Network-Centric Intelligence: An Approach to a Strategic Framework

Network Centric Applications Track

Peter J. Sharfman
Director of Policy Analysis
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102-7508

This paper is based upon the efforts of a study group that has been supporting the Intelligence Community Senior Acquisition Executive and the Assistant Director of Central Intelligence for Administration since late in the year 2000. The study group's efforts have been collaborative to such an extent that I do not know how to separate my own ideas about how to improve intelligence processes from those of Heidi Avery, Dr. James Babcock, Gordon S. Dudley, Dr. Michael P. Healy, Dr. Annette Krygiel, Dr. William Marquitz, Rob Newton, RADM Richard Nibe, USN (ret.), Janet L. Sorlin-Davis and Dr. Bruce Wald. However, the presentation of these ideas in the context of network centric warfare is my own, and does not necessarily reflect the views of my teammates or of our Government Sponsors.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Network-Centric Intelligence: An Approach to a Strategic Framework	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The MITRE Corporation,7515 Colshire Drive,McLean,VA,22102-7508**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
2002 Command and Control Research and Technology Symposium

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**14**	

Network-Centric Intelligence: An Approach to a Strategic Framework

Peter J. Sharfman[1]
Director of Policy Analysis
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102-7508

Abstract

The intelligence cycle (other than actual collection by technical or human means) is discussed in terms of the differences between normal processes and the processes used on the most difficult and important problems. It is argued that a network-centric intelligence process (analogous to network-centric warfare) would be more effective than the best of today's processes. The capabilities that must be developed to enable such network centric intelligence are identified, and experimentation is suggested as an effective path towards the development and fielding of these capabilities.

Introduction

The standard model for thinking about the work of the intelligence community is the "intelligence cycle" of requests for information, tasking, collection, processing, exploitation, analysis, and dissemination. Intelligence professionals understand that this is an idealization rather than a precise description, but the model is generally used as a basis for discussing and planning for systems modernization and other potential improvements. Thus, when the question is raised of modernizing systems in such a way as to facilitate the interactive use of multiple collection disciplines, it is often stated as the question of "Multi-INT TPED."

---

[1] *This paper is based upon the efforts of a study group that has been supporting the Intelligence Community Senior Acquisition Executive and the Assistant Director of Central Intelligence for Administration since late in the year 2000. The study group's efforts have been collaborative to such an extent that I do not know how to separate my own ideas about how to improve intelligence processes from those of Heidi Avery, Dr. James Babcock, Gordon S. Dudley, Dr. Michael P. Healy, Dr. Annette Krygiel, Dr. William Marquitz, Rob Newton, RADM Richard Nibe, USN (ret.), Janet L. Sorlin-Davis and Dr. Bruce Wald. However, the presentation of these ideas in the context of network centric warfare is my own, and does not necessarily reflect the views of my teammates or of our Government Sponsors.*

I have been requested to make it clear that while the DCI and DDCI/CM have approved the concept of Multi-INT, they have neither reviewed nor approved the specific proposals in this paper.

However, it is striking that while the classical intelligence cycle is a fair approximation of the way in which routine activity is conducted, the intelligence community departs from the cycle whenever a really important issue arises. Indeed, the more pressing the issue, the more urgent the crisis, and the greater the attention paid by the most senior levels of the Government, the less accurate is the classical cycle as a description of what the intelligence community is doing.[2]

Perhaps a better way to discover and plan improvements in U.S. intelligence is to take as a point of departure the best way we know to how to work – the processes that are followed today when the stakes are highest. Whenever the U.S. faces an intelligence problem that is really difficult and really important, all of the available collection disciplines are brought to bear. Rather than operating in carefully separated "stovepipes" and then turning their findings over to all-source analysts only at the end of the process, intelligence professionals with a wide variety of skills and organizational affiliations work together collaboratively. In the aftermath of September 11, these methods are being applied to the immediate challenge of homeland security. A brief and descriptive name for this community-wide process is "Multi-INT."

Multi-INT is in many ways analogous to contemporary "joint warfare." Detachments of skilled professionals, trained and equipped (with software tools rather than weapons) by proud organizations organized around distinctive core competencies, come together to wage a coordinated attack on an intelligence problem. In many cases the distinctive intelligence collection disciplines (SIGINT, IMINT, HUMINT, MASINT, and sometimes OSINT) have complementary strengths and weaknesses, so that using them in concert really does produce synergistic results.

As the U.S. military discovered some time ago, real jointness (or real Multi-INT) is not easy to execute. The laws of physics permit communications interoperability, but in practice classified email between one major intelligence organization and another is still a challenge. It is reasonably easy for a professional in one intelligence agency to locate "finished products" produced by a sister agency, but work in progress can usually be located only through informal personal contact, and unexploited data (of which there is a large and growing accumulation) is almost impossible to find outside one's own organization. Few individuals are genuinely cross-trained, and earlier this year the author was told in all seriousness by a senior professional that the SIGINT analysts and the imagery analysts build up impressive professional skills, while the all-source analysts are the people who could not or would not learn to do anything well except write.

There are a number of efforts under way to move towards Multi-INT. A program called ICMAP (Intelligence Community Multi-Intelligence Acquisition Program) was created jointly by the heads of the five major intelligence agencies. ICMAP is building tools and applications that will enable Customer requests for intelligence to be made to the intelligence community as a whole, improving the process by which intelligence

[2]This point is made forcefully by Bruce Berkowitz and Allan Goodman, *Best Truth* (New Haven: Yale University Press, 2000), pages 67-74.

requirements flow separately to the various organizations. When these tools and applications come into operation, the resources of the intelligence community will be used more efficiently and effectively, and intelligence Customers will no longer need a sophisticated understanding of how intelligence is collected in order to effectively request an answer to a real-world question. In addition, an interagency group called the MINTWG ((Multi-INT Working Group) is sponsoring a series of experiments with Multi-INT, just as JFCOM manages experiments with military jointness.

This paper explores the nature of the following step. Just as "network-centric warfare" makes collaboration among multiple platforms integral to the way fighting is done, and thereby moves beyond the kind of jointness in which the ground component, the maritime component, and the air component support each other while each doing their own thing – so we may ask whether "network-centric intelligence" could multiply the effectiveness of the intelligence community by making multi-disciplinary collaboration integral to the normal course of business.

This paper does not address improvements in the technology of collection, processing, and exploitation. The United States has led the world in these areas for half a century, and extensive investments are being made today to meet the collection challenges of the coming decades. More precisely, this paper takes as its premise that excellent collection, processing, and exploitation is a necessary but not sufficient condition of excellent intelligence.

The Path of Increasing Effectiveness

The simplest intelligence process is one that is organized around a single intelligence collection discipline, or INT. For example, there might be a situation in which the only available method to obtain information on an enemy's plans consists of intercepting enemy communications and deciphering them. In this case, technical systems will be tasked to identify and intercept particular communications, and other systems will be tasked to decipher these communications. Then SIGINT analysts will interpret what they mean, in part by comparing them with previously-intercepted communications, and the results will be provided to the Customer (presumably a military organization) that requested the information. Further analysis may take place, either in the SIGINT organization or in the Customer organization, that relates the substance of particular communications intercepts to other information about the enemy's plans or doctrine in order to obtain a "big picture" of enemy intentions.

A more complex process is one in which multiple intelligence disciplines obtain information relevant to the solution of a single intelligence problem. To continue with our previous example, it might be the case that the intercepted communication referred to a particular Army Division that was being ordered to advance. At the same time, we might collect imagery that showed that the Army Division in question was severely under-strength, because a large number of its tracked and wheeled vehicles had been put out of action by our bombing. This imagery would be collected in response to tasking to

carry out a bomb damage assessment, and photo interpreters (or imagery analysts as they are now called) would go over the images carefully to determine the extent of the damage. An all-source analyst would then take both the report from the SIGINT analyst and the report from the imagery analyst and combine them to produce a report that described both the enemy intent to advance and also the firepower of the unit that was to carry out the advance. This is today's "normal" intelligence process.

The next step in increasing effectiveness is what we might call Multi-INT. Still continuing with our previous example, we can improve on the process in which the SIGINT collectors and the IMINT collectors are separately tasked and operate independently. Interpretation of an image might reveal a particular type of command vehicle within the enemy division and this could cue the SIGINT collectors to look for communications on a particular frequency. A communications intercept might reveal the schedule for a particular battalion to move down a road, and this could cue the imagery collectors to image that road at that time in order to get a good look at the battalion, and even count the equipment items capable of moving. Such collaborative tasking can be called *micro-fusion,* to distinguish it from the *macro-fusion* carried out by the all-source analyst. A further example of micro-fusion could be the use of electronic emissions intelligence (ELINT) to help the imagery analyst interpret the blob in the shadow of a tree on an image. Today, multi-INT of this kind is used on an exceptional basis to address intelligence problems that are particularly difficult and particularly important.

Finally, we may look ahead to what we might call Network-Centric Intelligence. Here we must imagine a team, working together in a collaborative fashion. In all probability, the team is physically separated, but connected by secure broadband communications and equipped with software that enables them to work together as if they were all in the same room. The team would be led by somebody skilled in all-source analysis and familiar with the substance of the intelligence problem at hand. One or more team members would have access to a variety of data bases that would incorporate what is already known about the problem, including access to work in progress or to intelligence that was collected in the past, but not fully exploited. There would also be access to a database of lessons learned in the course of addressing analogous intelligence problems in the past. There would also be team members with the expertise to judge what each of the possibly relevant collection disciplines (IMINT, SIGINT, HUMINT, MASINT, and OSINT) could contribute if tasked, and with the ability to task such collection if it is judged to be useful. Finally, one member of the team would have a clear understanding of the problems and needs of the Customer (perhaps a military commander, perhaps the NSC), and could help the team prioritize its efforts in the light of the Customer's priorities, and also report back to the customer on interim results and on when to expect further information. Such teams would form and reform dynamically in order to meet the changing needs of national security.

Students of military transformation will see a similarity here to the path from single Service activity, to joint warfare as practiced prior to Goldwater-Nichols, to joint warfare as practiced today, to network-centric warfare.

From Hierarchy to Network

The intelligence community is organized today in a series of hierarchies, most of them following the familiar pyramidal form that characterizes large-scale armed forces and formal bureaucracies. Although information can be shared without moving up the hierarchy to the point where the management chains of the people sharing come together, collaboration among separate organizations generally requires approval at a moderately senior level. More importantly, the priorities of most intelligence professionals are set by their immediate supervisors, and the priorities are generally set in terms of the priorities of the particular organization rather than of the intelligence community as a whole or of the community of intelligence Customers.

The effects of the hierarchical organization are aggravated by the existing security regime. Because the basis for the security regime is the "protection of intelligence sources and methods," each of the major INTS (comprising a collection discipline and the methods for processing, exploiting, and carrying out first-stage analysis of the resulting data) has its own separate security regime. On this basis, each of the major intelligence organizations has an internal information infrastructure that enables a fair degree of collaboration, and strong protections against links between that internal network and any other network. Even though the all-source analysts are cleared for all of the various INTS, there are numerous security barriers and procedures that make collaboration difficult and time-consuming, and require that coordination of effort across the various major organizations been planned and approved rather than impromptu and spontaneous.

There have been proposals over the years to achieve the synergies of Multi-INT by reorganizing the intelligence community. Some of these proposals called for a division of labor along strictly functional lines – for example, that the CIA should do all the analysis and only the analysis. Others have called for moving in the direction of a single intelligence hierarchy exercising operational and budgetary control over the entire community. This paper argues that such reorganization would fail to achieve its objectives. The intelligence community is so large, so diverse, and so chopped up by security compartments that the agency directors often have difficulty in mandating changed modes of problem-solving. Turning the entire community into a single hierarchy would produce unity on the organization chart, but would be unlikely to produce coordinated action in practice.

A more promising approach is to move not towards a super-hierarchy but rather towards a network. A network is needed not just to provide many paths along which information can flow, but primarily to enable the members of the intelligence community to become *self-synchronizing.*

Just as network centric warfare means organizing a network around the battle to be fought (or more broadly around a set of military objectives to be achieved), so network

centric intelligence would mean organizing a network around an intelligence problem or set of related problems that need to be solved.

In the context of the intelligence community, self-synchronization would mean two major changes in today's normal ways of doing business. First, collaboration with people in other organizations who are assigned to work the same problem (that is, collaboration within a multi-organization community of interest), must be viewed by management as the normal way of doing business, requiring no special decisions or permissions by management, and with security rules that facilitate it rather than impede it. Second, when a shortage of time requires an individual to prioritize among several different opportunities to add value, the individual should feel a stronger obligation to a problem-solving community of interest cutting across agency lines than to colleagues in his or her own agency who are working a different problem set.

Network-centric intelligence would enable a process of agile collaboration, and moving problems to places where resources are (for the moment) available and opportunity costs low. It would also enable a process of making use of whatever resources would be most helpful in attacking particularly pressing and difficult problems. Neither of these is possible when organizations tightly manage their professional resources. Both are possible when intelligence professionals are required to manage their own time, and given incentives to manage their time in ways that are beneficial to the customer.

Experimentation As a Way Forward

Even if we are confident that building a network centric intelligence process would make intelligence more valuable to the nation, we cannot be confident that we know exactly how to go about it. Effective networks would require a complex mixture of new and old operational concepts, enabled by an equally complex mixture of new and old information systems. We do not know enough to design these operational concepts and systems deductively from our understanding of the capabilities required.

At the same time, we do have some good ideas about how to generalize effective Multi-INT processes from crisis use to more systematic use. We want to put these ideas into practice as soon as possible. Ideally, we want to move forward while working systematically to learn from the experience of new approaches; to refine our goals as we approach nearer to them.

A reasonable approach in this circumstance is to undertake a series of experiments. Each experiment would try out some innovative operational concept or concepts. If the experiments are designed and carried out in a disciplined way – that is with a meaningful hypothesis to test and a way of measuring the extent to which the hypothesis is confirmed – then we can learn and make progress even when the operational concept itself fails to achieve the desired capability.

In many cases, the operational concept with which we wish to experiment would require hardware or software that is not in current use – either in the Government or in the commercial world. This will call for the use of system prototypes, and the experiments will then serve to test such prototypes as well.

As long as it is made clear to all concerned – notably including the Congress – that network centric intelligence is a direction in which we are moving rather than a defined objective to be reached by a date certain, we can move forward by means of experiments and prototypes. Successes would be scaled up, and failures would be a source of valuable learning about what to try next.

Furthermore, the experiments will help refine the concepts of the capabilities we seek, so that as we progress we become increasingly clear about where we are going and what it means to our customers.

A Preliminary Glimpse of the Goal

In order to formulate hypotheses for experiments, and plan experiments with prototype processes, hardware, and software that have the potential to provide better intelligence output, we need a sense of what network-centric intelligence would be like if it existed. Presented below are seven *capabilities* that may serve to point the way. Each of these capabilities would represent an evolutionary improvement over what exists today, but used in combination they would arguably bring about a revolutionary improvement in the effectiveness of the intelligence community. We may speak of each of these capabilities in isolation as a "Multi-INT" capability, and we may think of them in combination as "network-centric intelligence."

It must be understood that these "capabilities" do not represent organizations or systems; instead, these capabilities each require the effective collaboration of many people from many organizations and the interoperability of many systems.

The first three capabilities are a *knowledge and data capability,* a *Multi-INT fusion capability,* and a Multi-*INT tasking capability*. They would, in combination, transform the exploitation and analysis of intelligence data from an INT-centered process to a process centered on the exchange and collaborative use of information. Such a change would be analogous to the impending change of military doctrine from platform-centric to network-centric, and the results may be equally powerful. The second three capabilities are a *security capability, a communications* capability, and an *enterprise management capability*. Each of these capabilities represents an enabler that is necessary if the first three capabilities are to function in the real world. Finally, we require a *Customer-focused knowledge capability* to bring the intelligence Customer[3] into the network, so that the intelligence community's work is properly focused and usefully disseminated.

[3] The term "Customer" is used to refer to a person or organization *outside* the intelligence community; a lower case "c" is used to refer to an "internal customer."

Of course, the point of experimentation is to learn, and it would be very disappointing if the concepts for these seven capabilities are not refined and modified in the light of experimental results. They should be viewed not as the answers, but as a place to start looking for answers.

1. *Knowledge and Data Capability (KDC)***.** The first step in solving an intelligence problem is to access what the intelligence community already knows. This cannot possibly be done by creating a single "mother of all databases;" rather, it must be done by creating a capability to access – to browse, if you will – a very wide variety of specialized data bases. This capability must have access to information stored by all the various intelligence organizations in the United States, which means that there must be a robust method to determine and enforce the need-to-know principle (see # 4 below). It also means that information about substance ("what we know") must be stored separately from information regarding the sources and methods used to obtain it ("how we know it").

   In addition, we must position ourselves to remember all that we know. We must learn to store and retrieve various kinds of information other than "finished intelligence", including: (a) information that was collected, but not fully processed or exploited; (b) information that was processed and exploited, but not subjected to analysis because its priority was not high enough at the time; (c) information that resulted from analysis, but which did not find a place in finished intelligence products; (d) information regarding people (including former employees of and former consultants to the intelligence community) with particular kinds of expertise; and (e) information regarding intelligence methods that were used in the past, and their strengths and weaknesses.

2. *Multi-INT Fusion Capability (MFC).* All-source analysis is an established discipline. In the classical model of the intelligence cycle, it transforms information obtained from a variety of sources into finished intelligence. However, the creation of the KDC and the CFKC (see #7 below) enables the application of this skill at an earlier point in the process. Given a good understanding of the Customer's problem, an all-source analyst can fuse together the information relevant to this problem that is available from the KDC. In some cases, this information may be sufficient to solve the Customer's problem without additional tasking, creating finished intelligence from diverse information already at hand on demand. In other cases it will be necessary to task intelligence collection, processing, and exploitation assets. However, this tasking will be made more efficient because (a) the tasking will be to fill gaps in existing knowledge (plus updating it as necessary), rather than to collect any information relevant to the Customer's problem; and (b) the tasking can be guided and informed by what is already known.

   The traditional work of the all-source analyst – enhanced by access to the KDC and collaboration with the CFKC – may be described as *macro-fusion.* Macro-fusion

takes available information and figures out what it means for the customers' problems. In a world of Multi-INT, a process of macro-fusion may take place several times during consideration of a problem: first in assembling relevant existing information to address the problem, second in fusing the results of new collection with this existing information to address the Customer's problem more effectively, and third to store in the KDC results that are likely to be of value in addressing future problems. In addition, the world of Multi-INT can benefit from *micro-fusion*, in which the work of exploitation benefits from collaboration across collection disciplines.

For example, a camouflaged command post might be captured on an image, while its emissions are also detected. The emissions make it clear what it is but not precisely where it is; the imagery pinpoints its location but not its function. In combination (micro-fusion), they identify the command post. Macro-fusion would then combine that information on location and function with other available information to evaluate the relevance and importance of the command post's existence in the context of the Customer's plans for upcoming operations, and thus provide the Customer with knowledge relevant to the decisions he must make.

3. *Multi-INT Tasking Capability (MTC)***.** When a need for intelligence has been identified, the MTC figures out the best way to satisfy the need, and how to reconcile it with other competing intelligence needs.

   This tasking is far from simple – given the perennial shortage of resources, the constraints of orbital mechanics, and (sometimes) the risk that a particular tasking will jeopardize the future availability of a source or method. Each tasking involves opportunity costs, by making other tasking wait its turn. Therefore, efficient tasking requires careful prioritization of intelligence needs, and also a detailed understanding of which taskings could be carried out in parallel, and which taskings are necessarily alternatives to each other. This process is facilitated by elaborate semi-automated systems, which have been separately developed to manage the tasking of IMINT and SIGINT. A truly Multi-INT tasking capability would permit tradeoffs in the opportunity costs of diverse collection methods, and would take account of the availability of HUMINT and open sources as well. It also would provide the ability to task processing and exploitation assets, since the needed information may be obtainable from unexploited collection that has already taken place.

   This MTC does not replace the "tasking" systems that currently exist to direct collection by the individual "INTs," but rather it connects with them. The MTC would not figure out how to aim a satellite, but since it does address the issue of whether a satellite should be aimed at a particular target (given the opportunity costs of doing so), the internals of the tasking of the individual INTs must be transparent to the MTC.

4. *Security Capability*. Security may be the most serious challenge to Multi-INT. While effectiveness in solving intelligence problems requires easy collaboration and

easy access to relevant data, experience shows that as secret information becomes more widely available, the risk of compromise grows. All too often, the compromise of a source or method causes it to become ineffectual in the future.

A balance must be realized between the need to share information and the requirement for protecting intelligence sources and methods. There are four principles that need to be followed.

First, information is collected and stored in order to solve problems, and using it to solve problems requires that it be shared. Given the fact that the most important intelligence problems have to do with avoiding surprise, we need to make information available to those who might discern significance that was not apparent to those who originally collected it, analyzed it, or requested it. Sharing information entails risk, but this risk must be managed rather than avoided because information sharing is essential.

Second, the circulation of information must be based not on organizational principles but rather on a need-to-know basis. This means that it may not be available to those without a need-to-know, even if they are in the same organizational unit as somebody with a need-to-know, and even if they are senior managers in an agency where some employees have a need-to-know. But it must be available to those with a genuine need-to-know, even if they work in an agency completely separate from the one that produced the information. It must also be available to those with a plausible reason why they *might* need to know, for information originally created to serve one purpose may prove very valuable to others with a completely different problem to solve. Furthermore, the security process must recognize that a need-to-know the substance of intelligence and a need-to-know how that intelligence was obtained are not necessarily correlated. Need-to-know, if properly implemented, replaces the idea that an individual, a work-group, or an agency "owns" information and has a right to share it or withhold it as they see fit.

Third, the processes by which individuals access secret information must be audited. Safeguards against accessing information without a proper need-to-know provide a hedge against the imperfections of the security clearance process, but only if enforced on the basis that nobody is above suspicion. Apart from strengthening security, this should make it easier for the various intelligence agencies to grant reciprocal access to each other's networks – something that is difficult today because no agency understands just who would obtain access as a consequence. An additional benefit is that an audit of the information obtained by an individual analyst would facilitate mentoring and learning.

Fourth, the substance of secret information must be separated as far as possible from the sources and methods used to obtain it. This requires that the Customers of the intelligence community trust it more than they do today – but the greater effectiveness arising from Multi-INT may over time generate such trust.

5. *Community-Wide Communications Capability.* The bandwidth available for secure communications between the major intelligence organizations may not be sufficient to enable widespread collaboration, and security considerations further restrict communication. A true Multi-INT communications capability would be one in which the volume and quality of communications ran with inter-agency communities of interest rather than with organizational boundaries among and within agencies.

6. *Enterprise Management Capability*. Given that multi-INT is Customer-driven, there must be a way to balance the competing needs of disparate Customers. This requires a capability to look across the various Customer needs and the variety of intelligence resources that might be brought to bear to meet these needs. Understanding the priority of needs at the enterprise level at any point in time enables managers to commit their assets most effectively.

   In addition, Multi-INT means that the valuable products of intelligence are more likely to be products of the "intelligence community" and less likely to be products of a particular agency. This means that it will be necessary to devise means to trace the process in order to judge over time which sources, methods, and activities are most cost-effective, and hence to make rational decisions for investment and for the growth or shrinkage of particular activities. It will also be necessary to put in place an incentive structure that rewards effective collaboration and penalizes efforts by individual organizations to work in isolation.

7. *Customer-Focused Knowledge Capability (CFKC).* The Customers of the intelligence community are people whose jobs are to make decisions involving national security, and who need intelligence information in order to make better decisions. The traditional Customers of the intelligence community are national policy-makers, warfighters, and the military acquisition community; homeland security issues involve additional customer communities. In what follows, the term "Customer" is strictly limited: intelligence community managers, intelligence analysts, and staff in customer organizations are important recipients of intelligence information, but they are NOT "Customers" because they do not use intelligence information to make national security decisions. On the other hand, tactical commanders are Customers just as the most senior decision-makers are Customers.

   The CFKC is the ability of the intelligence community to understand the Customer's problems well enough to understand what intelligence support would be most useful to the Customer. In the absence of a CFKC, the Customer must understand the intelligence community well enough to figure out what support he can realistically expect and then express his requirements in the vocabulary of the intelligence community. The CFKC allows the Customer to describe his problems in his own terms, and receive back intelligence information that has been tailored to meet his needs.

   In today's world, the CFKC is best approximated by the J-2 organization supporting a senior military commander, and by the staff that delivers the President's Daily Brief.

However, these are models that are susceptible to improvement. The CFKC must have genuine depth of understanding of the way in which the Customer views the world, and of how intelligence can help the Customer. Ideally, the various individuals who comprise the overall CFKC should understand the priorities of the needs of their various Customers, and they should interact to set the priorities for the major activities of the intelligence community. The CFKD does its best to anticipate the intelligence needs of the Customer and fill the needs even before the Customer expresses them.

At the same time, the CFKC must be at home in the world of all-source analysis, and indeed the same individual sometimes functions as both CFKC and analyst. The critical point is that the CFKC straddles the intersection of intelligence and Customer it is a part of the intelligence community, but its focus is on the needs of the Customer.

Summary: A Few Big Ideas

As these experiments lead the intelligence community towards the capabilities we characterize as Multi-INT, there will have to be an evolution towards network-centric processes as well as a staged deployment of more capable systems. Indeed, the capabilities described above will be wasted unless we harness them to carry out the daily work of intelligence. We will be reaping the benefits of the Multi-INT capabilities when our processes embody a few simple principles:

- The Customer will be king, and the intelligence community will understand that it exists to serve its Customers. To be sure, there are many Customers, and they cannot all be king at the same time. Moreover, the intelligence community strives to understand and provide what the Customer needs, which is not always what he thinks or says he wants. But the intelligence enterprise exists to provide knowledge, not to obtain knowledge.

- The "INTs" – that is, the enormous capabilities currently organized around the several collection disciplines – will be less autonomous than they were in the past, but they will remain the foundation of whatever value the intelligence community is able to provide to national security.

- The intelligence community as a whole will know what we know, and share it. We will make what is known easily accessible to those who can use it. We will remember what we learn, and we will also remember how we do things, so that the future does not need to reinvent successful methods and processes.

- The central focus of intelligence activity will be finding answers to the Customers' questions; providing such answers will be understood to be the metric for "solutions to intelligence problems."

- Therefore, we will analyze a Customer's problem before tasking. We will task for processing and exploitation before tasking additional collection. By tasking for collection *after* analysis, we will understand and report what is known, and focus tasking on what is unknown.

- We will "micro-fuse" data within the INTs and across the INTs in order to obtain information, while routinely "macro-fusing" information from multiple INTs to obtain knowledge.

If all of these things come to characterize the daily work of the intelligence community, then this daily work will no longer be centered upon hierarchical organizations created to operate and to protect specific sources and methods of intelligence. Instead, this daily work will center upon the acquisition, circulation, and dissemination of information. The center of the process will be the circulation of information among many people and organizations capable of adding value to it, and thus transforming the data produced by collection systems and the data retrieved from existing data bases into relevant knowledge and even understanding and wisdom. The intelligence network will be the processes that direct questions to the places where the most value can be added, and then direct usable knowledge back to the national security decision-makers. So network-centric intelligence will be the community's method for producing the best available answers to the widest range of intelligence problems.