Bricks and Mortar for a Theory of Intelligence*

LOCH K. JOHNSON
University of Georgia
Athens, Georgia, USA

Intelligence may be thought of as three kinds of activities carried out by secretive agencies: first, the gathering, interpreting, and distribution of information (collection and analysis, for short); second, clandestine attempts to manipulate events abroad (covert action); and, third, the guarding against the hostile operations of foreign intelligence agencies (counterintelligence). This paper examines a core set of propositions about these activities that, taken together, point toward the outlines of a theoretical framework for understanding intelligence. The propositions and the evidence suggest that effective collection and analysis is, above all, a function of national wealth, but depends as well on focused targeting, all-source synergism, and good communication links ("liaison") between intelligence officers and policy officials. Successful, sustained covert action also relies on national wealth, and is a function in addition of modest objectives, weak targets, and the support of well-armed local allies. Successful counterintelligence requires national wealth and technical sophistication, along with an attitude of serious attention to security matters (which usually rises only after a major security breach).

Introduction

Strategic intelligence may be defined broadly as a set of activities conducted by government agencies that operate largely in secret. These activities include, foremost, the collection and interpretation of information drawn from a mixture of open and clandestine sources to arrive at a product—knowledge—useful to illuminate foreign policy deliberations. This is intelligence as narrowly and traditionally defined. Yet the secretive agencies do more: they also engage in covert action to advance a nation’s international interests by seeking clandestinely to manipulate events and conditions abroad. Finally, these agencies have a mandate to conduct counterintelligence operations designed to protect a nation’s citizens and secrets against attacks from hostile intelligence services and other threats.1

The prominent features of the discipline of intelligence studies have been outlined elsewhere.2 This analysis carries the effort toward theory-building further by crafting core propositions about intelligence and providing a preliminary assessment of their empirical validity. The purpose is to provide a sense of the dimensions that a theoretical framework must encompass—particularly with respect to the central issue of when intelligence is likely to succeed or fail. The objective is less to impart new knowledge than to lay out what we know in such a manner as to suggest next steps in theory construction.

Most of the “bricks and mortar” presented here are from the American experience, although the propositions are framed in such a way as to invite testing in other nations as well. An opening caveat is in order: reliable evidence is fragmentary and hard to come

*The author expresses his appreciation to Leena S. Johnson of the University of Georgia for editorial assistance, Harry Howe Ransom of Vanderbilt University, British intelligence scholar Michael Herman, and this journal’s reviewers for helpful suggestions, and my student assistant Ian K. Stoeppelwerth for his research support—none of whom, of course, are responsible for whatever errors may occur here.
by even in open societies; most of the relevant data remain classified and stored inside government vaults. The results presented are perforce more heuristic than definitive.

**The Intelligence Cycle**

Any theory of strategic intelligence must be built around the so-called intelligence cycle, a model that describes the flow of activities necessary for the collection and the interpretation (“analysis”) of information. The cycle consists of five phases: planning and direction, collection, processing, production and analysis, and dissemination (see Figure 1). Each step involves behavior that must be taken into account in any theory of intelligence.

In reality, the intelligence “cycle” is less a series of smoothly integrated phases, one leading to another, than a complex matrix of interactions among intelligence officers (the “producers” of intelligence) and the policy officials they serve (the “consumers”). This matrix—a composite of intricate human and bureaucratic relationships—is characterized by interruptions, mid-course corrections, and multiple feedback loops. Analytically it is useful, though, to consider the process as a sequences of discrete steps, moving seriatim from early deliberations over questions of intelligence targeting to the final distribution of information to decision-makers. This is how intelligence professionals conceptually think of their work.

**Planning and Direction**

In the first phase of the cycle, intelligence managers and policy officials must decide what data should be gathered from around the world. The goal is to provide the president and other top leaders with knowledge—ideally, foreknowledge—helpful for their policy deliberations, on the assumption that facts and insight are better than ignorance in charting a nation’s course. Two features of this phase are particularly notable: the choices made regarding the scope of collection, and the distortions that arise as a result of flawed
communications between intelligence professionals and decision-makers about the kinds of information that should be gathered.

Scope refers to the breadth of intelligence tasks assigned ("tasked") by policy officials. Large, affluent nations with extensive international commercial transactions, widespread political alliances, and worldwide rivalries are likely to want a far-flung network of intelligence capabilities, in the form of agents ("assets") on the ground (human intelligence or "humint") as well as machines that can listen and watch from land, sea, or air (technical intelligence or "techint"). This breadth of coverage allows, for those fortunate nations (or groups) that can afford the luxury, a good chance of acquiring valuable "heads up" information about world affairs—information that lies far beyond the reach of the less affluent.

During the Persian Gulf War (1991), the United States enjoyed a remarkable battlefield transparency in Kuwait and Iraq, thanks to its extensive fleet of surveillance satellites and reconnaissance aircraft, while the Iraqi forces gathered information largely on foot in the deserts—not much differently than their ancestors had a thousand years before. Superior battlefield awareness explains much of the dramatically disproportionate casualty rates that favored the United States during this conflict by a ratio of some 1,000:1 (or as high as 3,000:1, according to some estimates).

In a paradox, though, well-heeled nations with behemoth intelligence services are also likely to suffer acute information failures. Because of the breadth of their concerns, not even expenditures in the range of $35 billion a year (the widely reported figure for U.S. intelligence in 2002–2003) can offer transparency for the entire globe—especially when adversaries choose to conceal their schemes and weapons systems in deep underground caverns, with camouflage, or by other methods of stealth to avoid the prying lens of satellite cameras orbiting above them. In contrast, the intelligence objectives of smaller nations are much more limited, say, to a single region or even a solitary enemy. Some may view this paradox as self-evident, but comparisons of the intelligence systems of different countries are often made without taking into account the differences in their funding abilities and targeting needs.

Consider the intelligence focus of the United States compared to New Zealand, or even Israel in its hostile setting. America’s intelligence failures have been extensive in recent years, including (most painfully) the terrorist attacks on the World Trade Center and the Pentagon in 2001, the mistaken targeting of the Chinese embassy in Belgrade in 1999, and the inability to find the Iraqi leader Saddam Hussein in 1991, the Somali warlord Mohamed Farah Aidid in 1993, or the Al Qaeda leader Osama Bin Laden in 2001–2002. While New Zealand may falter from time to time in its efforts to track illegal Japanese fishing for albacore tuna in its seas, and Israel may suffer the more hurtful inability to anticipate the next suicide bombing, the tasks of the intelligence services in these smaller nations are much more focused and manageable. As a result, the percentage rate of success for a given list of targets is apt to be better for smaller nations with a concentrated threat assessment than for a wide-ranging great power—although the more focused nations are hardly immune from major failures either, as when Israel reeled from the rash and unanticipated Egyptian attack on its territory at the onset of the Yom Kippur War in 1973.

In the form of a general proposition (P), we can say:

\[ \text{P1. The more affluent and globally oriented a nation, the larger its agenda of intelligence objectives and its institutional apparatus for espionage, and the more likely its chances for a large number of successes as a result of this saturated world coverage.} \]
P2. Yet, paradoxically, the more affluent and globally oriented a nation, the more it is apt to experience intelligence failures as well, because its broader global objectives cannot be completely satisfied in a world that is too large and complex for full transparency.

At the very beginning of the intelligence cycle, a basic difficulty often arises that distorts all the subsequent phrases: policy officials are unable or unwilling to articulate clearly their intelligence priorities. This happens for a number of reasons. Some officials do not know much about intelligence as a resource and, therefore, fail to use it properly. “I need information about Burundi,” for example, is too diffuse an intelligence request to elicit the precise data required to address a specific policy problem that may have arisen with respect to that African nation.

Or, in some cases, officials believe that their own personal sources of information (whether the New York Times, club colleagues, or visits with foreign dignitaries) are better and more timely than the sometimes sluggish responses of large bureaucracies like the Central Intelligence Agency (CIA) or its thirteen sister agencies that comprise the U.S. “intelligence community.” In other cases, the policy makers may simply be too harried to find time for consultation with intelligence professionals. Moreover, at times those in high office wear ideological blinders that cause them to eschew any information that fails to fit comfortably into their policy preconceptions, or that contradicts a decision or speech they made just last week.

P3. To the extent that policymakers focus and clearly delineate their foreign policy objectives and informational needs, the chances for intelligence collection successes correspondingly rise.

Collection

Once a nation’s leaders communicate to intelligence managers their intelligence requirements, however imperfectly, this “tasking” must be translated by the managers—in the United States, the Director of Central Intelligence (DCI) and subordinates—into specific targets: nations (civilized or rogue), terrorist cells, drug cartels, multinational corporations, individuals (“bad actors,” like Bin Laden), or some topic of interest, say, the efficiencies of Russian rocket fuel. The managers must decide, too, what methods (“tradecraft”) will be used to gather the information.

Every new administration in Washington, D.C., goes through a “threat assessment” exercise in which a list of priority intelligence targets is developed. The list, a tableau of friends and foes, is subject to rapid alterations as fresh threats suddenly arise: Burundi today, Rwanda tomorrow, Somalia the next day—each of these particular crises (“flavors of the month”) unanticipated by the Clinton administration. Mostly, though, the list is fairly easy to predict and, even though the threats are highly classified, the average history or political science major could guess what they might be, since—logically enough—the list concentrates on those nations and groups that can cause the most harm to the United States or its interests abroad. Russia, one suspects, is likely to have a reserved spot on the list despite the end of the Cold War, for the simple reason that its missiles can still destroy the United States in thirty minutes, in the witch fire of a nuclear holocaust. This capability draws one’s attention. Other nations known or suspected to have nuclear, biological, and chemical (NBC) weapons, coupled with a history of tension with the United States, are duly accorded prominence in the threat assessment. So are non-state
Bricks and Mortar

groups that blow up American embassies, ships, and military barracks, or fly planes into skyscrapers and government buildings. Generally, then:

P4. The greater a perceived threat (especially military, but also political and economic) from a nation or group, the greater the amount of intelligence collection resources that will be dedicated against that threat—although unanticipated crises frequently divert resources from the formal list of threats.

Even affluent nations will fall short of achieving perfect global transparency, since the world is large and adversaries and competitors are many. The intelligence services of rich nations with superpower aspirations are likely to pursue a policy of “global presence,” that is, having permanent assets in most of the world’s countries; poorer nations will have to settle for a more limited reach, relying on a policy of “global surge,” that is, sending assets temporarily into a new area of the world that has flared up (to the extent a nation has an interest there and intelligence assets to deploy). Even nations with extensive intelligence capabilities must sometimes resort to a policy of global surge, as when Rwanda and Somalia (where the United States had few assets) suddenly became important during the Clinton administration, then just as quickly faded off its radar screen. Global presence is a more effective approach, because it allows a nation to establish over time a reliable ring of spies and to put into place technical surveillance hardware. In contrast, sending assets and their CIA handlers (“case officers”) into a location unfamiliar to them, moving satellites into new orbits, and flying reconnaissance airplanes over unfamiliar territory is more difficult—and often too late and ineffectual.

P5. Affluent nations with great power aspirations will seek an intelligence policy of global presence; but, since resources are finite even for the affluent, they will rely on a global-surge capacity for regions of the world that are considered less threatening.

Affluent and poor nations alike, but especially the latter, will have gaps in their collection capabilities. These gaps may be a result of failing to properly identify emerging interests or threats, or an insufficient dedication of intelligence resources to the region in question. Even if the threat assessment has been accurate and the financial resources are available to purchase the desired intelligence coverage, the nation may have too shallow a pool of potential case officers who can live abroad in the places of interest and effectively recruit indigenous assets. Successful recruitment requires the development of rapport between a case officer and a potential agent, which in turns means the case officer must speak the local language and know something about its culture and mores. The United States has a dearth of case officers with Middle East or South Asia training and, in order to track and eradicate terrorist cells in those regions, its intelligence agencies have sought recently to bolster the hiring of American citizens with the requisite skills and knowledge—notably young Arab-American citizens with Middle Eastern and South Asian language abilities and unquestionable loyalty to the United States.

P6. A nation—however affluent—may suffer from a lack of well-trained case officers with strong foreign language and cultural skills and, as a result, will have limited success in recruiting assets in some parts of the world.

As for tradecraft, technical intelligence works a special magic within the inner sanctums of Washington, D.C., where decisions are made about questions of modus operandi. When intelligence briefers visit Capitol Hill, the National Security Council (NSC), or
budget analysts in the Office of Budget and Management, they come equipped with impressive photographs of foreign military bases snapped by U.S. satellite cameras (imagery intelligence or “imint”); with fascinating design renderings of the shiny, metallic “birds” themselves, orbiting deep in space; additional photographs of unmanned aerial vehicles (UAVs, like the low-altitude, rocket-equipped Predator used in the anti-Taliban war in Afghanistan and to hunt down suspected terrorists in places like Yemen); and accounts of successful telephone and e-mail intercepts, compliments of the technical services of the CIA and the National Security Agency (NSA). Audiences are impressed, as well they should be. During the Cold War, America’s intelligence machines watched the military activities of the Soviets, allowing great confidence in Washington that Moscow’s armies, bombers, and missiles could not be used against the United States in a successful surprise attack—an invaluable, reassuring capability both then and since.

In comparison, human intelligence comes across in briefings as mundane. The identities of assets must be kept a tight secret; no slide shows to dazzle legislators. And even though humint has scored some remarkable successes, as when documents given to the CIA by Soviet agent Col. Oleg Penkovsky helped to detect the presence of the Soviet missiles in Cuba in 1962, during the missile crisis, few of the hundreds of humint reports provided accurate information about the presence of Soviet missiles. Worse still, throughout the Cold War, local counterintelligence authorities doubled every CIA asset in Cuba and in East Germany and sent them back against the United States to sow disinformation.

So in the inner councils of intelligence planning and funding, techint has drawn more favorable attention; machines neither lie nor come down with the flu and miss two weeks of work. Yet, satellites and reconnaissance aircraft have their weaknesses, too. Imagery intelligence is most effective in identifying the capabilities of an adversary (how many missiles does he have?), rather than his intentions (will he fire those missiles and, if so, exactly when?). Cameras on satellites and UVAs cannot see through mud hut roofs or into the labyrinth of caves where Al Qaeda terrorists may still be hiding in Afghanistan or Pakistan, or into the vast caverns in North Korea where the government of P’yongyang is thought to be constructing weapons of mass destruction. This takes a human agent. In addition, nations and terrorist cells have become more clever at avoiding the scrutiny of satellite cameras, timing their orbits and using camouflage to conceal their activities on the ground.

The NSA’s signals intelligence (“sigint,” such as telephone taps) can be an important techint source of information about intentions, although adversaries will sometimes use this channel for disinformation and sigint intercepts must be used gingerly. Moreover, adversaries have begun to use more advanced encoding devices for their telephone, fax, and e-mail communications, and have turned to new technologies (like fiber-optic telephone cables) that—for the time being at least—greatly complicate the challenge of intercepting sigint. These technical problems notwithstanding, intelligence “hardware” consistently attracts a preponderance of the total expenditures for spying.

Looking more broadly at intelligence resources, the U.S. example suggests that national spending on espionage operations by affluent nations will occur at the rate of about 10 percent of the total defense budget—although data on this subject is hard to acquire, even in open societies.

P7. In the collection of intelligence, techint will be strongly emphasized by nations that can afford it, while poorer nations will be more restricted to humint.

P8. In the United States, intelligence activities attract resources at the rate of approximately 10 percent of the funds dedicated to overall defense spending.
Collection failures occur, too, because of a tendency by some nations to place their case officers inside the limited confines of their embassies overseas, giving them an identity (“cover”) as diplomats or military personnel—so-called “official cover.” By all accounts, these spies are relatively easy for local counterintelligence services to identify. Moreover, case officers under official cover are often content to limit their information gathering to the embassy cocktail circuit. To some extent this approach succeeded during the Cold War, since Communist diplomats and spies attended embassy parties and could be courted (in hopes of recruitment to the Western cause); members of Al Qaeda, though, are unlikely to be part of the embassy cocktail circuit.

More successful than official cover for most countries has been the use of individual spies operating outside the embassy, employing non-official cover (thus, the acronym NOC, pronounced “knock”), say, as a bartender, oil rigger, or freelance writer. These assets blend into local society more effectively and, unlike government officials abroad, are not automatically suspected as spies.

**P9.** Nations employing a system of non-official cover will have more success in gathering intelligence abroad than those relying on official embassy cover.

Another method used by nations to fill in their intelligence gaps is the development of liaison relationships with foreign intelligence services. The classic example is the espionage cooperation between the United States and the United Kingdom, which has led to a high level of information sharing. The British benefit from U.S. imagery intelligence and the United States is pleased to receive from its “cousins” information based on the U.K.’s humint networks that extend back to the days of empire (along with the first-rate sigint and code-breaking abilities of Her Majesty’s Secret Service). While a helpful addition to one’s own collection activities, foreign intelligence liaison is treated cautiously; after all, the interests of one’s ally are rarely fully congruent with one’s own. Moreover, too much sharing might reveal technical tradecraft that might be used against the home nation one day by an erstwhile ally.

**P10.** Nations resort to intelligence sharing with allies, but only with a sense of ambivalence and caution, less than full cooperation, and a realization that today’s partner can become tomorrow’s competitor.

Affluent nations (or at least those that are militarily powerful and have global interests) have displayed since the end of the Cold War a willingness to move beyond narrow “realist” pursuits to define their interests more broadly in terms of international humanitarian objectives as well. Intelligence tradecraft has been relied upon to provide evidence for international judicial proceedings against war criminals, as when U.S. satellites detected the mass graves of Bosnians slaughtered by Serbian paramilitary troops in the 1990s or when an American-piloted U-2 aided searches conducted by the United Nations for weapons caches in Iraq following the Persian Gulf War. Slowly, more intelligence sharing is beginning to take place, not just between close allies but less friendly countries, too, and even international organizations, as nations are drawn together by a common interest in thwarting terrorism and other worldwide threats.

**P11.** As the world moves further toward globalization, intelligence services are increasingly targeting nations or other entities that threaten the common good and sharing information with a wider set of coalitions than usual, including international organizations.
Processing

Information collected by intelligence agencies is often in a form decision-makers would find unreadable. The tiny black-and-white squiggles on satellite photographs require an expert eye to ferret out the specifications of weapons systems and other valuable data; the Farsi telephone transcript and the Chinese military manual must be translated into English. This process of conversion can be daunting, as satellite photos pour into the National Reconnaissance Office (NRO) in Virginia at the rate of 400 hundred a day and a steady stream of sigint and humint reports inundate the NSA and the CIA. The processing of this information cannot keep up with the incoming volume and a majority of the data must be stored for later “mining,” should its subject matter become of particular importance to policymakers.

P12. In affluent nations that collect large volumes of secret information from around the world, the processing of this information will lag far behind ongoing collection, leading to an extensive warehousing of unexamined data.

Analysis

Intelligence seldom speaks for itself; it must be interpreted by smart, well-trained people who understand the country, group, or topic at question. This effort at analysis (“assessment,” in the British phrase) amounts to a search for insights into the meaning of “raw” or unevaluated data. Information collected overseas by intelligence assets and machines must be placed into the context of what the analyst knows or can learn from public sources, whether archives at the Library of Congress, the Internet, or the Washington Post. Once the analyst mines this open-source intelligence (“osint”), he or she can then supplement this broad framework of understanding with “value added” information derived from clandestine sources. In this sense, analysts proceed in the manner of academic researchers, with the additional step of integrating secret sources of data into their work. These extra “nuggets” may (or may not) add value to the findings that a university scholar could just as well provide to the president, based on a scouring of sources in the campus library or on the Web.

P13. The overwhelming percentage of information in intelligence reports comes from open-source searches, augmented by a small percentage of clandestinely derived data.

Even though osint is predominant in intelligence reports, the secret add-ons are sometimes of great significance. On occasion, intelligence assets have access to data that newspaper correspondents, scholars, and others writing on world affairs simply do not have, especially with respect to terrorist organizations, the political and military machinations that occur within closed societies, and the specifications of weapons systems possessed by foreign regimes. Conversely, at times, writers in open organizations—like the media and the academy—may have information sources superior to the intelligence agencies, as when a journalist or a scholar has spent years in a foreign nation and knows its culture, language, and politics inside out (unlike most U.S. intelligence officers, who rotate frequently from one country to another). That is why a blend of osint, techint, and humint—what the professionals call “all-source” intelligence—is vital and can produce important synergies.
P14. A blend of the intelligence “ints”—osint, humint, techint—produces valuable “all-source” synergies, leading to a more complete understanding of world affairs.

P15. Clandestine collection is particularly important for the information it provides about terrorist organizations and activities, events and conditions within closed regimes, and the capabilities of foreign weapons systems.

In a similar fashion, interagency cooperation (not just a blending of all-source tradecraft within separate agencies) usually leads to a more complete picture than reliance on any single agency. In 1947, President Harry S. Truman created the CIA in response to the intelligence disaster at Pearl Harbor. This failure stemmed in part from a lack of coordination among U.S. intelligence agencies. By establishing a Central Intelligence Agency, the President hoped to bring about better integration of the secret agencies and a more fused intelligence product that would assemble in a timely manner all of the pertinent information the White House needed to make an informed decision. The supposition was that many “heads” (agencies) could think better than one, and that their findings—including dissents—should be presented to policy officials in a coherent whole: one-stop shopping.

P16. In contrast to a loose confederation of secret agencies, their close institutional integration increases the chances of full reporting and, therefore, the delivery of more comprehensive information to policy officials.

The integration of a nation’s espionage resources requires, though, a strong intelligence manager with authority over spending and personnel for each secret agency in the government. Instead, in the United States, the intelligence “community” remains a loose confederation. Nine agencies are organizationally wired to have dual supervisors: the DCI and the Secretary of Defense. The Sec Def dominates this relationship, in part because of his higher status as a member of the NSC. Even more significant are the Pentagon’s longstanding ties to the congressional defense and appropriations committees, which give the Sec Def great leverage over intelligence spending on Capitol Hill (since funding decisions for intelligence are not made by the Intelligence Committees alone, but in conjunction with these other congressional panels).

Four other agencies also enjoy the protection from control by the DCI afforded by reporting as well to such luminaries as the Secretaries of State, Treasury, and Energy, and the Attorney General. The only agency over which the DCI supposedly has full authority is the CIA in Langley, Virginia, where his office resides. Yet even this Agency’s component directorates have proven resistant to control from the Director’s aery on the seventh floor. This absence of institutional integration has interfered with the all-source intelligence fusion envisioned by President Truman.

P17. Generally, in the absence of full authority for an intelligence director over a nation’s cluster of secret agencies, the institutions of the “community” will exhibit strong centrifugal forces that lessen the degree of interagency cooperation and comprehensive intelligence reporting to policy officials on both military and civilian topics.

And an important corollary in the United States:

P18. A nation’s defense secretary will attempt to dominate intelligence resources for military purposes, resisting efforts that might lead to greater civilian (DCI) control and better civilian–military analytic synergism.
This tilting of intelligence toward military concerns, understandable in time of war, has the effect in peace time of weakening diplomatic intelligence (political, economic, cultural) that might help ward off the outbreak of war or terrorist attacks in the first place. In light of the DCI's difficulties in gaining formal control over all of the secret agencies in the United States, the Director is likely to seek less formal means for bringing about greater institutional integration, informational synergism, and a better balance between military and civilian intelligence priorities.

_P19._ To improve the degree of coordination and synergism in the intelligence community, as well as to bring about more of a civilian focus to intelligence priorities, DCIs will resort to the establishment of informal institutional arrangements, such as special integrative task forces and centers that draw together personnel on temporary assignment from throughout the community.

Whether a president or a prime minister, a dictator or a king, leaders want to know about threats to their regimes, as well as opportunities for advancing their interests. Ideally, they hope to be forewarned by their intelligence services about every twist of fate. For better or worse, though, the gift of clairvoyance lies beyond the ken of human beings. Intelligence officers confront a world of secrets and mysteries. The secrets they may discover, with good tradecraft and some luck: information like the number of Russian ICBMs (from NRO imagery) or the fallback position of Japanese automobile negotiators (from NSA intercepts). In contrast, mysteries—events and conditions that elude empirical verification—can defy the best efforts at collection and analysis. Who will succeed President Vladimir V. Putin in Russia? How long will Al Qaeda remain an attractive career option for disenchanted Muslims?

Even with respect to secrets, all the pieces of the jigsaw puzzle are rarely found; the analyst must try to discern the full picture from the few parts he or she may have acquired from osint, humint, and techint sources. Moreover, the fragmentary evidence is often filled with contradictions (“noise”), forcing the intelligence professional to make hard choices that move analysis into the realm of speculation.

The best an analyst can hope for is reasonably complete and reliable data about secrets, which must then be augmented with educated guesses about the world’s mysteries. Given humankind’s “incapacity to pierce the fog of the future,” intelligence analysts will always be subject to failure—an existential reality of espionage.11

_P20._ Since data about secrets are rarely complete and since humans are unable to predict the future (mysteries), intelligence analysts will fail from time to time in their efforts to anticipate and comprehend the meaning of world events.

Good analysis depends on having a stable of well-educated minds—Ph.D.s and others with special skills, whether individuals who speak Pashto and have a deep knowledge about the politics, economics, culture, and military affairs of places like Afghanistan, or scientists with insights into global disease surveillance or the effects of radiological bombs. Such training is expensive and not all nations have the luxury of drawing on the wellspring of a well-educated populace for the recruitment of intelligence analysts.

_P21._ The more affluent the nation and the more extensive its global interests, the greater its pool of potential intelligence recruits with advanced training in world affairs.

Even affluent nations will have trouble tapping into expertise for the whole planet, especially nations like the United States and Australia that are removed by oceanic moats
from close proximity to other continents with a diversity of languages and cultures. Rela-
tively isolated nations, however affluent, will find themselves deficient in knowledge
when it comes to many corners of the globe, especially territories that have not tradi-
tionally posed a threat to them. Such has been the case with the United States in its
recent wars in the Middle East, the Balkans, and South Asia. This liability of distance
from Europe and Asia (though often a blessing in the nation’s history) was mitigated to
some extent with respect to the Soviet Union during the Cold War, as Washington poured
massive intelligence resources into learning about the well-armed Eurasian power.

Even affluent nations with global aspirations will display gaps in their col-
collection and analytic capacities, until sufficient new resources are dedicated to
overcome the knowledge deficits.

Intelligence analysis has been charged by some critics as being too often an exercise in
crying wolf. Military analysts are notorious for portraying their adversaries as ten
feet tall, armed to the hilt, and ready to storm the home front at any moment—the
“worst-case” scenario. “The armed services always want more funds than are available,”
notes intelligence scholar Harry Howe Ransom, “producing a tendency to exaggerate the
threats to each of the armed services separately.” The end result of too many worse-case
scenarios is a mushrooming intelligence budget based on ungrounded speculation about
the supposed strength of an enemy.

Military intelligence analysts are inclined to exaggerate the nature of the threat.

Sometimes an analyst will succumb to a different temptation, known as “politiciza-
tion,” that is, putting a spin on or “cooking” intelligence to serve the political needs or
beliefs of an intelligence manager or policy official—“intelligence to please.” Rejec-
tion of the honored intelligence tradition of objectivity is a cardinal sin of the profession.
British scholar Michael Herman has observed that politicization is rampant in authoritar-
ian regimes. “Despite its collection successes, Soviet intelligence selected and interpreted
its material to suit the preconceptions of the regime of which it was an integral part,”
he writes, “and encouraged misleading estimates of Western intentions.” This happens
from time to time in democratic regimes as well, but a stronger sense of professional
ethics seems to tether intelligence analysts in open societies closer to the norm of objec-
tivity.

Intelligence can become politicized in democratic regimes, but because of the
countering influence of professional integrity this happens far less frequently
than in authoritarian regimes.

Dissemination
The best intelligence reporting in the world would not be worth much if it remained
bottled up within the secret agencies; it must make its way into the hands of the men
and women who make decisions, or become nothing more than a “self-licking ice cream
cone.” This end stage is often the most difficult step in the intelligence cycle because
the information must have certain key attributes before it will be appreciated and used
by policy officials.

First, the finished intelligence must be relevant. If it fails to help extinguish fires that
have flared up in the policymaker’s in-box, it will be shunted aside. Incisive reporting
on political elections in Estonia has its place; however, what the White House really
wants to know about is the location and the plans of Al Qaeda leaders, the nature of
weaponry in Iraq and North Korea, and how Turkey and Iran are likely to respond to a U.S. invasion of Iraq. Timeliness is equally vital. The worst acronym an analyst can see scrawled across his intelligence report is OBE—"overtaken by events." Further, the importance of accuracy is self-evident in the information business. Once proven irrelevant, late, or unreliable, intelligence officers will find it much harder to gain access to decision councils in the future.

A corollary of this proposition has to do with intelligence liaison inside the Washington Beltway (as opposed to foreign intelligence liaison). If the secret agencies have liaison personnel assigned to the various policy departments in the government, these individuals can attend staff meetings and be a part of the informal hallway or watercooler discussions about policy concerns (what intelligence officers jokingly refer to as "rumint"—rumor intelligence). At the close of business, they can return to their respective agencies (CIA, NSA . . .) to inform analysts more confidently about what kind of information is most needed by policymakers the next day.

P25. If intelligence is irrelevant to current crises, or if it is late or inaccurate, it will be ignored by policy officials, with a concomitant diminishment of access for intelligence officers to key decision councils.

P26. Intelligence agencies with a liaison team in a policy department or agency will be in a better position to provide relevant and timely information to inform policy deliberations.

At the end of this intelligence pipeline, policymakers have often been more responsible for "intelligence failures" than the secret agencies. Just as at the very beginning phase of planning and direction, office holders at this last stage sometimes display distorting ideological or political biases against information that may be disagreeable. Or they may be too busy, or arrogant, to read intelligence reports; speaking truth to power is notoriously difficult, because power often refuses to listen.

P27. Policymakers will sometimes ignore intelligence reports, no matter how relevant, timely, and accurate, because the reports may fail to pass an ideological litmus test; or because policymakers are too busy to read the reports, or deem themselves already sufficiently well-informed.

Further, policymakers may never act on important intelligence assessments, because the policymakers have too many other concerns to consider or may decide that taking action might be too difficult or expensive. As early as 1995 (six years before the airplane attacks against the World Trade Center), the CIA's Counterterrorism Center was reporting to high-level policymakers that "aerial terrorism seems likely at some point—filling an airplane with explosives and dive-bombing a target."16 Yet nothing was done to improve airport security or to monitor individuals in the United States receiving flight training.

P28. Policymakers may ignore important intelligence findings, because acting on this information is perceived as too difficult or expensive, or because the information is crowded out by other pressing concerns.

**Covert Action**

Intelligence agencies have a more aggressive mission called covert action, the secret manipulation of events abroad to advance a nation's interests. Its primary forms are propaganda, political and economic action, and paramilitary operations. These clandestine activities can include, respectively, planting stories in foreign media outlets, bribing
politicians overseas, sowing economic disruption, and providing weapons to a favored
side in a civil war.

Presidents often find covert action an appealing “quiet option,” less noisy than send-
ing in the Marines and quicker than the glacial pace of diplomacy. For the United States,
covert action led to quick successes (at least over the short run) in Iran in 1953 and
Guatemala in 1954, where anti-U.S. regimes were easily toppled and replaced with
friendly dictators. The supply of shoulder-held Stinger missiles to the mujahideen in
Afghanistan for their war against Soviet invaders (1979–1989) also produced, over the
short term, a useful outcome for the United States (though this intervention was more of
an “overt-covert action,” closely covered by the media).

Presidents are persistently drawn to covert action (the “Third Option” between
Marines and diplomats)—even those, like Jimmy Carter, who railed in presidential cam-
paign rhetoric in 1976 against this approach as a corruption of American foreign policy.
Covert action is particularly appealing to presidents engaged in an ideological or mili-
tary struggle against an aggressive global competitor. Carter turned to this instrument of
foreign policy when the U.S.S.R. invaded Afghanistan; and, throughout his two terms
in office, President Ronald Reagan employed covert action against the Soviet “evil em-
pire” as it intruded into the developing world (a response labeled the Reagan Doctrine
by the media). American presidents who find themselves more free of major military
provocations or ideological confrontations overseas are inclined to leave covert action on
the shelf. Presidents may also, Ransom suggests, turn to covert action when no national
consensus exists for open military intervention against a target.17

P29. Covert action is used most frequently by presidents engaged in an ideological
or military struggle against an adversary, or when no national consensus exists
for open intervention.

Money is a consideration, too, since covert action can be costly—especially major,
long-term paramilitary operations. In Laos, the CIA and its local Hmong (Meo) assets
fought a secret war for a decade (1963–1973); and the supply of weapons to the contras
in Nicaragua and the mujahideen in Afghanistan kept Uncle Sam’s cash register ringing
during the 1980s. Only a well-to-do nation can undertake such sponsorships, although
the successful paramilitary attack against New York City and the Pentagon in 2001 by
the Al Qaeda organization demonstrates that extensive short-term damage can be inflicted
against a target without much financial cost. More prolonged covert actions, however,
are expensive.

Even with the money to support significant covert actions, most will be successful
only within modest parameters. Successes are most likely to occur when a targeted regime
is weak to begin with (as in Iran in 1953 and Guatemala in 1954); when paramilitary
surrogates are dedicated, experienced fighters with widespread indigenous support (as in
Laos or in Afghanistan in 2001–2002); or when a quick, dramatic use of paramilitary
force is carried out against civilian or military targets (like the terrorist strikes against
the United States or the U.S.S. Cole in the Yemeni port of Aden, also in 2001).

P30. Affluent nations can afford to conduct more extensive covert actions than poorer
nations, especially when it comes to major paramilitary operations—although
even weak states or groups can inflict considerable damage through surprise
paramilitary attacks.

P31. Major covert actions (and especially those with a paramilitary component)
conducted over a longer period of time are most likely to succeed when a
target regime is weak and when local paramilitary surrogates are dedicated,
experienced fighters with indigenous support.
Counterintelligence

The third core mission of intelligence agencies is the protection of their nation against hostile intelligence services and other enemies of the state, a practice called counterintelligence. The defensive side of this mission depends on barbed wire fences around agency buildings, patrolled by armed guards; polygraph tests; identification badges; and encoded communications. Counterintelligence has an offensive side, too: the penetration of the opposition with a mole of one’s own, to discover what operations the enemy has running against the homeland and to foil his attacks. Again, money is important. Sophisticated telephone and personal computer safeguards are costly, as is the wide gamut of defensive barriers from fences to well-trained security guards. Yet, even wealthy nations have experienced counterintelligence failures, such as the Cambridge spy ring in England or the cases of Ames (CIA), Hannsen (FBI), and the Walker family (Navy Intelligence) in the United States. When failures come to light, investigations are carried out and counterintelligence is usually provided additional resources to enhance security.

P32. The more affluent the nation, the less porous its counterintelligence defenses.

P33. Some counterintelligence failures are inevitable; but their frequency is likely to decline in the aftermath of a major security breach, because of a nation’s efforts to tighten its defenses.

Intelligence Oversight

A theory of intelligence must take into account efforts to maintain supervision over the conduct of secret operations, at least in those few open societies where accountability has been attempted in this hidden domain. Even in the United States, which has given intelligence oversight the most attention, the experiment is of relatively recent vintage. From 1789 until 1975, America’s intelligence agencies were considered a separate government whose sensitive operations could not be subjected to the normal checks and balances of the U.S. Constitution. Improper domestic spying led to a scandal in 1974, however, which produced strong pressure to bring the principles of accountability into the secret side of government.

P34. Intelligence scandals, especially if they involve domestic spying, stimulate efforts to establish greater accountability over secret agencies.

Short of a scandal, the vigor with which intelligence accountability is carried out will be related to the degree of consensus behind a nation’s foreign policy; and that consensus is likely to be highest in times of perceived external threat. The efficiency of a nation’s war and espionage capabilities are of greatest concern in times of danger, with questions of civil liberties and the close legislative supervision of intelligence a secondary consideration as the nation rallies behind its leader and the executive branch of the government in times of peril. In contrast, during periods of normalcy a nation (if it enjoys basic freedoms) will be more inclined to engage in vigorous debate about policy directions, allow criticism of its chief executive, and concentrate on the safeguarding of civil liberties and democratic procedures.

The political science literatures reminds us, though, that the legislative supervision of executive branch agencies can fail even during times of normalcy, as a result of co-optation. Over time, lawmakers become the advocates and protectors of the very agencies they are meant to oversee.
P35. In times of military crisis, a nation tends to rally behind its leader in favor of an efficient response to the threat, placing at a lower level of concern questions of civil liberties and intelligence accountability.

P36. Over time, intelligence oversight committees are apt to become co-opted by the agencies they are assigned to supervise.

Although in the United States some intelligence officers initially looked with horror on the prospect of having to submit to normal governmental oversight procedures, most DCIs since 1975 have come to appreciate the new partnership with Congress in sharing their weighty responsibilities. (William J. Casey, 1981–1987, is the exception.) They have also expressed few concerns about the diminution of intelligence effectiveness as a result of the new oversight procedures. Moreover, although intelligence oversight has displayed some of the usual weaknesses of co-optation, some legislators have take accountability seriously and provided a check on many (if not all) misguided initiatives. The executive “energy” that Alexander Hamilton extolled remains important in government and especially within the national security domain; but, as James Madison countered at the founding, safeguards against the overzealous use of executive power is even more vital.

P37. Nations that have experimented with procedures for greater intelligence accountability have found that this approach allows some semblance of policy debate and a healthy “look over the shoulder” by elected representatives—in a word, the advantages of democracy in providing a check on ill-conceived intelligence initiatives.

Preliminary Evidence

Most of the data needed for a rigorous test of these propositions are locked up in government vaults. Given this situation, one must resort to the only possible remedy: sifting through the public literature, which is both voluminous and often unreliable, and interviewing officials involved in intelligence work. Based on this evidence, only limited findings may be offered regarding the propositions presented here.

The Intelligence Cycle Propositions

Planning and Direction. The opening propositions underscore the difficulties of measurement in this field (no doubt one reason why many scholars have steered away from intelligence as an intellectual pursuit). We don’t really know details about the size, the successes, and the failures of intelligence agencies around the world to either confirm or reject the propositions with confidence. Yet we do know some things that raise doubts about the posited relationship between national wealth, the size of intelligence communities, and their performance (P1, P2). Russia is reported to have one of the largest intelligence services, but one could hardly call Russia affluent. Rather, to protect and advance its international interests, Moscow has been prepared to spend its limited resources on a vast information gathering empire—one it has tried to sustain since the end of the Cold War, despite economic difficulties.

Moreover, the degree of success enjoyed by intelligence services does not necessarily depend upon national wealth. Israel is poorer than many industrialized nations, but the success of its premier intelligence service (Mossad) is legendary. When a nation is under daily mortal threat, its intelligence services must be successful—or the nation will perish. Norway illustrates another exception to the wealth proposition. This small nation has
an elaborate, costly intelligence capability, especially with respect to the monitoring of military operations and training carried out by the Russians and others in the Barents and Norwegian Seas—affordable to the Norwegians because the United States substantially subsidizes the effort in exchange for access to the intelligence data. But despite some exceptions, national affluence is definitely a plus and the United States has enjoyed many intelligence successes as a result of its expensive and sophisticated global coverage of events. It also appears true that affluent nations with global aspirations (if only for the purposes of improving their international trade relations), build large information gathering agencies in search of early warnings about threats and opportunities as they reach out around the world. As the U.S. example suggests, intelligence failures occur with some frequency as aspirations for global transparency fall short.

As for the frequency of intelligence success rising with the clarity of tasking (P3), the author’s interviews with intelligence officers over the past quarter century suggest this to be the case. The CIA’s case officers have often expressed exasperation over the ambiguity of the information requests coming from both Republican and Democratic administrations. “What’s going on in Nicaragua?” is not a very useful intelligence question, yet that level of abstraction is commonplace.

The posited relationship between perceived threat and resources seems to hold true (P4). During the Cold War, the United States spent upwards of 60 percent of its intelligence resources on the Soviet target. Israeli intelligence focuses on Hamas, Islamic Jihad, and other Palestinian adversaries. It is true, as well, that unexpected crises elsewhere can siphon off considerable resources from time to time, as the experience of the United States illustrates (the Korean War, for example, or, more recently, the Al Qaeda attacks). Occasionally, what seems like a temporary crisis may in fact be a critical or “realigning” intelligence event (to borrow terminology from the field of voting studies), as when attention in the United States shifted from Russia and the problem of weapons proliferation in the immediate aftermath of the Cold War to a concentration on Al Qaeda after September 11, 2001.

In 1995–1996, officials in the United States often spoke of turning more toward an intelligence posture of global surge (P5), especially in light of the belt-tightening ethos that had descended upon Washington at the time (however short-lived). Subsequent emergencies in various parts of the world (embassy bombings in Africa, the Cole attack, the terrorist attacks of September 11th) have persuaded many observers, however, that a global presence remains necessary for the United States, given its widely spread interests. Even so, Washington has had to surge its intelligence capabilities on occasion, because of the exorbitant costs that a blanket presence around the world entails. The recent war in Afghanistan is the most obvious case, where the CIA had few assets and was forced to send in case officers cold, who scrambled around Pakistan and other perimeter nations in a hurried recruitment of local spies (with all the concomitant dangers of questionable loyalty). At least to supplement these make-do humint efforts, the United States could afford to send in complementary techint resources (particularly effective was the Predator drone).

As suggested by P6 (and again well-illustrated by the war in Afghanistan), even when employing global presence and surge together, affluent nations like the United States will continue to experience intelligence gaps. A fully transparent planet remains a quixotic goal. “Where’s Bin Laden?” is a question on many people’s lips, and the list of other information gaps is long. How far along is Iraq toward The Bomb? How about North Korea’s long-range missile production? Iran’s nuclear program? These questions
are hard to answer via techint; a well-placed, reliable asset might do the job; but this would require beforehand a skillful case officer to make the right recruitment, which in turn depends on language skills and cultural knowledge. For want of a nail a shoe was lost . . .

With respect to the fascination of affluent nations with techint (P7), the United States provides a classic illustration. Since the 1960s, the techint versus humint spending ratio has been about 7:1, although with the terrorist attacks on the American homeland in 2001 more spending is now moving toward humint in a stepped up effort to infiltrate Al Qaeda and other terrorist organizations.24 Costly techint spending is most apparent in nations that have major space surveillance programs (notably the United States and Russia)—the major source of imbalance in the techint/humint spending ratio.

In the United States, intelligence spending has tallied about one-tenth of the total spent on defense (during and since the Cold War)—the basis for P8. But the spending ratio between intelligence and defense for other countries remains (for the most part) shrouded in veils of secrecy. Even in the United States, only once has the aggregate budget on intelligence been released to the public ($26.4 billion in 1996), although estimates of $35 billion, widely reported in the American media in 2001–2002, continue (approximately) the hypothesized 10 percent ratio. Subtracting the costs of space-based surveillance, the U.S. intelligence budget would plunge to about 5 percent of defense spending. This happens to be the rough aggregate figure for the only other country for which we have reliable data: the United Kingdom.25 So this funding proposition might more accurately posit a 10 percent intelligence-to-defense spending ratio in affluent nations with major space-based surveillance programs, dropping to half that amount for affluent nations without such programs (like the United Kingdom).

Acquiring information overseas under embassy cover (P9) does appear less successful than the use of non-official cover; however, once more—the curse of intelligence as an academic discipline—accurate data on the subject are elusive. Instead, we must turn to the published experiences of insiders and interviews with intelligence professionals (government reports are largely silent on this delicate question). Here the evidence is compelling that embassy cover is too thin; so is the information available on the cocktail circuit—especially regarding such key topics as terrorism and weapons proliferation. “NOCdom” is slowing gaining interest in the United States as the preferred means for espionage cover abroad and, reportedly, it has long been the practice of other nations.

The literature on foreign intelligence liaison (P9)—one of the most tightly kept secrets in this invisible world—uniformly indicates that intelligence sharing does occur, but within strict confines and always laced with ambivalence and caution.26 By combining their intelligence efforts with those of their allies, nations are able to trim intelligence costs and compensate for gaps in their own surveillance; yet, fear that the other service has been penetrated by a common foe, and an awareness that the ally (however close) is likely to have some divergent objectives, keep the romance at arm’s length. The proposition warrants a corollary: the greater the perceived common danger, the more likely an effective liaison. Even Russia and the United States are sharing intelligence these days on terrorism, counternarcotics, and international crime.

Indeed, as globalization (interdependence) seems to bring in its wake a greater incidence of worldwide terrorist, drug, and criminal activity, victimized nations have proven more willing to provide some of their intelligence findings to one another and—a dramatic change in norms—to international organizations, in what Herman refers to as the “globalization of intelligence.”27 With recent help from member nations (particularly Great Britain, Russia, and the United States), the UN has been able to develop a more
effective Situation Center since the end of the Cold War, and the European Union has set up an Intelligence Division in Brussels with a companion center for imagery analysis in Spain.

**Processing.** Information overload has become a source of enormous frustration for intelligence managers in the United States and elsewhere (P12); for example, they never have enough photo-interpreters and language translators. Only about 10 percent of the imagery gathered by U.S. satellites is ever examined by a human eye; most of it is stored in warehouses, either virtual or old fashioned, along with unevaluated sigint transcripts and stolen documents. At least, though, during crises or when pressing issues change, stored data can be retrieved and evaluated, and can yield significant information that would never be available if it had not been collected when priorities were different.

**Analysis.** In the United States, open-source information has long accounted for some 80–95 percent of final (“finished”) intelligence reports forwarded to policy officials (P13). Most valued by policy officials are reports that bring together information from a wide array of sources or “ints” (P14). Some targets, though, are especially difficult to acquire information about, short of spying, and intelligence reports on these targets (terrorism, weapons proliferation, closed societies) have—as stated by the proposition (P15)—a higher component of secret information.

Also as suggested by Proposition 16, a blending of the ints in the quest for more comprehensive reporting depends on an effective institutional integration of the intelligence agencies—an organizational ideal that the secret agencies in the United States usually fail to reach. Research into why the U.S. agencies display more centrifugal than the desired centripetal forces points to a key cause (P17): a weak Office of the Director of Central Intelligence. On paper, the U.S. intelligence community looks like it is run by the DCI; but, in reality, it is dominated by the Sec Def (P18), with virtually no efforts by presidents thus far to shift the balance more toward civilian intelligence (trade, diplomacy, political and cultural affairs). Eighty-five cents of every intelligence dollar is divvied out to the nine agencies that deal with defense intelligence issues.

In the United States, recent DCIs have tried to overcome the centrifugal forces and military dominance in the intelligence community by establishing interagency “fusion centers” and “task forces” housed at the CIA (P19). While staffed predominantly by CIA personnel, they have members from throughout the intelligence community. Since the mid-1980s, these structures have proliferated, focusing on such “hot button” topics as counternarcotics and (the largest center) counterterrorism. The DCI also created special task forces to guide the conduct of America’s secret operations in Iraq, the Balkans, and Afghanistan.

Regardless of the $35 billion spent on intelligence, or all the elaborate ints and organizational structures, the United States has continued to be surprised by world events (P20). Sometimes this has been true because of deficiencies in well-placed assets or techint; at other times, because no nation has a crystal ball to anticipate the mysteries of the future. The shock of the September 11th attacks falls into the first category; the inability to predict leadership ascension in Russia, China, or even Germany fall into the second. As open as American society is, pundits find it difficult even to predict accurately the outcome of presidential and congressional elections in the United States.

Improving one’s chances at finding secrets or predicting future outcomes depends in part on having a deep national reservoir of well educated people from which to draw case
officers and analysts. Affluent nations, like the United States and Britain, have an educated populace with advanced academic degrees and opportunities for world travel (P21); one would expect intelligence reports in such nations to have a greater sophistication than in poorer nations. Certainly the United States produces an enormous number of intelligence reports; but it is impossible to compare them systematically to documents prepared by the intelligence services in poorer nations, since such papers remain unavailable for public scrutiny.

The quality of some U.S. intelligence reports, though, has been examined and the record is mixed. Some are mediocre, like the National Intelligence Estimate (NIE) in 1950 that predicted the unlikelihood of immediate armed hostilities on the Korean peninsula—just days before war broke out; and some have provided value beyond what was available in the public domain, like the intelligence report about the buildup of Iraqi forces along the Kuwaiti border in 1994 (in another test by Saddam Hussein of American resolve). Analytic blind spots have been improved by concentrating resources on specific intelligence targets (P22), as when the CIA began to have a better grasp of the Soviet economic system by undertaking on this subject the largest social science study ever carried out in history. Even then, however, analysts fell short of being able to predict that the sharp decline of the Soviet economy in the 1980s would contribute so significantly to the dissolution of the U.S.S.R. in 1991.

The American intelligence community has been guilty of issuing worst-case scenarios, especially its military agencies (P23). In the 1950s, for example, U.S. Air Force intelligence projected the existence of a “bomber gap” and then a “missile gap” that supposedly placed the Soviet Union far ahead of the United States in both categories. The empirical data provided by U-2 and satellite imagery soon shattered those twin myths; in truth, the United States was ahead. The military has hardly been the only guilty party, though. Former Secretary of State Dean Rusk (1961–1968) accused the CIA of frequently overreacting, noting wryly that “the Agency predicted twelve of the last four crisis.” This criticism tends to be overstated, however; most analysts want to get it right, without over- or underestimating.

For the same reasons—professional training, integrity, pride—analysts have also eschewed the politicization of intelligence for the most part (P24), although there are troubling examples on the record. Richard Helms, DCI from 1966–1973 came under this cloud when a congressional committee accused him of altering intelligence to suit the policy needs of the Defense Department during the Nixon Administration. DCI Casey’s own deputy accused him of trying to intimidate analysts into providing the President with information more in harmony with the Reagan administration’s strong anti-Communist views of the world. Most recently, during the second Bush Administration, the Wall Street Journal reported a quote from the former head of CIA counterterrorism that “basically, cooked information is working its way into high-level pronouncements,” and USA Today said that “pressure has been building on the intelligence agencies to deliberately slant estimates to fit a political agenda.”

One might suppose that intelligence managers with political backgrounds (Casey served as Reagan’s presidential campaign manager in 1980) would be most susceptible to this deviation from the mores of objectivity; yet, George Bush (1976–1977) had served as Chairman of the Republican National Committee earlier in his career and managed to avoid charges of cooking intelligence as DCI. However exceptional “intelligence to please” may be, the phenomenon must be constantly guarded against by analysts and their overseers.
**Dissemination.** In the final phase of the cycle, nothing so turns away policy officials from the information products of the secret agencies as their irrelevance, untimeliness, or inaccuracy (P25). Often intelligence is irrelevant to policymakers, because analysts become infatuated with their own research interests—say, the state of the Mongolian People’s Army—at the expense of other topics currently more pressing to decision-makers. “We publish too much intelligence of questionable relevance to policymakers,” a prominent CIA official has conceded. Tardiness is equally unhelpful. Reports on the whereabouts of terrorists are notably perishable, as the Clinton administration discovered in 1999 when the United States fired cruise missiles at Bin Laden’s encampment in the Zhawar Kili region of Afghanistan’s Paktia Province, only to learn he had departed hours earlier. Further, the accuracy of information is critical; the CIA’s misidentification of the Chinese Embassy in Belgrade serves as an embarrassing reminder.

In the United States, better liaison inside the Beltway as a means for improving the relevance and timeliness of intelligence (P26) genuinely works. The Commerce Department, for instance, has permitted a team of over 100 CIA liaison officers to become “witnesses” to its daily events, in order to provide more precise intelligence the next day. In contrast, the international division of the Environmental Protection Agency was completely unaware in 1995 that the CIA engaged in environmental intelligence collection and had liaison officers available to interact with the EPA. Intelligence was not just irrelevant or untimely; it was missing altogether.

Clearly, intelligence is pushed aside sometimes because it fails to suit the policy needs of an Administration (P27), as when President Lyndon B. Johnson refuses to accept the honest reporting from the CIA that the war in Vietnam was going badly for the United States. Further, sometimes officials are too busy with meetings and other responsibilities to pay much attention to intelligence. A senior Defense official observed that he had only five minutes a day to devote to reading intelligence. Arrogance can play a role as well. Secretary of State Henry Kissinger, with all of his high-level contacts abroad and extensive traveling, is widely reported to have viewed himself as his own DCI. Finally, the failure of policymakers to act upon intelligence reporting as early as 1995 about the possibility of terrorists using airplane to flying into American buildings is a tragic reminder of the potential gap between good information and wise policy decisions (P28).

**The Covert Action Propositions**

Before the current war against global terrorism, the CIA had been called upon to conduct its most extensive covert actions during the Reagan administration, with a concentration on two nations: Afghanistan, to help drive out the Soviets, and Nicaragua, to undermine a Marxist-leaning regime. Other high points in the modern use—though no administration has come close to the emphasis placed on covert action by the Reagan Presidency—occurred, moving back in history, at the end of the Carter administration (again to counter Soviet aggression in Afghanistan), as well as during the Vietnam War, the early Kennedy years (especially against Cuba), and the Korean War. All of these instances corresponded with strong expressions of ideological conflict against the U.S.S.R. and its satellites or outright warfare against its Communist allies (P29). The present war against terrorism—an ideological struggle between American globalism and Islamic extremism—could well become an arena for the most extensive use of covert action by the United States in its history.

Each of these peaks of covert action reflects the extensive use of paramilitary operations. These operations involved the arming of surrogate forces, who either fought
side-by-side with U.S. overt forces (Korea, Vietnam, the second Bush Administration in Afghanistan) or were guided by U.S. military and intelligence advisers (Bay of Pigs, Reagan in Afghanistan, Nicaragua). Modern weaponry is expensive and, thus, not many nations can match the United States in the frequency of its sponsorship of prolonged paramilitary operations (P30). Moreover, the major successful covert actions for the United States have depended upon weak regime targets and strong indigenous allies (P31). Iran, Guatemala, Afghanistan in the 1980s, and again in 2001–2002, are prime examples.

Although the CIA has enjoyed some covert action successes, the ledger is filled with setbacks as well, most infamously the Bay of Pigs in 1961 and the Iran-contra scandal in 1987. The latter struck at the very constitutional foundations of the legislative process. Furthermore, the long-term results of the “successes” in Iran, Guatemala, and Afghanistan (during the Reagan years) eventually turned to ashes. In these instances, the negative “blowback” effects included a revolt of Muslim fundamentalists against the corrupt Shah supported by the United States; a series of brutal military dictatorships in Guatemala; and, as Afghanistan tore itself apart with internecine warfare, the rise of the Taliban regime.

The Counterintelligence Propositions

Expensive as well is guarding a nation against attack by hostile intelligence or other secretive organizations, like Al Qaeda (P32). A nation has many vulnerabilities, from its skyscrapers and computer networks to its secret documents and codes. Helping the military and law enforcement community protect them is a major challenge for any intelligence service. Even twenty-five years ago, before the Information Age moved into high gear, over 2,000 people in the CIA alone were engaged in the maintenance of secure communications between CIA Headquarters and clandestine stations throughout the world.42

Despite considerable funding in the affluent nations to build strong counterintelligence defenses, breaches still occur. There is no perfect defense against every adversary’s attempt to penetrate one’s inner government circles (P33) and, during the Cold War, every major European nation suffered even more extensive counterintelligence failures than the United States. The shock of each major counterintelligence breach in America has led to panels of inquiry, reorganizations, and more money for defenses—but not always success in improving security. All the hullabaloo over Aldrich Ames’s treachery at the CIA failed to uncover Robert Hannsen’s treason at the FBI; that took subsequent mistakes of his own.

The Accountability Propositions

The genius of American government lies in its safeguards for protecting civil liberties through a system of accountability. For most of the nation’s history, the intelligence agencies were allow to operate outside these safeguards. When the inevitable abuses of power came to light, critics called for inclusion of these agencies into the framework of checks and balances required for the rest of the government (P34). The Bay of Pigs fiasco stimulated a congressional inquiry and floor speeches for reform in 1961; so did the revelation in 1967 that the CIA had connections to the National Student Association and other American organizations.33 Yet successful reform required the even greater shock that came in 1974: charges, subsequently confirmed, that the CIA had spied on American
citizens at home. This scandal provided the catalyst for the first major investigations into the activities of the intelligence community.44

As a result, the Congress created Senate (1976) and House (1977) oversight committees, along with new laws that required reporting to legislators on covert action, a special court for national security wiretaps (the Foreign Intelligence Surveillance Court, 1978), and regular briefings to members of the oversight committees on the full range of intelligence activities. The Iran-contra affair (1987) again involved the misuse of intelligence, this time efforts by the Reagan administration to bypass both the established intelligence oversight and appropriations procedures on Capitol Hill. The scandal led to a further tightening of supervision over the secret agencies.

Interest in intelligence accountability has been offset in the United States by a periodic overriding concern about security (P35). When the nation has been more or less united in a common struggle against a foreign adversary who appears highly threatening, the question of democratic principles becomes less pressing than defeat of the enemy. This defeat (so goes the argument) may require a relaxation of restraints on the conduct of military and intelligence activities. From 1947 until President Richard M. Nixon’s experiments with Soviet détente in 1974, the CIA and its companion agencies were relatively free of oversight strictures. As the Cold War thawed, however, and the Watergate scandals and CIA domestic spying came to light, Congress took up the issue of intelligence oversight and established rigorous new standards of accountability. In the aftermath of the direct attacks on the United States carried out by terrorists on September 11th, these standards now face the criticism that they have stifled the ability of the intelligence agencies to fight against America’s enemies.

The proper degree of intelligence accountability promises to be a subject of national debate in 2003, and one can see early signs that the second Bush Administration is trying to slip the bonds of well established congressional reporting requirements on intelligence activities.45 One can also see signs of co-optation of the two congressional Intelligence Committees, as an increasing number of their staffs come from the secret agencies and more and more of their members speak publicly of being advocates for the intelligence service, not vigilant overseers (P36). Nonetheless, intelligence oversight since 1975 remains infinitely more serious than before that year, as at least a few members of the two congressional Intelligence Committees have been prepared to carry out robust accountability.46

Further, every DCI since 1974 (with the Casey exception) has publicly expressed support for the supervision Congress has provided in this era of increased oversight (P37). Robert M. Gates, DCI from 1993–1997, sums up this shared view. “Some awfully crazy schemes might well have been approved had everyone present [in the White House] not known and expected hard questions, debate, and criticism from the Hill,” he writes in his memoirs. “And when, on a few occasions, Congress was kept in the dark, and such schemes did proceed, it was nearly always to the lasting regret of the Presidents involved.”47

**Conclusions and Policy Implications**

Intelligence refers to the gathering, interpreting, and distribution of information (collection and analysis, for short); the secret manipulating of events abroad (covert action); and the guarding against foreign intelligence agencies and other hostile organizations (counter-intelligence). Effective collection and analysis is, above all, a function of national wealth; but it also depends on focused targeting, all-source synergism, and good
liaison ties between intelligence officers and policymakers. Successful, sustained covert action also relies on national wealth, along with modest objectives, weak targets, and well-armed, popular local allies. Watertight counterintelligence requires national wealth and technical sophistication, plus an attitude of serious attention to security matters (which usually rises after a major breach). Rigorous oversight is most likely to take place following spy failures and scandals that remind citizens of the importance of accountability, as well as—in a more routine fashion—during times of peace when democratic nations exhibit a more sensitive appreciation for civil liberties.

These propositions make up some of the essential bricks and mortar for a theory of intelligence, although the list is not meant to be exhaustive. Each requires extensive testing as more information on intelligence becomes available to the public (and, though moving slowly, the trend in the United States has been in this direction since 1975). The large amount of work that remains to be done in this field of inquiry should whet the scholarly appetites of those with an interest in the hidden side of government.

An important incentive for developing a theory of intelligence is the hope for more surefooted policy guidance that might be derived from an enhanced understanding of key intelligence issues. Even the preliminary framework presented here suggests some useful steps for strategic planning in the wake of the September 11th attacks on the United States. As a starting point, policymakers (as well as commissioners on the newly created panel to examine the 9/11 intelligence failure) must realize that no perfect intelligence system can be devised. Failures are an existential reality of trying to anticipate world events. Yet, robust funding for intelligence activities can improve the chances of success. The spending must be sensible, though, not lavished on gold-plated surveillance satellites with every bell and whistle at the expense of human intelligence and the establishment of a deep-bench analytic capacity—particularly with respect to regions of the world relatively ignored by the United States in the past (such as South Asia).

The theoretical framework examined here suggests, as well, that policymakers need to be more focused and explicit in their threat assessments. Intelligence managers need a stronger sense of an administration’s priorities and specific information requirements—beyond the obvious one today of pinpointing the location and plans of Al Qaeda operatives. When intelligence tasking is excessively diffuse, it invites failure; a more exact tasking permits intelligence agencies to marshal their resources more effectively in the search for information regarding the most urgent dangers that confront the nation.

This raises the larger issue of America’s foreign policy objectives. If they are too scattered, so will be the nation’s intelligence needs to support them; if they are more focused, so will be the intelligence effort—with concomitant higher odds of success (and the added benefit of reduced federal spending that would attend less expansive global aspirations). A worldwide intelligence presence is a luxury that even the wealthiest nations can ill afford; in lieu, the United States will need to fashion a more discriminating, less interventionist foreign policy, along with a more effective intelligence surge capacity.

Important, also, will be a stronger reliance on intelligence liaison with other nations and with international organizations. Such ties have always been a part of America’s intelligence effort, but they must be further nurtured. The common global threats of terrorism, illegal drugs, and international crime should be catalysts enough to encourage the success of expanded liaison relationships. The evidence suggests, too, that the NOC debate should come to an end; official cover simply does not provide the United States sufficient access to hidden information overseas. Clandestine human collection must make a radical shift toward the use of non-official cover.
The findings on intelligence processing and analysis hold obvious policy ramifications. Officials must redouble efforts to fund language translating, photo-interpreting, and data-mining capabilities that remain inadequate, despite notable improvements in the past year. Especially vital will be the development of advanced methods for sifting through the large volume of data collected via humint, techint, and open sources. Closer attention to information technology (IT) is essential. The nation cannot allow its intelligence agencies to drift in this domain, as IT advances outside the government rush forward—as happened at the FBI under Director Louis Freeh for almost eight years in the 1990s.48 Similarly, translating the day after September 11th NSA communications intercepts that warned of an impending major Al Qaeda attack against the United States does nobody any good. One can be sympathetic to the enormous challenge that data-mining presents to the intelligence agencies, for they are deluged with streams of daily intelligence from around the world; one cannot be sympathetic, however, to their lethargic response to this challenge in recent years.

As part of the effort to improve data-mining, the intelligence agencies still need to pay closer attention to the scouring of information from the public domain—open-source intelligence—before resorting to more expensive and risky clandestine collection operations. A good librarian or researcher can be as valuable as a good spy.

Necessary, too, are improvements in the ability for analysts to talk to one another via secure communications channels within their own agencies and across agency lines. One of the most astounding and disheartening current realities about the U.S. intelligence agencies is their technical inability to share data, a condition further exacerbated by cultural disinclinations to share. These agencies have a computer network called Intelink (established in 1994), but its list of users is tightly restricted and excludes many low- and mid-level analysts. Law enforcement and intelligence officers at the state and local level have no access to Intelink whatsoever, not to mention personnel in immigration and naturalization or airport security. Even those with access to the network will find there only “secret” or less highly classified information, rarely the “top secret” or specially compartmented data given to a select few at the top of the nation’s intelligence and policy hierarchy—even though this top-secret information is likely to provide the most significant insights and warnings about pending calamities.

Accompanied by the requisite counterintelligence security (anti-hacking) measures to safeguard the integrity of the system, Intelink must be upgraded to serve federal, state, and local officials in an integrated all-source, electronic web of communications about national security threats. This is a manageable technical problem. More daunting is overcoming the decades long cultural norms of keeping information and analysis contained within one’s own agency, letting other agencies fend for themselves. This hoarding can take place even within pockets of the same agency, as when (prior to 9/11) FBI agents in Minneapolis and Phoenix never compared notes on their respective concerns about terrorists engaged in flight training inside the United States.

One of the most compelling results of research on intelligence in recent years is the concern about the tilting of the intelligence apparatus in the United States too much toward the side of military concerns, at the expense of gathering and assessing worldwide information on political, economic and cultural matters (“diplomatic intelligence,” for short). A better understanding of the world—the raison d’etre of intelligence—will require a better balance between military and diplomatic intelligence than the current approximate 9:1 ratio (as measured by annual funding).

In perhaps the most important finding of recent intelligence research, these problems of inadequate intelligence sharing (all-source fusion) and an imbalance in mili-
tary/diplomatic intelligence can be remedied only by elevating the stature of the Director of Central Intelligence. At long last, the DCI must become the true—not just the titular—leader of the intelligence community, with all the necessary budget and personnel authorities to establish the kind of central intelligence that President Truman sought but never achieved in 1947. Unfortunately, the plan to create yet another intelligence analytic entity within the new Department of Homeland Security further undermines the DCI’s intended role of providing a central repository of all-source information and assessments for policymakers.

The politicization of intelligence will always be a danger that must be guarded against. Until analysts become angels they will remain susceptible to the normal risks of subjectivity in human judgments, amplified by the beguiling charms of policymakers looking for “intelligence to please” and prepared to reward analysts who are helpful in that regard. Recently, a former CIA counterterrorism chief accused the Pentagon brass of “politicizing intelligence, no question about it” when the Department of Defense established a new analytic shop to find links between Al Qaeda and Saddam Hussein, because the CIA had concluded that none existed.49

Just as greater electronic and cultural “jointness” is necessary among intelligence analysts, so must the intelligence connections between consumers and producers be tightened—again, both electronically and culturally. The Aspin-Brown Commission discovered in 1996 that a policymaker sitting in the Old Executive Office Building could not communicate by top-secret e-mail to an analyst at the CIA. Even a State Department desk officer was unable to communicate in this fashion with an intelligence officer in the Department’s Intelligence and Research Bureau—both in the same building! Once more, these are solvable technical problems (and can be reduced as well by good intelligence liaison personnel inside the national security departments).

Once more, the cultural problems are harder: the resistance by policymakers to information that challenges their preconceptions, their lack of time to seriously absorb analysis, their arrogance that they already know everything they need to know. Often “intelligence failures” are really policy failures. In 1995, for example, the CIA warned White House officials about the possibilities of aerial terrorism of the kind that would strike the Twin Towers and the Pentagon on 9/11; nonetheless, terrorism remained down the list of priorities for policymakers. Imagine if—six years before the attacks—policymakers had taken aerial terrorism more seriously and moved to strengthen airport security, as well as the monitoring of pilots enrolled in flight schools.

Shifting away from the intelligence cycle toward the other aspects of intelligence discussed in this article (covert action, counterintelligence, and accountability), it remains likely that policymakers will fail when they attempt to carry out large covert actions in regions where a target regime is strong and local paramilitary surrogates are weak. Some $70 million in CIA-dispensed funds to buy off local, powerful warlords in Afghanistan did much to undermine the Taliban regime; a comparable amount of funding provided to disorganized and bickering Iraqi opposition groups, who are up against a more cohesive regime, has proved feckless.

Covert action, though, can have purposes other than immediate victory. Covert propaganda beamed into the U.S.S.R. never brought that empire to its knees; but it helped keep hope alive among Soviet dissidents and—when the time was ripe—that hope was channeled into regime change (thanks to many other complicated historical conditions, including the rise of a reform-minded Soviet leader, Mikhail Gorbachev, and a deteriorating Soviet economy that cried out for change). Moreover, covert action used in concert with other instruments of foreign policy—notably, the use of overt military force in the
recent Afghan regime change—can be effective, as well may be the case in Iraq, too, if a U.S.-led UN coalition goes to war there again in 2003.

With respect to counterintelligence, suffice it so say that one can never rest. When the CIA relaxed its attention to counterintelligence in 1975 with the firing of James Angleton and the dispersal of counterintelligence responsibilities, it set the stage for moles to prosper and they did over the next two decades.50 With the major traitors Ames at the CIA and Hannsen at the FBI now behind bars, the intelligence agencies may fall back into complacency. Keeping up the guard against moles will be a significant challenge. So will be the maintenance of secure electronic communications among collectors, analysts, and policymakers—and, generally, protecting against a much-predicted “ electronic Pearl Harbor” attack on the communications infrastructure of the United States.

Intelligence overseers will be sorely tried, too, as America and its allies wage a war against global terrorism. The research evidence suggests that accountability and concern for civil liberties take a back seat to aggressive intelligence collection and law enforcement in times of domestic and foreign crisis. In the balance between security and liberty, the scales drop toward the security side. There is nothing preordained about this tipping of the balance. The nation can enjoy both security and liberty, but this requires close vigilance by lawmakers and White House overseers. They must ensure that laws like the USA Patriot Act of 2001, and the ruling of the Foreign Intelligence Surveillance Court of Review in 2002 that had the effect of lowering standards for wiretaps,51 do not lead to improper spying against people in the United States because of their ethnic heritage or political views, rather than their actual support of terrorism or other criminal activities. If we throw out the Constitution to catch the terrorists, we will have lost everything worth fighting for.

Notes

5. For sources on the statistics in this paragraph, see Johnson, Secret Agencies.


15. A saying sometimes used by CIA analysts when their work is ignored by policymakers.


17. Ransom, correspondence to the author (January 30, 2002).

18. See Ransom, “Politicization.”


21. I am grateful to British intelligence scholar Michael Herman for drawing this exception to my attention, panel remarks, annual meeting, International Studies Association, New Orleans, March 24, 2002.


25. Michael Herman, correspondence with the author (November 23, 2002), based on 1999 estimates. Herman notes that, in the wake of the attacks on September 11, 2001, the percentage is “probably” somewhat higher and that, generally, the British spending ratio for defense and intelligence is around 12:1 or 10:1. See, also, Michael Herman, *Intelligence Services in the Information Age: Theory and Practice* (London: Case, 2001), p. 71.

26. See Westerfield, “America and the World of Intelligence Liaison.”

27. Michael Herman, remarks, Contemporary British History Seminar, University of London (November 28, 2001).

28. John Millis, staff director, U.S. House Permanent Select Committee on Intelligence, speech, Central Intelligence Retirees Association (October 5, 1998).

29. This was true in the 1950s and early 1960s when Allen Dulles was DCI [see his *The Craft of Intelligence* (Westport, Connecticut: Greenwood, 1977)], though closer to the lower 80 percent end of this range; and true today, though closer to the 90–95 percent range, as once closed societies around the world are more open now to public reports on their activities (Johnson, *Bombs, Bugs*, p. 185).

30. Based on the author’s examination of a wide range of intelligence reports while serving as Special Assistant to the Chairman on the Aspin-Brown Committee in 1995–1996.

31. This was a central conclusion of the Aspin-Brown Commission.


33. Johnson, “The CIA’s Weakest Link.”

34. Comment to the author, Athens, Georgia (July 4, 1983).


37. Author’s interview with Robert M. Gates (March 28, 1994).


40. These examples are drawn from the author’s experiences as a participant-observer on the Aspin-Brown Commission in 1995–1996.


43. For background, see Ransom, *Intelligence Establishment*.


45. George W. Bush, *Statement by the President*, The White House (December 28, 2001), which criticizes the assertion in the Intelligence Authorization Act for Fiscal Year 2002 that the executive branch should report in writing to Congress on “significant anticipated intelligence activities or significant intelligence failures”—an expectation that goes all the way back to the Hughes-Ryan Act reporting requirements passed on December 31, 1974 [Section 662, Foreign Assistance Act of 1974 (22 USC 24220)].


