually every historical case warning came too late to be effective or, more often, was simply ignored by skeptical national leaders. Indeed, history teaches that surprise attacks almost always succeed.

Attack warning will never be clear and unambiguous. Instead, it will be mixed with contrary evidence, or "noise". Moreover, warning is never very welcome. Nobody *wants* to believe a war is about to begin, especially when the indicators are ambiguous and subject to interpretation. In short, policymakers will always be reluctant to accept the worst. Because if they do, they must then take drastic military mobilization actions that will have unpleasant economic and political costs and may further destabilize what everyone hopes is a threatening but manageable international crisis.

Estimates.[25] While almost all intelligence reports or products are likely to contain some analytical comment, estimates are specifically designed to offer *predictions* about the future, often years or even decades ahead.

National Intelligence Estimates (NIE's) are the "Cadillacs" of the whole intelligence product line. Coordinated Community products, they reflect the best judgments of the best analysts from all the organizations and agencies. Dissenting views are footnoted or, in more recent practice, written into the body of the estimate. NIE's are usually many months in research, drafting, coordinating and redrafting. When new international problems suddenly appear, special, "fast-track" SNIE's, are produced, often within weeks or even days. Estimators are the cream of the analytical profession, and the most sensitive and highly classified information is reviewed. A maximum of care, talent, time and effort is lavished on NIE's. As forecasts they are excellent – the best that humans can achieve. Nevertheless, they are not infallible.

Estimates, of course, are just that – the predictions and views of intelligence analysts. They may reflect the personal biases and preconceptions of those individuals as well as the organizational biases of either the intelligence producer, or those of the intended customer, or both. And don't forget that the bottom line of a national estimate often represents a negotiated compromise, the outcome of many hours of bureaucratic bargaining between intelligence agencies.

As in the case of warning intelligence, policymakers may expect too much from estimates. The future is simply not knowable, and intelligence does not have a crystal ball. To visualize the difficulties, put yourself into the shoes of a Soviet analyst. Could you predict where the U.S. SDI (star wars) program will be in 10 years? Imagine all the variables, most of them also unknowns: US elections, Soviet international behavior and defense programs, the US economy, the outcome of many floor votes and multiple political compromises that will take place in Congress, the results of SDI research programs yet to be completed and scientific breakthroughs still to come, and so on.

In addition to the NIE's, which are magazine-sized publications, there are a number of other estimative products. There are, for example, tables which forecast foreign weapons inventories, by year – which are especially useful for defense planners and programmers.

Threat Assessments. Within the military, this term refers to a particular type of estimate – those that are prepared to accompany a specific contingency plan, policy initiative, or weapons procurement proposal. Thus a military operations plan will have appended to it a threat assessment geared specifically to that plan. Likewise, a proposal to fund a new weapon system, such as a new missile or a nuclear submarine, will be accompanied by an assessment of the threats the system will have to contend with over the many years of its operational life – and includes intelligence judgments about how successful the proposed system will be against those threats.

Because these threat assessments are so closely tied to proposed budgets and policies, they can, depending on what they say, serve to justify or negate those proposals. For that reason, they sometimes generate a great deal of attention and become the focus of considerable argument and enormous pressures.

Operational Intelligence. In a military headquarters, operational intelligence, or ops-intel, will be at the forefront in wartime. In times of peace, it is probably the third most visible product, after current intelligence and warning. For the most part, ops-intel is simply intelligence working hand in glove with operators (or policymakers). It is preparing the threat annex for contingency plans, being a member of crisis response cells or staff working groups, taking part in exercises, providing an input to budget programming, and so on. Whatever it is that the headquarters is doing, the intelligence staff should be involved and be providing inputs. Ops-intel also involves briefings to aircrews, and other combat operators, prior to combat missions, and debriefings on their return. And it includes combat related intelligence specialties like prisoner of war interrogation and targeting.

Targeting. Targeteers are ops-intel specialists who recommend enemy targets for attack. They do the detailed target studies that identify the enemy's most vulnerable nodes and prepare the target folders that aircrews carry into battle. Targeteers also work side-by-side with mission planners, developing radar and anti-aircraft missile overlays, and helping to select the most advantageous routes into and out of a target, as well as refueling points, bomb jettison and emergency bailout areas, and so forth. Their work is critical to operations planning in peacetime, and even more crucial to war fighting.

Had the Japanese attack on Pearl Harbor been based on a good intelligence target study, for example, that attack could have been much more devastating. Although the battleships and aircraft that the Japanese destroyed were "juicy" targets, they were far less significant to the future American war effort than the petroleum storage and ship repair facilities that were spared.

Targeting began as an Air Force intelligence specialty and since World War II has been primarily associated with nuclear weapons and the development of the Strategic Integrated Operations Plan (SIOP). While that is still part of the targeting business, changing threats, advanced weapon systems and strategies are placing significant new demands on targeteers. NATO's newest planning strategy, the Follow on Forces Attack, or FOFA, is essentially a targeting scheme. And Low Intensity Conflict is presenting whole new problems. Special operations forces require minutely detailed targeting support – many orders of magnitude different than working on the SIOP. What times does the guard detail change? How high is the perimeter fence?

The advent of the cruise missile is generating another new workload for targeteers and also putting at a premium detailed geographic terrain data (still another product of intelligence). In pre-planning cruise missile missions, targeteers not only select the targets but essentially "fly" the missions in advance, from launch to impact, by computer, and store it all in the missile's memory.

Crisis Support. When an international crisis is in full swing the demands for intelligence mushroom. Normal operating procedures won't suffice. So crisis reaction teams or special intelligence task forces are formed and placed in command centers, on rotating 24 hour shift duty for the duration. These teams include analysts, of course, but may also involve typists, briefers and graphics people as well as collection managers who work to refocus collection assets on the new hotspot. In addition, Washington or theatre based intelligence personnel may be deployed to the on-scene commander's headquarters (or ship) to assist with special intelligence communication needs and insure prompt dissemination of relevant intelligence products.

Arms Control Support. Arms control has become a growth industry for intelligence. Each step of the process, from formulating the U.S. negotiating position, to evaluating Soviet proposals, to negotiating the agreements, to promoting the ratification process back

in Washington, to monitoring the final treaty, all require intelligence input. Whether a START proposal is worthwhile, for example, may depend on the relative capabilities of Soviet weapons systems and their strategic target set versus our strategic target set.

Monitoring of treaty compliance is probably the part of arms control most closely associated with intelligence. During negotiations, intelligence has to keep making clear to policymakers what treaty provisions it will be able to monitor and with what level of certainty. (Since treaty monitoring can never be done with absolute certainty, the negotiators, and ultimately the President and the Senate, have to decide just how much uncertainty can be tolerated.)

Once the treaty is in place, *monitoring* is essentially an intelligence function, while *verification* is a policy function. Without belaboring the point, suffice it to say that monitoring and verification are not one and the same. Monitoring is the process of keeping track of what the other fellow is doing – that's intelligence. Verification goes on from there and involves policy judgments about intent, legal interpretations of the treaty and estimates of military significance along with considerations about domestic politics and ramifications for our own future plans.

Exercise Support. Months before a military exercise begins, intelligence experts are called on to help design and write the scenario. Later, when the exercise is played, that scenario will unfold in the form of simulated intelligence messages arriving at the various participating headquarters. Those messages, hundreds of them, have to be scripted in advance and loaded into computers – a massive undertaking and another intelligence "product". Additionally, intelligence is increasingly being asked to play the red, or adversary, side of red versus blue war games, and that is becoming still another intelligence specialty.

Foreign Intelligence Sharing. Cooperation and exchange of information takes place between the intelligence services of friendly governments and within formal alliances such as NATO. The US and Great Britain, for example, have a well known intelligence exchange relationship that goes back to World War II and ULTRA.[26]

Another exchange phenomenon is more recent and less well known. It involves the use of intelligence information as a foreign policy *tool*, as a valued commodity in foreign assistance (one that costs little and does not require appropriations).[27]

With their sophisticated "national technical means" of collecting intelligence the US and the USSR are in a position to make their unique and valuable information selectively available in the game of statecraft. Intelligence sharing really ought to be listed in textbooks as a separate tool of foreign policy, along with the familiar listings of diplomacy, foreign aid, military assistance, propaganda, covert action and force. Intelligence information is also used publicly as a diplomatic tool. Recall the 1962 Cuban missiles crisis when our UN Ambassador, Adlai Stevenson, dramatically illustrated his publicly televised Security Council speech with intelligence photos taken from a U-2 reconnaissance aircraft.

Sensitive Information Security. In most organizations, the intelligence function also includes SCI safeguards, the province of the Special Security Officer, or SSO. This is still another product, or service, of intelligence – the whole world of sensitive information handling, codeword security clearances, security violations, and so on.

Counterintelligence.[28] More active than security, but related, is counterintelligence, or CI. This function encompasses the activities conducted and information gathered to protect this country against foreign espionage, other clandestine intelligence activities, sabotage, and terrorism. Counterintelligence is sometimes associated with law enforcement and uses some of the same methods and investigative techniques. Indeed, in the Air Force, counterintelligence is assigned to the Office of Special Investigations (OSI), the USAF law enforcement arm, rather than intelligence. That's somewhat similar to the Navy but very different from the Army, where CI is under intelligence. Within the borders of the United States, the FBI has overall responsibility for CI while the CIA carries that mission abroad.

This is the stuff of spy novels. Some cases lead to criminal prosecutions, while at other times diplomats may be expelled, or the spy may be fed disinformation, or perhaps recruited as a double agent.[29]

Counterintelligence came under heavy criticism from the Church Committee and other critics for alleged abuses – collecting information about student radicals and other American dissidents. As a result, there are extensive legislative restrictions on CI, which generally exempt US citizens from surveillance except when there is a foreign connection.[30] With the string of spy cases that came to light in the

eighties – Walker, Pollard, Howard, et al – CI is being strengthened.

Covert Action. This is an entirely different realm from information gathering and dissemination. Covert actions are secret *operations* designed to influence foreign governments, events, organizations or persons in support of US foreign policy. They may include political, economic, propaganda or paramilitary activities.[31] Covert actions are traditionally designed so that sponsorship cannot be traced or confirmed (plausible deniability). Secret propaganda campaigns, or funneling money to a foreign institution such as a trade union, or providing support for freedom fighters, might be examples.[32] Covert action provides options to policymakers when allies ask that their cooperation not be disclosed – or when diplomacy isn't enough but sending the Marines would be going too far.

Covert action is **not** intelligence per se.[33] Presidential Executive Order 12333 (4Dec81) uses the terminology, "special activities approved by the President." The Executive Order goes on to say:

> *No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution (87 stat. 855) may conduct any special activity unless the President determines that another agency is more likely to achieve a particular objective;*[34]

Because of the controversy and headlines surrounding covert action, much of the public equates it with intelligence. For many, it may be the only product they associate with "intelligence". Covert action has become commingled with intelligence for good reason. It is an important additional function which many governments, including our own, assign to their intelligence services. The CIA's assignment of that responsibility in the late 1940's has been reaffirmed in subsequent Executive Orders of several Presidents as well as in legislation.

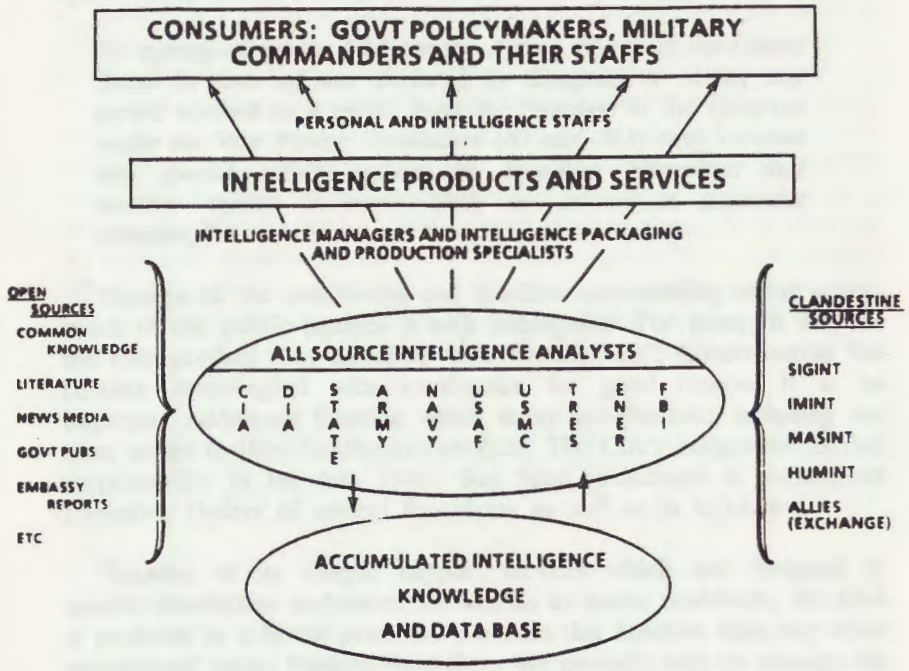
Because of its unique support services which are designed to sustain clandestine endeavors, as well as its assets worldwide, the CIA is probably in a better position to handle this function than any other government entity. Nevertheless, there are periodic calls to reassign the covert action responsibility to the military, as the British do, or elsewhere within the government.[35]

While covert action seems to get the lion's share of attention and headlines, including scrutiny by the two Congressional oversight committees, it is actually a relatively small part of what the CIA does. Dr. Robert Gates, former Deputy Director of Central Intelligence, reports that less than 5 percent of the CIA budget and 3 percent of CIA personnel are involved.[36] The remainder of the CIA, as well as the rest of the US Intelligence Community, is focused on turning out the more traditional intelligence products discussed above.

INTELLIGENCE: THE BIG PICTURE

So far we have discussed the organizations of the Intelligence Community, the collection disciplines, and some 15 intelligence products and services. Now we can step back and look at the big picture – how it all fits together to form what is sometimes referred to as the "intelligence business."

The diagram below offers one way to look at the intelligence business. Day and night, raw information pours into intelligence analysts who work in the various agencies and departments as well as the armed services. Much comes from open sources listed on the diagram's left, while additional information comes from clandestine sources and sensors.



In the center are the analysts, experts who continuously take aboard the new information, test it against and combine it with what they already know, and enter it into their accumulated data base. From that vast reservoir of knowledge and data, the analysts prepare their various "products." These are disseminated up the chain to consumers in many forms – briefings, published studies, memos, video-tapes, computer discs, target folders, annotated maps, and so on. Usually these intelligence products are *tailored* for a specific customer and are often filtered through layers of intelligence managers as well as production and packaging specialists (briefers, editors, graphic artists) plus the personal staffs of senior officials. Those products and services include current intelligence summaries, warning, estimates, arms control support and so on.

Note that analysis and production are at the center of our diagram. *That's because analysts are the heart of the intelligence business.* Also very significant, the consumers are on top – for intelligence, the customer really is the boss.

INTELLIGENCE AND POLICY:

CUSTOMER RELATIONS

The feud was rooted in the classic power struggle that has been endemic in military organizations since men first answered the call to arms: the struggle over who should control military intelligence. " ... " Not only had it made a major contribution towards ensuring that the Japanese succeeded with their surprise attack, but had almost cost us the Battle of Midway. In truth it had plagued our military commands through World War II -- and it is still going on today.

Admiral Edwin Layton[37]

We turn now to the final stage of the business – dissemination, getting the product into the hands of customers. This is the critical stage. Intelligence failures are seldom caused by a lack of information. Instead, the weak link is usually dissemination – which is dependent on the *relationship* between intelligence and policy. Both intelligence officers and policymakers need to pay close attention to that relationship. It's critical, and it's often strained. As we shall see, there are some very formidable barriers that stand in the way.

Lack of Understanding. To begin with, intelligence and policy come together in almost total ignorance of each other's business. Policymakers, even those who have been using intelligence products for years, often know little about where those products come from and how they are produced. Indeed, more than a few policymakers confuse intelligence with anything classified, or with "dirty tricks." Thus, stealth aircraft or Ollie North are mistaken for examples of intelligence.

If anything, the situation is worse on the intelligence side. In my experience, intelligence officers, especially military intelligence officers, are likely to be unusually naive about how Washington works – the politics of policymaking. Intelligence personnel enter a service or agency, are trained in their new specialty and go straight to work – collecting and analyzing *foreign* political, economic and military information. Buried in the depths of intelligence organizations, they remain blissfully ignorant of counterpart information about their own country. It's little wonder that the two, producer and customer, have trouble with each other.

Objectivity and Integrity. Being right about the facts is what intelligence is all about. That implies analytical skill and, above all, objectivity – letting the chips fall where they may. But objectivity can actually be dysfunctional within a bureaucracy. Policymaking in the US government is essentially an advocacy process. And in the give and take of policy debates, commitment, persuasiveness, and single minded loyalty are what count. Thus intelligence, which prides itself on being objective, is always at risk and under pressure. By taking objective positions, as it must, intelligence operates differently from virtually all other large organizations, especially the military and foreign affairs bureaucracies where group loyalty and cohesion, even parochialism, are sometimes considered virtues. In the bureaucrat's world of "us versus them," intelligence is often an unloved devil's advocate, especially among the players on its own team.

The military commanders and government policymakers who consume intelligence are invariably in the intelligence organization's chain of command. The customer really is the boss, and pressures to "get on the team" can be enormous. As Lt Gen Perroots, former Director of DIA, liked to say,

Telling our masters what they don't want to hear is the hardest part of the intelligence business.

Facts and estimates that might contradict or undermine established policy or organizational interests are resented, and may be rejected outright. And woe to intelligence if their contrary analyses end up in the hands of their master's bureaucratic opponents, as they frequently do. The impulse to be objective is one of several factors that pit intelligence against its customers.

Classification and Compartmentation. The so called "green door", behind which intelligence is alleged to hoard its secrets, has always been, and forever will be, a problem. Classification is necessary to protect intelligence sources and methods. But classification can and too often does keep intelligence from getting to the very consumers who need it most. Sensitive information, especially if it was collected by "national technical means," is protected by special compartmentation. Although much effort has been spent trying to break down the "green door," the continuing flood of classified information leaks plus all the recent spy scandals have been tightening access.

Military personnel at the operating level do not normally hold codeword clearances. Nor do most foreign service officers. In theory, they will get necessary intelligence when the time comes, when they have a need-to-know. In practice it doesn't always work, and bitter operators have countless stories about troubles encountered in getting intelligence.

It's a serious dilemma. There are very real security needs in direct conflict with valid consumer requirements. The problem generally exists with command levels below the one where the intelligence is produced. At the uppermost levels, the President and other senior consumers obviously "have the tickets." But down the command chain, it's a different story. Most information can be "sanitized" – by removing references to the source, and perhaps toning down the specificity and timeliness of the report. That's a good fix; it allows the general thrust of the information to be distributed at lower levels of classification. But sanitization is time consuming and therefore expensive. Moreover, it must be done by upper echelons of intelligence (whose own customers have already gotten the word) on behalf of someone else's customers at lower levels.

The key to the green door problem ultimately lies with the senior intelligence officer at each level. He or she must aggressively take the initiative to find out, on a continuing basis, what is being held at higher levels which may be of relevance to his or her customers. Once the existence of needed intelligence is known, the problem is manageable. Arranging for dissemination of a specific, known product is relatively easy – it's the products you don't know about that the green door hides.

A related problem is the "black door" behind which policymakers keep their plans and new technologies secret. The intentional exclusion of intelligence from policy, especially in early planning, is a serious and long standing problem. Washington has become a place where it seems virtually impossible to keep a secret. As a result, sensitive operations must be very closely held, to as small a group as possible – sometimes excluding intelligence. And even if the senior intelligence leadership is cut in, lower level analysts, the real experts, may still be left out. More than a few so-called "intelligence failures" have resulted from the willful exclusion of intelligence from operational planning. The 1983 Grenada operation and the "Iran-Contra" affair are two of the more recent, and spectacular, examples.[38]

"Intel Weenies" -- Personalities and Personnel. Intelligence, as its name implies, is an intellectual calling, and intelligence analysts are generally a different breed than their customers. Analysts tend to be men and women of ideas, studious and introspective, more comfortable with ambiguity and objectivity. Their customers, on the other hand, are the movers and shakers of the policy world. They are generally more extroverted, decisive, goal oriented, and impatient with uncertainty.[39] The personality differences are reinforced by status differences, especially in the military.

Intelligence officers find they are always junior in rank vis a vis their customer, and, as staff support officers, not fully accepted into the profession of arms. They lack the combat medals and gung-ho warrior flair that mark the top brass. Sometimes, behind their backs, they may be referred to as "intel weenies." These personality, rank and status differences intrude on the intelligence-policy relationship – and can disrupt dissemination.

Military personnel systems are another problem. Those systems are designed to develop commanding officers – generalist managers who need frequent moves for career broadening. But frequent reassignments conflict with the need for analysts to develop expertise through a lifetime of specialized study. Also, officer promotions are likewise geared to combat leadership, and do not usually encourage or reward the intellectual types that are likely to excel at the intelligence business.[40] For these reasons, along with the personality and status differentials, intelligence doesn't always attract and retain the best officers. Partly as a result, military intelligence organizations are employing increasing numbers of civilian analysts. But that could generate new problems – organizations that cannot readily go to war, and analysts who might not appreciate the military significance of information.

Sheer numbers are also an issue. The production of information is one of the most labor intensive of human endeavors, and our government employs tens of thousands of intelligence personnel – about three fourths of them in the Defense Department. Because intelligence is a policy support function, most are concentrated alongside policymakers – especially in Washington. As a result, intelligence, which is lean in the field, is invariably the largest staff element at higher headquarters.

The numbers are so overwhelming that intelligence is usually kept off the organization charts. Thus, the charts indicate that the J2 of the Joint Staff at the Pentagon is the Director of DIA plus a staff of about 40. Not counted are thousands of other DIA personnel. If they were counted, the J2 would dwarf the rest of the Joint Staff.

Red and Gray, But not Blue. Intelligence specializes in foreign, or "red", threat information, and to the consternation of operators and policymakers is often igorant of parallel U.S., or blue, information. Moreover, well established norms within the military strictly forbid intelligence from concerning itself in any way with blue information. That is the uncontested province of commanders and operators where intelligence dare not tread.

Nevertheless, estimates, background papers and briefings that portray red-only are sometimes criticized for being irrelevant, like a single bookend. This is still another factor that stands between intelligence and its customers. But for intelligence to unilaterally provide red versus blue comparisons, it would have to acquire extensive knowledge of US capabilities, double its workload, and open itself up to a new and extremely dangerous arena of bureaucratic vulnerability. The military services strenuously resist such comparisons and intelligence makes comparative evaluations at considerable peril. An intelligence estimate that rates U.S. tactics or servicemen inferior to those of a potential adversary, for example, would be sure to generate a firestorm of bureaucratic wrath. Because of that, intelligence will almost always finesse questions that ask how foreign data relates to the counterpart U.S. situation. (Congress is frequently a source of such queries.)

Resource Competition. A final impediment is competition over sharply declining defense dollars. In the last decade, Congress has become a major consumer of intelligence products and is taking an increasingly assertive role in shaping intelligence policy.[41] That is a new development with major implications.

Intelligence information may be used by members of Congress to criticize and challenge the Administration's policy. And if that's not enough to get intelligence in hot water, Congress has also been mandating significant extra funding for intelligence. Because intelligence appropriations are imbedded in the Defense Department's budget, and since these are times of sharp declines in defense

spending, that's a zero sum game. Every increase for intelligence means another unanticipated and painful cut in some other defense program. And that, of course, further exacerbates the often strained bureaucratic relationship between intelligence and its Executive Branch masters, especially in the military.

Intelligence and Its Customers. Intelligence is irrelevant without policy, while policy is blind without intelligence. Nevertheless, there are strong impulses for intelligence and policy to go their separate ways. Policy hates to hear bad news, intelligence that might contradict or undermine organizational interests or preconceived policy. Furthermore, policymakers are a different sort – they don't mix easily with their intelligence colleagues whose intellectualism makes them uncomfortable and whose objectivity is anathema. Intelligence, for its part, is shy; it doesn't understand the policy process and tends to hang back.

Nevertheless, if it is to be effective, intelligence must be brought into the policy arena, close enough to be in tune with the policymaker's goals, close enough to understand the context of the policy struggle. At the same time, policymakers can't expect intelligence to become a policy advocate, or a "team player". Should it do so, its credibility and therefore its usefulness will be compromised, and the stage will be set for failure.

THE LIMITS OF INTELLIGENCE

Wartime Vulnerability. Unlike a fighter squadron or an armored battalion, intelligence does not spend its time training and preparing for the possibility of a future national emergency. Intelligence is executing its mission today and every day, in peacetime. Intelligence also differs from most military units in that it is largely designed and optimized for peacetime.

The intelligence infrastructure is fragile and would be very vulnerable to attack in the event of major hostilities. Those high tech sensors and Washington-based agencies are not designed to absorb hits. Sensors may also be subject to jamming or other interference and could be stymied by wartime frequency or code changes. Furthermore, intelligence is highly dependent on our own communications facilities that surely would be saturated and would themselves be subject to attack. Finally, there are far too few ops-intel specialists, like targeteers and prisoner of war interrogators. While many of those shortcomings could be corrected, the price would be extremely high – especially in the sacrifice of peacetime capabilities.

Costs and Trade-offs. Intelligence is not free (although commanders and policymakers often seem to treat it as such). Indeed, economists tell us that the single most expensive commodity in the business world is information. The reason? The production of information is extremely labor intensive. The situation is much the same in the foreign policy world, where every new intelligence requirement has a high price. Collection systems as well as analytical talent are finite.

When the nation's attention turns to a new international problem, intelligence refocuses its efforts accordingly. But not without foregoing opportunities elsewhere. Collecting more on the Persian Gulf inevitably means paying less attention to some other part of the world. There are always trade-offs. If new information, such as drug smuggling data, is produced, something else will no longer be collected and analyzed. Furthermore, while intelligence has considerable flexibility, it is not without limits. Refocusing may mean sensors must be redirected or moved, perhaps even redesigned. Maybe linguists and analysts have to be trained, and new human agents recruited.

Camouflage, Concealment and Deception. Intelligence analysis, like the research of scholars or scientists, can be likened to assembling a jigsaw puzzle. The task for all three is to see the big picture despite the missing pieces. Unlike a scholar or a scientist, however, the intelligence analyst faces a cunning adversary. One which actively seeks to stymie his or her "research." Not only is information denied by keeping it classified, but active measures may be taken to feed disinformation to intelligence sensors or suspected agents.

Even cameras can be fooled. For one thing, adversaries might know when a reconnaissance vehicle is approaching. Ongoing operations and equipment may simply be covered up, temporarily. Also dummy equipment may be displayed, or false signals transmitted, or phony information released. Sometimes deception schemes are detected, but that might not always be the case. Intelligence analysts and their customers must always keep this unsettling possibility in mind.

Faulty Analysis. Assembling puzzles is tough – especially when pieces are missing. Although most intelligence analysts are extremely bright individuals who are good at their work, they are neither clairvoyant nor infallible. Their analyses may be distorted by biases and preconceptions, their own as well as those of the organizations they belong to. Wishful thinking as well as "mirror imaging" sometimes cause errors, while subtle pressures to tell the customers what they want to hear can be nearly irresistible.

Uneven Distribution of Attention. Intelligence does not know everything. First of all, it deals only in *foreign* information. And regarding foreign information, the emphasis has always been overwhelmingly on the Soviet Bloc and other potential threat countries such as Iran or Libya. Resources are limited, and concentrating on known or potential threats makes sense, but it means intelligence knowledge is spread very unevenly. Beyond the communist countries and the recognized third world hotspots, in the "gray" areas, the capability to collect information or provide analytical judgments is spread very thin – still another limitation policy makers should keep in mind.

Dissemination. The final limitation is perhaps the most serious – the many bottlenecks that keep the product from getting to the customers who need it. When intelligence failures occur, it's seldom because the information wasn't available. More often, failures come

about because the information wasn't delivered to the specific decision makers or operators who needed it in the format and at the time they needed it. We've just outlined the many barriers to good relationships that can come between intelligence and its customers – they interfere with dissemination.

Another very serious problem is getting intelligence disseminated **down** to the worker level – down to the pilots and planners, the foreign service officers and trade negotiators. The problem here is that intelligence sometimes serves the top policymaker too well – lavishing attention on the top echelon (White House, Secretary of State, CINC, Commanding Officer) while neglecting the lower levels. But those who actually prepare the policy papers, write the contingency plans, draft legislation and policy speeches, attend the many staff meetings, negotiate the treaty details, and, ultimately, execute the policy, need intelligence too.

Sometimes this failing may be caused by senior policymakers who demand that 100 percent of the intelligence effort be focused at their level. More often, the cause is on the intelligence side and reflects the human impulse to serve the boss – an look as good as possible. It goes against our natural bureaucratic impulses to do less for the CINC at headquarters in order to do more for a lieutenant on the flightline.

The "green door" and "need to know" restrictions also contribute to this problem, as does the general shortage of intelligence resources. Whatever the cause, failure to disseminate intelligence far enough down into the policy making structure is a pernicious one. It leads to situations, for example, where carrier pilots might find themselves sitting alert with 10 year old target folders, while back in Washington, and maybe even up on the bridge of their ship, senior policymakers are being briefed with last night's intelligence "take."

USING INTELLIGENCE:

TIPS FOR COMMANDERS AND POLICYMAKERS

Commanders and policymakers are in charge of the intelligence staffs that serve them, but they often tend to think of intelligence as something different, not really an integral part of their organization. That's a mistake. *Intelligence is a basic command responsibility*. Make it part of your team! The commanders and decision makers who use intelligence best are those that bring intelligence into their inner circle of decision; they are also the ones that demand first rate support and clearly communicate their expectations to their intelligence staffs. That's the approach recommended here.

MAKE SURE YOUR INTELLIGENCE STAFF KEEPS YOU PLUGGED INTO THE LARGER INTELLIGENCE COMMUNITY. This is by far the most important service they can perform. Only be aggressively mining the holdings of the entire Community can they possibly be certain of supplying what you need, when you need it. That means that your senior intelligence officer should be in touch with the Community leadership in Washington. More important, each of the analysts needs to be on the secure phone daily, comparing notes with his or her counterparts at other agencies. From time to time, those analysts also need to be given the opportunity to meet with their counterparts, to establish the contacts which will later pay off for you and your organization. Similarly, your analysts should be encouraged to follow media reporting and keep up with the work of academics and other non-government experts who report on their area. All that may seem obvious, but some intelligence officers, especially the analysts, may be shy about calling Washington, or try to go it alone.

KEEP INTELLIGENCE IN THE OPS/POLICY LOOP. This is by far the most important thing *you* personally can do. In order to anticipate your needs and see to it they are met, your intelligence staff must know your plans and priorities. There's no other way. Unless you take intelligence into your confidence, make it part of your inner circle and do what you can to nurture your ops-intel relationship, you're not going to be well served. "Asking the right question" is emphatically *not* the way to get intelligence support. It's the job of your intelligence staff to know what information is available and to deliver the intelligence you need when you need it. They do that by *anticipating*

your needs – something thy can only do if they know what's on your mind – what you intend to do. Too many "intelligence failures" have been caused by operators or decision makers who intentionally excluded intelligence from the planning stags of a close hold operation. Don't make that mistake.

DEMAND INTEGRITY AND OBJECTIVITY, AND PERMIT IT. Slanted, or "cooked," intelligence is worse than none at all. To succeed as a commander or policymaker, you must have good, objective intelligence. To get it, you have to make clear that's what you expect, fully realizing that it will sometimes clash with your own beliefs and established policies. In short, you can't get good intelligence unless you allow "academic freedom." At the same time, intelligence is only one of several considerations when you make decisions, and it's not infallible. There will be times when you disagree with intelligence. When that happens, feel free to challenge the analysts and ask tough questions. However, you should never order intelligence reports be *changed* to suit your own predispositions. And don't get a reputation for "shooting the messenger."

UNDERSTAND WARNING. Get a thorough briefing on your indications and warning system – it's important. Discuss potential surprise attack scenarios with **both** your planners and your intelligence analysts. Find out what's not known and may not be knowable, the missing pieces. Check to see if there's a mismatch between the timeliness of warning assumed in your contingency plans and what the analysts believe would actually be available. (There often is.) Finally, realize that if there really was going to be a surprise attack, there would be massive deception, a good deal of ambiguity and many skeptics.

ASK FOR PROBABILITY ESTIMATES AND DISSENTING VIEWS. Before accepting an intelligence estimate at face value, ask questions, especially if policy decisions are at stake. Talk directly to the *analysts* as well as the senior intelligence manager. Find out the underlying assumptions and logic. What were the minority views? And what probabilities do they assign to various possible outcomes?

CONSIDER WARTIME INTELLIGENCE POSTURE. For intelligence, the mission is now, and intelligence is primarily designed for peacetime. In the event of war, our intelligence infrastructure would be very vulnerable. While many shortcomings could be corrected, the

price would be high – in dollars as well as in reduced peacetime capabilities. The question of optimizing intelligence for peace, or making it more survivable during war, is important. The trade-offs are something **you** as a commander or senior policymaker should be considering now. It's a critical part of your command responsibility, and if war comes, it will be too late to redesign the intelligence infrastructure. Ask to be briefed on this issue.

DON'T OVER CONSUME CURRENT INTELLIGENCE. You and your headquarters need to know what's going on in the world, but you may not need a three-screen, technicolor extravaganza every morning of the week. Intelligence is expensive although the cost is often hidden. Over production of current intelligence inevitably means that some other intelligence product is being neglected. Maybe cruise missile targeting is falling behind, or perhaps order of battle or biographical files aren't being updated. Maybe you are getting *too much* attention while your action officers, planners and field units are being short changed. Those discrepancies won't show and probably won't matter – until there's a crisis, or a war.

DEMAND RELEVANCE AND BREVITY. Intelligence analysts, if they are really good, are likely to be the sort of people who are absolutely enamored with ideas and intellectual details. That's as it should be, but from time to time you may want to remind them to be focused and brief.

FINAL TIP: AVOID SECURITY VIOLATIONS. There really are "bad guys" out there doing their best to steal your secrets, penetrate your organization or compromise your personnel. Support your SSO and set a good example. Be especially careful of NOFORN and SCI, as well as the strict legal restrictions on counterintelligence, covert action and anything involving US citizens.

END NOTES

1. This essay was originally prepared when I was the DIA Representative at the National Defense University and was intended for classroom use. It is still being used at the National Defense University as well as at the Air and Naval War Colleges, Armed Forces Staff College, the Army Command and General Staff College, the Defense Intelligence College, the Naval Post-Graduate School, all three service Academies, and at other military schools and civilian universities. Earlier versions with the title, "Intelligence: A Consumer's Guide," were presented at the 1988 meeting of the American Political Science Association and published in *The International Journal of Intelligence and Counterintelligence*, Winter 1988. Dan Mozeleski, a CIA analyst and colleague on the faculty at the National War College, made many useful comments and suggestions on the early draft. While this paper has undergone Pentagon review to assure it contains no classified information, the particular view of intelligence and opinions given, and especially the advice for policymakers, are strictly my own.

2. Walter Laqueur, "Spying and Democracy: the Future of Intelligence," *Current*, March/April 1986, p. 34.

3. The descriptions and mission information that follow are extracted from Presidential Executive Order 12333, 4 Dec 1981, reprinted in the *Federal Register*, V46, N235, Tuesday, 8 Dec 1981, pp. 59941-59954.

4. Adapted from CIA brochure, *Fact Book on Intelligence*, CIA, Office of Public Affairs, September 1987, p. 20.

5. While this title does not formally exist, the function is very real and growing.

6. Stansfield Turner, *Secrecy and Democracy: The CIA in Transition*, Perennial Library paperback, New York, 1986. p. 92.

7. Herbert O. Yardley, *The American Black Chamber*, Bobbs-Merrill,, Indianapolis, 1931.

8. Frederick W. Winterbotham, *The Ultra Secret*, Harper & Row, New York, 1974. This was the first book in English to reveal in detail the SIGINT story of World War II. Many have followed, including works by Patrick Beesly, Peter Calvacressi, Francis Hinsley, RV Jones, Edwin Layton and Ronald Lewin. For an excellent review, see James Rusbridger, "Winds of Warning: Mythology & Fact about ENIGMA and Pearl Harbor," *Encounter*, V66, N1, January 1986, pp. 6-13.

9. President Carter made the first public acknowledgement of photo satellites on October 1, 1978, as part of his effort to secure ratification of the SALT II treaty.

10. Turner (note 6), p. 48.

11. Ibid., p. 59-60, 141 and 228.

12. E. Luther Johnson, "Current Intelligence," in Gerald Hopple and Bruce Watson (Eds), *The Military Intelligence Community*, Westview Press, Boulder, CO, 1986, pp. 117-127.

13. Arthur Hulnick, "The Intelligence Producer/Policy Consumer Linkage," in *Intelligence and National Security*, V1, N2, May 1986. p. 225. Hulnick relates current intelligence to warning; I see it as a separate service, or product.

14. Margaret Munson, *Intelligence for Operational-Level Commanders*. Student Research Report, National War College, Washington, DC, February 1987, pp. 25 & 30 (reproduced for use in courses at the National Defense University).

15. Stephen Andriole, "Basic Intelligence," in Hopple and Watson (note 12), pp 96-116.

16. Arthur Hulnick (note 13), p. 227

17. Bernard Grundy, "Scientifc and Technical Intelligence," in Hopple and Watson (note 12), pp. 99-116. Also, Margaret Munson (note 14), p. 10.

18. John Barron, *Mig Pilot: The Final Escape of Lt Belenko*, Reader's Digest Press, New York, 1980.

19. Timothy Lauer, "Principles of Warning Intelligence," in Hopple and Watson, (note 12) pp. 149-168. Margaret Munson (note 14), pp. 7-8.

20. Hulnick (note 13) p. 223

21. Lauer (note 19), p. 153-154. Seymour Hersh provides a vivid description of these mechanisms in his book on the shootdown of KAL 007; he also does a good job of portraying the use (or misuse) of intelligence by policymakers: *The Target is Destroyed*, Vintage, 1987.

22. When required in a classroom exercise to make their assumptions about future strategy explicit, most of the mid-level military and civilian officials who attended the National War College assume "timely and unambiguous warning will be available". This despite my arguments and their exposure to readings by Richard Betts, Michael Handel and other academic experts on surprise attack. Richard Betts, "Analysis, War and Decision: Why Intelligence Failures are Inevitable," *World Politics* 31, October 1975; also, "Surprise Despite Warning: Why Sudden Attacks Succeed," *Political Science Quarterly,* V95, N4, Winter 1980-81, pp. 551-572. Michael Handel, "Strategic Surprise: The Politics of Intelligence and the Management of Uncertainty," in Alfred Mauer, Marion Turnstall and James Keagle, (Eds), *Intelligence: Policy and Process*, Westview Press, Boulder, 1985, pp. 239-269.

23. Betts, 1980 (note 22). p. 555.

24. Ernest May, (Ed), *Knowing Ones's Enemies: Intelligence Assessment Between the Two World Wars*, Princeton University Press, 1984, p. 503.

25. G. Paul Holman, Jr., "Estimative Intelligence," in Hopple and Watson (note 12), p. 129.

26. Winterbotham (note 8).

27. Stephanie Neuman, "Arms, Aid and the Superpowers," *Foreign Affairs*, V66, N5, Summer 1988, p. 1054.

28. Stephen Beitler, "Counterintellience and Combatting Terrorism," in Hopple and Watson (note 12), pp. 169-196.

29. Ibid., p. 174

30. Foreign Intelligence Surveillance Act of 1978 (FISA), Public Law 95-511, 25 October 1978.

31. *Glossary of Intelligence Terms*, student handout, Defense Intelligence College, Washington, DC.

32. Turner, (note 6) p. 76. Also, *Report of the Select Committee To Study Governmental Operations with Respect to Intelligence Activities*, (Church Committee), US Senate, GPO, Washington, DC, (multiple volumes) 1975-76.

33. In this writer's opinion. Most militay intelligence officers would probably agree; some CIA officers might not.

34. See note 3.

35. David Charters, "The Role of Intelligence Services in the Direction of Covert Paramilitary Operations," in Mauer, Turnstall and Keagle (note 22), pp. 239-269; also, Turner (note 6) p. 175. Both Charters and Turner conclude that covert action should remain with CIA. See also, Steven Emerson, *Secret Warriors*, Putnam, New York, 1988.

36. Robert Gates, "The CIA and Foreign Policy," *Foreign Affairs*, V66, N2, Winter 1987/88, 216. Admiral Bobby Inman, another former DDCI, says that, at its height covert action involved less than 1% of the total Intelligence Community budget: "Foreign Policy Notes," *Institute of International Studies*, V1, N1, 12 Dec 1986, p. 1.

37. Edwin T. Layton with Roger Pineau and John Costello, *And I Was There*, William Morrow & CO, Inc. NY, 1985, p. 20.

38. Robert Gates, "The CIA and Foreign Policy," *Foreign Affairs*, V66, N2, Winter 1987/88, p. 228.

39. Comparisons of data from Meyers-Briggs personality tests administered to students at the National Defense University (policymakers) and to mid-level intelligence students at the Defense Intelligence College support this idea. See, John Macartney, "Intelligence and Bureaucratic Politics," paper prepared for the 1988 Meeting of the American Political Science Association, Washington, DC, September 1988.

40. This problem is especially acute in the Air Force where non-rated intelligence officers have to compete with pilots for limited promotion slots. Both the Army and Navy have separate intelligence corps with their own internal quota of promotions.

41. Robert Gates, "The CIA and Foreign Policy," *Foreign Affairs*, V66, N2, Winter 1987/88, pp. 215-230. Dr. Gates, former Deputy Director of Central Intelligence, writes that intelligence is now "poised nearly equidistant between the executive and legislative branches." A version of this article also appeared in *The Washington Post*, 29 November 1987, p. L1.