Government and the Information Marketplace

by

Douglas H. Dearth

The Problem

In this highly-touted era that we call the Information Age, we are all — public institutions, private corporations, and individuals — trying to come to grips with the importance of information. Traditionally, information has been considered to be a "service" — i.e., as a "support function." In short, information "comes with the furniture," and it costs less than the light bill.

The civil marketplace, however, is beginning to think about information as a "commodity" or as a "product" — something that has exploitable value. That value, in classic economic terms, is established in the give-and-take, supply-and-demand, hurly-burly of the market. "Competitive Intelligence" is now a by-word in the private sector. A company's success increasingly is thought to depend on its ability to derive *value* from information. The military is beginning to think about information as a "weapon" — something that can be used offensively to inflict harm on an adversary, or something against which to be defended. In defensive terms, information is a critical "capability" to be protected in terms of its availability, integrity, and confidentiality. Hence, the terms "Information Operations," "Information Warfare," "Information Assurance," "Information Superiority," etc.

Yet, the government generally, including the military establishment, has not truly come to grips with the implications of the concept of information as "product," "commodity," and "weapon." Intelligence — the purposeful, tailored application of information — is still treated as free goods. The American intelligence budget was until quite recently classified, but it is now publicly reported to be $26.7 billion, with a marginal increase in the offing next year. In government terms, that is almost real money. We argue occasionally over the appropriate level of the intelligence budget, but the argument is in reality an argument over budget levels and mechanics, not over the value of intelligence *per se*.

The argument here is that the U.S. Government — and the military establishment in particular, since it consumes a reputed 80% of the national intelligence budget — should begin to treat intelligence and information as a product, a commodity, and as a weapon when appropriate, and to take these concepts seriously. In short, it is time to handle intelligence — both classified and open-source — as a principal line function, rather than as free goods for which there is no direct accountability by policy-makers and military commanders, or indeed by producers of intelligence. Among the few people who have thought about this approach, it has been called

"industrial funding" of intelligence. This would be a most unfortunate and inappropriate term for the post-industrial Information Age.

Market Intelligence

A better term might be *"market-pricing"* of intelligence. If we are to be serious about intelligence, the Information Age, and Information Operations, should we not take money — initially — out of the hands of the producers, and put it in the hands of the consumer? Such an approach would serve several constructive purposes.

First: It would serve to instill discipline in, and make customers responsible for, the use of a vital resource. Policy-makers and the most senior levels of the military establishment would need to think constructively about, and come to grips with, just how much real *"value"* intelligence and information provide to the policy and decision-making process. That "value" would be determined by the criticality of need, the difficulty of collecting and producing, its timeliness, and degree of veracity and utility.

Second: It could conceivably instill some rationality upon the elaborate guild structure that we have come to call the Intelligence Community. Intelligence organizations have always competed with one another. Collection disciplines vie for the purported superiority of their wares. Production elements, which have proliferated for reasons both of specialization and consumer sponsorship, compete within a limited realm (classified consumership), extolling the uniqueness of their product and value of their insights. Uniqueness of product will become increasingly difficult to assert in an era of increasing availability of information, much of it directly and more accessible to consumers.

Third: Market pricing of intelligence would elevate the current insidious intra-Community budget process from the pervasive nit-picking and log-rolling to more explicit, value-driven deliberations. The current bickering over "roles and missions" and "lanes in the road" could be jettisoned in favor of an "industry shake-out." The historical "command economy" approach to community management, belied by such buzz-words, could yield to a market-driven, value-added ethos more in line with our purported national political, economic, social, and cultural norms.

The Politics of Intelligence

Professor Michael Handel advanced the idea of "politics of intelligence" in his definitive book *War, Strategy, and Intelligence*.[1] He identified four kinds of "politics" in the intelligence process: Politics as an "*interest*," essentially the competition within the process in terms of primacy, attention of consumers, and resources (i.e., budget); politics as a "*bargaining process*," again within the profession, resulting from differing perspectives on the process and the substantive issues at hand; "*politicization*" of intelligence, through interference by senior leaders, which distorts "purely professional" considerations; and "*political use*" of intelligence by political leaders through selective application for partisan advantages.

These issues that Handel identified a decade ago echo concerns expressed by Sherman Kent in his *Strategic Intelligence for American World Policy*[2] as early as 1949. These problems are never quite resolved because they cannot be; they are simply endemic to the intelligence process and the nature of government. The current process, however, allows them to fester and to become insidious.

A market-driven intelligence process would not change the phenomenon of "politics as an interest;" it would merely make it more explicit. Such a market-driven process might, however, serve to sublimate the budget and "attention-getting" competition among collection disciplines by making them, in a sense, sub-contractors of the *real* producers of intelligence, the analytical elements. The real budget process, however, would largely pass to the ultimate customer: the policy-makers and senior commanders. The indirect result might be more relative emphasis on those collection disciplines that do not cost much (e.g., HUMINT and clandestine SIGINT) and less capricious "show-and-tell" use of "happy-snaps" provided by IMINT. Given the immense costs of developing, launching, and operating aerial- and space-based imaging systems, the market might drive the industry toward less-costly systems.

The "bargaining process" within the intelligence sector would likely change in a market-driven process. Rather than the obsession with finessing the bottom-line judgments on substance, the intelligence sector might be forced to negotiate industry standards for data-base design, data reliability criteria, certain reporting formats, etc. However, analysis bartering as reflected historically in the national estimates process would disappear, except in the mechanics of whatever intra-industry sub-contracting arrangements between analysts and collectors that various intelligence enterprises might find useful. If the customer were to receive differing answers or interpretations because the customer *financed* competing analysis, the customer could choose the product that best suited the needs of the moment or was more congenial to policy interests. This is essentially what consumers in fact do anyway. In any case, the competition to provide proven value-added analysis should increase.

"Politicization" of the intelligence process is a normal human impulse. It is only resolved within the context of producer-consumer relationships. Policy-makers and senior commanders of integrity tend not to do it — much; and producers with professional integrity (or who are simply stiff-necked) do not allow it — any more than they can help. Let the real market decide: Let failed policy face the voters — or the adversary; and let the purveyors of shoddy product and vendors of shady reputation sink in the market. At a minimum, this would allow *policy failure* to stand on its own, rather than to be clouded with accusations of *intelligence failure*.

Politicians — and senior appointees — are in the *business* of politics. Since they would *pay* for intelligence product explicitly, they may *use* the product as they see fit. Collaboration — or indeed collusion — between producers and consumers of intelligence has frequently been the norm. The "political use" of intelligence essentially is the *point* of the whole process. In any case, good intelligence cannot save bad policy, and there is no necessary correlation between good or bad decisions and good or bad outcomes. In economic terms, the only relevant relationship in the decision-making process is the degree to which decisions are based on the best information available at the time they are made.[3] Again, let the viability and integrity of both policy and policy input be exposed to the success-failure test.

Intelligence for an Information Age

Command economy has become a historical dead-letter. It has proved to be a bankrupt concept. Those former communist countries that have embraced the market economic model are beginning to thrive. Those that have resisted the trend are struggling; and the worst recalcitrants are failing, as economies, states, and societies. The last vestiges of Cold War, command-driven, ideology-dominated economies are to be found in China, Belarus, and the American national security apparatus. Even the once-moribund American automobile manufacturing sector has learned to adapt to modern realities. "Competitive intelligence" now helps to drive capitalist enterprise, which appears to be flourishing everywhere in unprecedented ways. It is time for American government, particularly the national security sector with its garrison-state mentality, to join this broad historical trend toward a more enlightened future.

The effect of information technology, broadly considered, threatens the traditional intelligence priesthood. Information and data generally are more available in more volume to more people in more ways than even before. As information becomes more ubiquitous and more readily accessible, government cannot possibly maintain a monopoly on the data and information, much less the classified intelligence, or the talent and creativity that produces it. Although there will be much to protect in terms of confidentiality, availability, and integrity of information, too often have security classifications been used to cover the mundane, the trivial, and the criminal.

Our thinking about the Information Age tends to concentrate on information technology, largely because it is so new and so obtrusive. We are probably only on the cusp of the true Information Age in this sense. Technology will become ever more ubiquitous, and in the process less obtrusive and perhaps less costly. However, as the technology costs and visibility recede, more attention will be focused on the *utility* of information. It has been axiomatic that, when confronted with the choice between allocating resources for a tangible weapons capability — tank, ship, or aircraft, for instance — or intelligence support, defense policy-makers and commanders tend to opt for the tangible and potentially lethal. For instance, the shortcomings in intelligence connectivity experienced during the Gulf War were guaranteed by a generation of operator-driven resource decisions. Intelligence Community whining over this state of affairs has been generally ineffective and self-serving.

Our fascination — indeed obsession — with technology has generated a trend toward amalgamation of command-control-communications technology and staff with that of intelligence. Hence, the trend toward C3 and C4 (adding computers) staff organizations. This phenomenon is an understandable effort to rectify undisciplined staff performance. Yet the result has been to subordinate the *"why"* of information to the *"what"* and *"how"* of information. This situation has caused us to confuse the *medium* for the *message*. MacLuhan's adage might apply to entertainment, but it should not corrupt decision-making. While intelligence must take opportunistic account of available information and communications technologies and command-and-control methodologies, the latter must also accommodate the needs of the former.

The problem is that supplications by intelligence officers tend to lack a critical and convincing demonstration of effectiveness. This impasse will rarely be breeched under the current budget process. Thus, the money must be taken from one group of culprits and handed to another: the customer. Senior policy-makers and senior commanders need to think deeply and honestly about how much their enterprises depend for success upon information. Then, they need to budget for this vital resource. In the end, we will still have a "budget-driven" capability for providing intelligence — as opposed to a "threat-driven" capability. Practicality must arbitrate the process. Requirements will almost certainly always outstrip capabilities because of budget realities. At least we will have a system that more explicitly reflects the relative value of capabilities, utility, and effectiveness.

The current process is designed to pay for physical infrastructure, technology, and meeting payroll. There is no agency line-item for *results*. Today, the national intelligence budget is dominated by two primary factors: the burgeoning costs of: 1) technical collection systems and 2) payroll. In the absence of an exceedingly forgiving Congress and electorate — or a convincing and significant external threat, this fiscal dilemma will not be resolved. We might at least be able to rationalize the process by making more explicit the value costs of intelligence.

A "privatization" process for intelligence comes up against several practical difficulties:

First of all is the enormous sunk-costs of the infrastructure: buildings, technology, communications, etc. In the short run, infrastructure should simply be turned over to physical plant management and service-provider entities, e.g., General Services Administration, military services, leasing companies, etc. This is pretty much the case, anyway. The public switch telephone providers already own and operate the communications. If it can be demonstrated that individual agencies can operate all or part of their infrastructure more efficiently and effectively, they should be allowed to do so, bearing in mind concentration on "core-competencies."

Second, the government personnel system should be scrapped. Each operating element of the intelligence sector should be allowed to hire, fire, develop, and retire its employees as it sees fit, consonant with operating realities, but fully within the regulations and provisions of applicable Federal and state employment laws. Intelligence organizations should be able to maintain on payroll as many or as few employees of whatever qualifications required and that they can afford within operating realities. Compensation packages should be individually negotiable within broad "industry" guidelines.

This operating model could include a multi-tiered staffing system that could include a relatively small core of career professionals and support staff, an array of term contract employees (individually negotiated) hired for periods of perhaps two to five years, and increasing reliance on short-term (days to two years) contract substantive knowledge specialists to perform services as needed. This sort of scheme has already been proposed by Robert Steele.[4] Its objective would be to "harness the knowledge potential of the nation," in Mr. Steele's terminology.

Such a staffing scheme is fully in line with the sorts of broad trends identified by economists, corporations, and management specialists. Lifetime employment is no longer the model in many private-sector enterprises. While many bemoan this phenomenon, this situation has considerable benefits for both employers and employees. The key advantages for employers

are competitive agility and staffing flexibility to meet market imperatives. For employees, too, it offers flexibility and the opportunity to innovate and find more opportunities for contributing in the market-place of ideas. The Government's Federal Employees Retirement System (FERS) already makes the employee more responsible for his or her lifetime well-being. Employees should be free (responsible) to provide for perceived retirement needs inside a government-sponsored system, outside of it, or both.

There will still be concern among intelligence providers for security vetting of its employees and contractors. Little need change under a market-driven system. Standards of behavior and methods of vetting can still be set and enforced. There might be less concern over exotic security levels for shorter-term contract employees, or there might not. The cherished smoke-screen of requiring polygraph examinations as part of the vetting process might atrophy under a labor-service market system, or it might not. In any case, it would be useful to encourage a more unified set of standards and procedures, rather than paying for the redundant security vetting systems currently in operation. Indeed, a centralized security clearance system for the entire Government is long overdue.

Thirdly, the knowledge-market might serve to sort out the current tension between classified and open-source intelligence. Responsible proponents of open-sources have never meant for those sources to supplant classified sources. The argument has been explicitly for better synergy, and implicitly for better and more effective resource allocations in pursuit of national security and operational goals. A market-driven intelligence system would at a minimum force the classified intelligence priesthood and the classified intelligence guild structure to more effectively prove their wares. This will only happen by letting the customer test the market.

The days of government monopoly of technical collection systems are passing. Even middling states will have remote-imaging capability, as will private corporations via commercial systems. There will be decreasing differences in the resolution of government and private satellite systems. HUMINT will probably continue to be largely an in-house capability, but this function is fairly cheap. The problems are: control and values; and for these reasons a policy-maker likely — and Congress certainly — would not want to take too many chances with "third-party" HUMINT operations, except with very close allies. Similarly, certain core operational counter-intelligence functions might remain "proprietary." Yet many of the more mundane, encyclopedic information requirements, which clandestine and overt collectors tend to ignore anyway, can in fact be increasingly accessed directly by analysts and even consumers.

Lastly, a market-driven streamlining of intelligence should serve to reduce the bloated, redundant myriad of so-called "management" staffs at Community and agency levels. As documented repeatedly by high-level Intelligence Community reviews, the Director of Central Intelligence does not control the national intelligence budget. Further futile attempts to enable that person to do so likely will be frustrated by the existing guild system and bureaucratic politics. If anyone *really* wanted such centralized budget control, something would have been done about it by now.

So, let's just give up on this chimera. This would call into question much of the Community Management Staff and their largely useless tentacles known as "functional managers." Neither of these sorts of entities have ever *managed* anything. They have not even been very effective observers. Likewise, the Defense Department's mini-CMS, known as the C3I Integration Support Activity, is redundant, in both American and British meanings of the term. These entities have tended to be refuges for the bored and dissatisfied, clever bureaucrats, and the otherwise unemployable. Every productive employee should not require a personal "functional manager."

Certain intelligence sector coordinating functions would continue to have value: principally those that perform standard-setting and inter-operability functions. These residual elements should constitute themselves much in the way professional associations do. The American Retail Florists Association should be the preferred model, rather than the American Bar Association or the American Medical Association guilds. Those members of such staffs who retain employable skills and those with true entrepreneurial interests will find satisfying employment within or outside the new system. The remainder can be grandfathered into retirement with the thanks of a grateful nation.

* * * * * * * * * * * *

The American Intelligence Community, as it has evolved, accreted and mutated since the early days of the Cold War has much of which it can be proud, much for which it has never been made to answer, and much that might never be proved one way of the other. Nonetheless, let us embrace the dawn of the Information Age. Let us emulate the finest examples of private sector commerce and the struggling efforts of former authoritarian states by allowing the knowledge-based market to determine the true value of intelligence. Let us finally make the intelligence budget the *answer*, not the *question*. Policy-makers, commanders, tax-payers, and freedom-loving people everywhere deserve no less.

Endnotes

---

[1] Michael I. Handel, *War, Strategy, and Intelligence*, London: Frank Cass and Co., Ltd., 1988, pp. 187-228.

[2] Sherman Kent, *Strategic Intelligence for American World Policy*, Hamdon, CT: Archon Books, 1965, esp. Pp. 180-206.

[3] See Roger G. Noll, "The Economics of Information: A User's Guide," Institute for Information Studies, *The Knowledge Economy: The Nature of Information in the 21st Century*, Annual Review, 1993-1994, pp. 25-52.

[4] As developed in Robert Steele's presentations to the National Senior Intelligence Course, Joint Military Intelligence Training Center, Bolling Air Force Base, Washington, D.C.

PROCEEDINGS 1998 7th International Conference & Exhibit OPEN SOURCE SOLUTIONS: Global Intelligence Forum - Link Page

Previous	OSS '98 Robert David Steele, TAKEDOWN: Targets, Tools, & Technocracy,
Next	OSS '98 Stephen Arnold, The Future of Online,

Return to Electronic Index Page