National Intelligence Agencies and Transnational Threats: The Need for a New Intelligence Paradigm

By

William J. Lahneman, Ph.D.

Assistant Professor
Department of Political Science
Towson University
&
Senior Research Scholar
Center for International and Security Studies at Maryland
University of Maryland, College Park

Contact Information:
Towson University
8000 York Road
Towson, MD 21252-0001
Ph: 410-704-2581
Email: wlahneman@towson.edu

Revised 27 January 2008

The author gratefully acknowledges funding provided by the Center for International and Security Studies at Maryland to enable me to revise an earlier draft of this article.

NATIONAL INTELLIGENCE AGENCIES AND TRANSNATIONAL THREATS: THE NEED FOR A NEW INTELLIGENCE PARADIGM

Intelligence organizations must deal with both traditional state-based threats and transnational phenomena. Each requires a different approach. The traditional intelligence paradigm does not work against transnational threats. A new paradigm called an adaptive interpretation is necessary in these cases. Unfortunately, the continuing need for national intelligence agencies to use the traditional paradigm prevents them from tapping into the vast amounts of information needed to perform adaptive interpretations. To enable the intelligence community (IC) to use both types of paradigms, it is necessary to change the way the IC views information and the associated information flows. This leads to the need for a radically transformed U.S. intelligence enterprise.

INTRODUCTION

While traditional state-based security challenges will remain important, the most serious threats to international security will increasingly come from transnational phenomena. Transnational terrorism is the most visible current threat of this type, and governments are all too aware of the problems of fighting such a networked opponent that operates across borders, skillfully capitalizing on the increased travel, multifaceted communications, and expanded financial capabilities resulting from the process of globalization. Transnational criminal networks pose another serious threat, albeit one that lacks the visibility of terrorist networks because criminals seek financial gain rather than mass casualties.

Other transnational threats have the potential to cause destruction and upset international stability to a degree that will dwarf the effects of terrorism. These include both human-induced and naturally-occurring phenomena. Nuclear proliferation, the development of harmful biopathogens, continued illegal trade in conventional arms, and climate change are examples of human-induced phenomena, while the continued spread of HIV/AIDS and the potential for outbreaks of highly infectious and deadly diseases such as mutated avian flu and Sudden Acute Respiratory Syndrome (SARS) are examples of naturally-occurring ones.

All of these threats have one thing in common beyond their potential for destructiveness: all are transnational. As such, none can be understood – let alone defeated or reduced in intensity – by the actions of single states. In an ideal world, all states would cooperate to deal with these common threats. Cooperation would take many forms depending on the specific circumstances and nature of the threat, but the need to share large volumes of information and knowledge would be a common thread running through these efforts.

In the real world, there are significant impediments to sharing on this scale. This is because the knowledge and information in question fall into two broad categories. First, there is information and knowledge that virtually all governments and other actors have an interest in sharing voluntarily, although they might not recognize this fact. Second, there is information and

knowledge that governments desire to keep secret. It is difficult for single institutions to deal with both types equally well.

Intelligence agencies are the part of national governments charged with making sense of future security challenges. However, intelligence agencies' traditions and organizational cultures emphasize secrecy, not knowledge sharing. While there are valid reasons for this approach, the bias toward secrecy impedes knowledge sharing. Mandating that the U.S. intelligence community (IC) improve its knowledge sharing is a step in the right direction, but it is not sufficient to achieve the desired flows of both types of knowledge. This is because one set of rules and structures cannot manage both types of flows as long as the bias toward secrecy persists. Recognizing this fact and designing separate processes and structures to facilitate both kinds of information flows require a new approach to the intelligence enterprise.

THE PROBLEM[1]

The world and the threats within it are becoming increasingly diffused in nature, with non-military threats increasing in relation to purely military ones. Since the end of the Cold War, the intelligence community has contended with the emergence of new threats to national security from a number of quarters, including increasingly powerful nonstate actors such as transnational terrorist groups. Many of these actors have capitalized on the still evolving effects of globalization to threaten U.S. security in nontraditional ways. At the same time, global trends such as the population explosion, uneven economic growth, urbanization, the AIDS pandemic, developments in biotechnology, and ecological trends such as the increasing scarcity of fresh water in several already volatile areas are generating new drivers of international instability. These trends make it extremely challenging to develop a clear set of priorities for collection and analysis.[2]

Intelligence analysts are tasked with making sense of these developments, identifying potential threats to U.S. national security, and crafting appropriate intelligence products for policy makers. They also will continue to perform traditional missions such as uncovering secrets that potential adversaries desire to withhold and assessing foreign military capabilities. This fact has three implications. First, it means that, besides using traditional sources of classified information, often from sensitive sources, analysts must also extract potentially critical knowledge from vast quantities of available open source information. Significantly, the community must devise ways to monitor open source information in transformed ways. Additionally, some kinds of information currently not considered open source must be brought into the open domain.

For example, the process of globalization, empowered by the Information Revolution, will require a change of scale in the IC's analytical focus. In the past, the IC focused on a small number of discrete issues that possessed the potential to cause severe destruction of known forms. The future will involve security threats of much smaller scale. These will be less isolated, less the actions of military forces, and more diverse in type and more widely dispersed throughout global society than in the past. Their aggregate effects might produce extremely destabilizing and destructive results, but these outcomes will not be obvious based on each event

alone. Therefore, analysts increasingly must look to discern the emergent behavioral aspects of a series of events.

Second, phenomena of global scope will increase as a result of aggregate human activities. Accordingly, analysts will need to understand global dynamics as never before. Information is going to be critical, as well as analytical understanding of the new information, in order to understand these new dynamics. The business of organizing and collecting information is going to have to be much more distributed than in the past, both among various US agencies as well as international communities. Information and knowledge sharing will be essential to successful analysis, and most of the necessary sharing will need to be conducted on a voluntary basis.

Third, future analysts will need to focus on anticipation and prevention of security threats and less on reaction after they have arisen. For example, one feature of the medical community is that it is highly reactive. However, anyone who deals with infectious diseases knows that prevention is the more important reality. Preventing infectious diseases must become the primary focus if pandemics are to be prevented. Future analysts will need to incorporate this same emphasis on prevention to the analytic enterprise.

It appears evident that in this emerging security environment the traditional methods of the intelligence community will be increasingly inadequate and increasingly in conflict with those methods that do offer meaningful protection. Remote observation, electromagnetic intercept and illegal penetration were sufficient to establish the order of battle for traditional forms of warfare and to assure a reasonable standard that any attempt to undertake a massive surprise attack would be detected. There is no serious prospect that the problems of civil conflict and embedded terrorism, of global ecology and of biotechnology can be adequately addressed by the same methods.

To be effective in the future, the IC needs to remain a hierarchical structure in order to perform many necessary functions, but it must be able to generate or otherwise access collaborative networks for various lengths of time to provide intelligence on issues demanding interdisciplinary analysis. These networks should integrate open source intelligence (Osint) and should contain experts from the private sector as well as the IC. The IC also should seek ways to include the knowledge of former IC analysts in these networks.

Clearly, the magnitude of this challenge means that analysts in one intelligence agency will need to share information with analysts in other parts of the intelligence community – and with outside organizations – to produce accurate intelligence about complex issues. However, achieving successful collaboration is difficult because this goal clashes with the secretive organizational cultures of the various U.S. intelligence agencies. As a result, the intelligence community has been criticized for “stovepiping” – failing to share information when appropriate—and is now wrestling with this difficult problem.

THE TRADITIONAL INTELLIGENCE PROCESS PARADIGM

Conventional wisdom holds that the intelligence process is analogous to solving puzzles, but puzzles to which pieces are missing. Sometimes these missing pieces are quite important for understanding what the puzzle represents. The goal therefore is too amass as many pieces as possible – preferably the most important ones – so that analysts can make well-informed guesses (estimates or assessments) of what the complete puzzles look like. In particular, the IC attempts to describe the level of "substantive uncertainty" in its products. The IC achieves this by answering three questions:

1. What do we know about this issue?
2. What don't we know?
3. To what degree is what we don't know important?

In this traditional paradigm, puzzle pieces fall into three categories. Some are secrets. Secrets are information that is knowable but that certain actors want to keep hidden from others. The nature of North Korea's nuclear arsenal is an example of a secret. Other pieces to the puzzle are mysteries, which consist of information that is unknowable. This is often because the actors thought to have this information haven't yet decided how they will respond to a given set of events. Today, how certain transnational issues will develop also fall into the category of mysteries because their complexity offers a number of alternative paths along which they might develop. Information derived from open sources constitutes the third type of piece to the puzzle. Although it has received considerable emphasis following the 9/11 attacks, intelligence analysts have always recognized the value of the open source intelligence (Osint) produced from open source information available through sources such as the print media (journals, magazines, newspapers, and books), news broadcasts, Internet sites, academic courses and scholarly opinions, and personal observations and conversations.

Thus, the traditional paradigm for the intelligence process involves solving puzzles using pieces that are secrets, mysteries, or Osint. The process emphasizes discovering secrets. This is understandable when one considers the kinds of state actors – first and foremost the Soviet Union – that were the targets of western intelligence agencies during the Cold War, and the central role played by military power in that conflict.

Under the traditional paradigm, pieces of intelligence puzzles are assumed to be relatively static in terms of their contribution to the overall analysis. Furthermore, an analysis produced from such static pieces is unlikely to change significantly over the short run. These are good assumptions most of the time precisely because the traditional paradigm is used to deal with the capabilities and intentions of traditional state-based actors. In these cases, it is a state's large-scale, expensive outlays in the traditional foundations of power – principally military forces – that translate into the biggest threats. Fortunately, these kinds of expensive, large-scale forces tend to leave large footprints that help intelligence collectors to locate them. They also tend to be static in that, once a country fields a new army division or a new weapons system, the country maintains these assets for a considerable time and the threats posed by them remain essentially the same.

These characteristics explain why the traditional paradigm works well for traditional threats. First, the most threatening aspects of an opponent's capabilities are also the easiest to find because they are large in scale. Once collectors have found most of the "largest" pieces of the puzzle, they can feel fairly confident that they can perceive the entire picture with reasonable accuracy. Second, once an analysis is produced, it will remain fairly static for a considerable time. Any changes, such as another army division in an area, will be additive in nature. It will not change the meaning of the entire puzzle.

PROPOSAL OF A NEW INTELLIGENCE PROCESS PARADIGM

The traditional paradigm will remain essential for developing intelligence about traditional state-based threats, and the IC must preserve aspects of the intelligence enterprise that maintain its effectiveness. However, the nature of many transnational threats and trends warrants consideration of a different kind of paradigm for the intelligence process. This new approach replaces the notion of intelligence as solving puzzles with that of intelligence as performing "adaptive interpretations."

Adaptive interpretations involve constructing extremely complicated puzzles for which *virtually all of the pieces are available*. Furthermore, most pieces to adaptive interpretations are not secrets or mysteries.

Constructing adaptive interpretations is a two step process. Both steps must be performed simultaneously and continuously. The necessary pieces of information must be procured and assembled into an accurate picture. Because these pieces of information come from sources across the globe, solving adaptive interpretations requires a very high level of pre-arranged information sharing. In addition, all information must be continuously updated.

When dealing with adaptive interpretations, however, the situation is much more dynamic than under the traditional paradigm for two reasons. First, single pieces of information can change their value -- becoming much more or less significant – in short periods of time. This is also true for the relationships among pieces of information. Pieces that are relatively unrelated one moment can become significantly related the next. Accordingly, one should expect adaptive interpretations to constantly change their "picture," sometimes in dramatic ways. Second, in adaptive interpretations, small pieces of the puzzle can be decisive. In fact, most analyses requiring adaptive interpretations will not have any large pieces, only a vast number of small ones. This means that collectors, processors, and analysts need to find new ways to assign value to each small piece of collected information and to continuously reassess this value.

States already use adaptive interpretations to achieve certain important functions. The integrated systems for routing international mail and telecommunications provide some insight into adaptive interpretations. They involve a large-scale tracking system, and patterns change over time, requiring periodic adjustments of procedures. National and regional Maritime and air traffic control schemes are better examples of adaptive interpretations because they combine both complex data requirements dynamic change. For instance, all major U.S. ports maintain rigorous traffic separation and control schemes to allow commercial vessels to enter and leave

port safely and efficiently. All vessels above a certain displacement must file arrival and departure reports in advance, and must check-in with local authorities, who monitor vessels transiting through their area of responsibility. Similarly, air traffic control within the United States is a rigorous system that tracks virtually all aircraft – particularly commercial aircraft – throughout the country. The air traffic control system also interfaces with those of other countries. Aircraft leaving and entering U.S. airspace must check in with controllers at predetermined points. In both of these cases, the need to ensure public safety and to maintain public confidence in economically vital, high-visibility, capital-intensive industries have driven the development of these systems for achieving adaptive interpretations.

The United States is currently in the process of expanding both its air and maritime domain programs to provide an integrated national picture for purposes of homeland security. In the case of shipping, the goal of the "Maritime Domain Awareness"[3] program is to monitor shipping within 1,000 miles of the U.S. coastline so that any suspicious vessel can be intercepted and boarded well before it could perpetrate an attack. Similar identification and tracking schemes exist for air traffic. Both programs depend on the cooperation of a number of foreign governments as well as private firms around the world to provide information.

The U.S. Container Security Initiative (CSI) is another attempt at an adaptive interpretation, in this case one that improves the security of standardized shipping containers entering the United States. The CSI focuses on pre-screening cargo at its last port of call before arriving at a U.S. port. The goal is to reduce the efficacy of using containers to smuggle weapons of mass destruction (WMDs) and other terrorist equipment into the country while minimizing the impact of increased security on the flow of trade.[4]

All of these applications of adaptive interpretations involve processing large quantities of information in a dynamic environment where each piece is only a small piece of the overall bank of information. There are no large pieces to these puzzles. The purpose of these systems is to flag the very small number of overall aircraft or ships or cargo containers that pose a threat.

All of these examples have another thing in common. They involve activities – international communications, trade, public safety – that every responsible state and private firm support. Accordingly, both states and private firms are motivated to cooperate voluntarily to make them effective. While none of these systems can guarantee 100% success, they improve security while minimizing the negative effects on commerce. What if these systems operated on a fully integrated, global scale rather than within their current limited domains?

POTENTIAL APPLICATIONS OF THE NEW INTELLIGENCE PARADIGM

Many transnational security issues lend themselves to adaptive interpretations. Some issues will be much more difficult to solve than others. One way to improve the chances for success is to divide possible issues into three tiers, with Tier 1 being the easiest to solve and Tier 3 the most difficult.

Tier 1 systems would be comprised of expanded and integrated versions of existing systems related to commerce. For example, imagine a fully integrated global tracking system for shipping, air traffic, personal travel, and container routing. Anomalous or suspicious activity in one domain could be correlated with the other domains to look for patterns. Such a 'system of systems' could provide valuable intelligence concerning terrorism and criminal activity. For example, if a known terrorist had traveled to a point from which a suspicious container had been shipped, perhaps on a vessel that had raised concerns in the past, then red flags would be raised to focus increased attention. Under current processes, it is much less likely that such correlations would be detected, and efforts to do so would involve far more labor and time.

Such a system is not that far-fetched when one considers that, as noted above, several independent systems to track shipping, cargo containers, commercial aircraft, and passengers currently exist because of pressing needs separate from any intelligence function, such as public safety concerns, the desire to collect revenue, and economic efficacy. As a result, many of these systems enjoy a high degree of voluntary compliance. While much of the information in these systems is closely held by governments and private entities due to proprietary and privacy concerns, it also is shared among governments when deemed appropriate. It does not seem like such a large jump of imagination to visualize globally integrated versions of these systems in which large volumes of information are routinely exchanged across borders for the mutual benefit of all participants.

Tier 2 systems would involve tracking transnational issues that go beyond purely economic issues and address issues that, while not affecting national security directly, are often regarded as "sensitive" by state governments. For instance, a Tier 2 system might involve tracking sales and transfers of conventional arms. The U.N.-sponsored Register of Conventional Arms could serve as a starting point for an expanded system.[5] A system to detect and track the progression of infectious diseases would be another Tier 2 system. For example, many consider the World Health Organization's Global Outbreak Alert and Response System (GOARN) – an Internet-based system for reporting the outbreak of Sudden Acute Respiratory Syndrome (SARS) and other infectious diseases – the best method for detecting outbreaks. It uses reports by both private and public health care providers and, based on the 2003 SARS outbreak, appears to be more effective for signaling potential outbreaks than waiting for affected states to report them.[6]

Tier 3 systems involve information about security issues in the case of governments, and core strategies and activities in the case of private firms. As such, these will be the category of information that states and firms are least likely to submit into a global system. Tier 3 systems will track things such as biopathogen development and nuclear weapons inventories and thefts.

The fact that Tier 1 and Tier 2 systems are already being implemented in some areas is a testament to their value in combating transnational phenomena. Tier 3 systems are probably only likely to become possible when experience with Tier 1 and 2 systems demonstrates the value that adaptive interpretations can bring to bear on pressing transnational security concerns. How should these systems be developed further? Should some systems be integrated to help the IC solve particular adaptive interpretations? If so, what role should the IC play in this effort?

TWO PARADIGMS, ONE INTELLIGENCE COMMUNITY

The 21st century security environment leaves intelligence organizations in the position of needing to embrace two distinct paradigms to accomplish their mission. Intelligence organizations must apply the traditional puzzle-solving paradigm in the case of traditional state-based security threats, but they must use a new adaptive interpretation paradigm to address transnational threats. How should this be accomplished?

A major problem arises because the traditional model relies on secrecy, while solving adaptive interpretations relies on openness. The need for secrecy breeds mistrust among national intelligence organizations, foreign governments, and private enterprises, but openness requires mutual trust among all participants to succeed. This produces an apparent conundrum. Intelligence organizations' continuing need to solve puzzles requires secrecy, which breeds mistrust, but this mistrust prevents intelligence agencies from participating in adaptive interpretation processes, which are essential for dealing with transnational threats.

How can this conundrum be resolved? Since different approaches to information and knowledge sharing are at the heart of the matter, an examination of IC information flows can provide valuable insights.

INFORMATION FLOWS IN THE INTELLIGENCE ENTERPRISE

The U.S. government categorizes information as either secret ('classified') or open ('unclassified').[7] This means that any given piece of information originates from either secret or open sources, and is then used to compile either secret or open intelligence products. This means that four types of information flows are possible. Table 1 summarizes these flows, along with an example of each type.

TABLE 1 Information Flows in the Intelligence Enterprise

	Recipient of Information	secret	open
Source of Information			
secret		I. Intelligence about impending terrorist attack is derived from sensitive sources and methods, and then analyzed within traditional classified IC channels to produce a classified product to brief U.S. government officials.	III. Intelligence about impending terrorist attack to the U.S. homeland is derived from sensitive sources and methods, then sanitized and declassified for distribution to state and local law enforcement agencies.
open		II. CNN reports that large scale civil war has begun in Iraq. IC seeks correlation using classified sources and methods. All resulting products are secret, used to brief U.S. government officials.	IV. CNN reports the occurrence of several human Avian flu cases in Beijing. Used by U.S. Center for Disease Control to issue travel advisories for Americans planning trips to China.

Secret-to-secret (Block I) and open-to-secret (Block II) information flows are associated with the traditional intelligence enterprise. Both secrets and open sources are employed. However, secrets are valued more greatly than information derived from open sources, use of OSINT is not systematic, and all processing, exploitation, analysis and production remain within classified channels. Release of intelligence to U.S. government agencies outside the IC, to foreign governments, private firms, and the general public is the exception rather than the rule.

The need for secret-to-open information flows (Block III) has received increased attention since the 9/11 attacks, when it became apparent that all levels of government as well as private sector entities are important collectors, analysts, and consumers of intelligence in the U.S. homeland security effort. It also was recognized that existing information security classification and clearance systems impeded information sharing among these entities.

The last category – open-to-open information flows (Block IV) – has not been developed systematically by the IC, but its importance is recognized. For example, government officials constantly monitor what the major media outlets report since the media frequently are the first to break news of important events.

POST-9/11 REFORMS AND INFORMATION FLOWS

Since the 9/11 attacks, the heightened awareness of the need to collect intelligence against al Qaeda and other transnational terrorist groups has underscored the need to improve all four types of information flows in order to improve the sharing of both secret and open information across organizational boundaries. Given the widely dispersed, networked nature of these threats, the list of organizations that must share now includes not only IC and other U.S. government agencies but also, state, local, tribal, private, and foreign actors.

The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) mandated three principal reforms aimed at improving information sharing. First, IRTPA required the President to designate '…a single entity to oversee the security clearance process and develop uniform standards and policies for access to classified information. The President also designates a single entity to conduct clearance investigations….Reciprocity among clearances at the same level is required.'[8] Second, IRTPA emphasized the need for the Director of National Intelligence (DNI) to '…ensure that the IC makes efficient and effective use of open source information and analysis.'[9] This has led to the establishment of an 'Open Source Center' in the Office of the Director of National Intelligence (ODNI). The Open Source Center is responsible for ensuring that Osint is fully integrated into all IC processes. Third, IRTPA mandated that the President take action to establish an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information among all appropriate federal, state, local, tribal, and private sector entities through the use of policy guidelines and technologies.[10] The ISE is the agent to research, recommend, and monitor the implementation of any technological, legal, and policy changes to improve information sharing while preserving the security of classified material.

These reforms are firmly grounded in the traditional intelligence process paradigm and the understanding of information flows derived from it. In response to the need to increase sharing with many nontraditional partners, the IC has embarked on a program to provide security clearances for individuals in newly partnered organizations so that they can have access to classified information. This approach addresses this issue by expanding secret-to-secret information flows. An alternative approach would have been to design ways to declassify information so that state, local, tribal, and private partners could have access without the need for clearances. Is the IC's decision to expand secret-to-secret information flows the optimal course of action?

Similarly, the IC's approach to integrating Osint involves expanding open-to-secret information flows. The Open Source Center's mission is to improve Osint collection and integrate it into all aspects of intelligence analysis and production. This means that relevant Osint will be made available at the right time and place to support classified analysis. Once again, the approach has been to expand the universe of secret information. Is this appropriate?

Lastly, the ISE will be designed to support the other two mandates. This means it will enable greater sharing of secret-to-secret and open-to-secret information and knowledge.

Expanding the body of secret knowledge and the number of persons with access to it has a number of disadvantages. Expanding the number of individuals with clearances will prove expensive and time-consuming. It also runs the risk of being ineffective – after all, how long can information remain secure if hundreds or thousands of individuals have access to it?

However, choosing this course of action has one important advantage that overrules the disadvantages: it preserves the security of classified material, which is essential for maintaining the effectiveness of the traditional intelligence paradigm. Despite IRTPA's emphasis on greater knowledge sharing, all initiatives for this purpose must preserve the integrity of secret information. In most areas of the U.S. government, information is highly classified because it pertains to activities and capabilities the government prefers to keep secret, such as war planning, new weapons systems, or proposed negotiating strategies. In the case of intelligence, however, much of the most highly classified material has been assigned its classification because it involves particular types of collection activities. These are referred to as "sensitive sources and methods."[11] The information derived from sensitive sources and methods is highly classified because knowledge of the information gained from these sources and methods can be sufficient for an opponent to deduce their existence. Once the existence of a particular sensitive source or method becomes known, opponents can take actions to neutralize its effectiveness. Thus, effective security systems are absolutely essential if the IC is to learn secrets using sensitive sources and methods, and use the information derived from them to solve traditional intelligence puzzles. Given this need, the IC has been correct in expanding information sharing through secret-to-secret and open-to-secret channels. Efforts to expand open channels would jeopardize the effectiveness of the traditional paradigm.

At any rate, large-scale efforts to expand open channels would encounter serious problems. Security systems are designed to restrict access to classified information to the minimum number of individuals who need the information in order to perform their duties effectively. To achieve

this purpose, all individuals with security clearances are indoctrinated in the consequences for disclosure or loss of control of classified material. These consequences are not trivial. They can involve lengthy prison terms even when unauthorized disclosure of classified material is inadvertent. There currently are no countervailing incentives for sharing information. As a result, given the clear penalties for unauthorized disclosure of classified material, personnel subject to security classification programs will remain strongly biased toward withholding information, not sharing it.

Recognizing these facts is valuable, but it still fails to answer the question of how the IC will expand information sharing to include the very large number of actors needed to provide information to solve adaptive interpretations under the new intelligence paradigm. The sheer number of required partners, many if not most of whom are foreign, rules out extending security clearances to everyone in this group. Even if the IC could surmount this hurdle, the conundrum would still remain because expanding the domain of secret information in the IC will exacerbate mistrust among potential partners. Clearly the traditional view of IC information flows is inadequate to resolve this dilemma. A new conception of information flows is needed.

A NEW CONCEPTION OF INFORMATION FLOWS

The traditional concept of information flows is still relevant when the IC performs its traditional mission of solving puzzles using secrets and OSINT. This suggests that, rather than abandoning the traditional view in favor of a totally new conception of information flows, traditional flows should be augmented by new types in order to perform adaptive interpretations. A new conception of information is needed. This new view will include a new form of information known as 'trusted information' in addition to secret and open information.

Trusted information is circulated within 'trusted networks.' A trusted network is one in which all of the members are trusted to enter only validated information and to use network information responsibly. Within these constraints, network members can be any organization that can provide needed information. This will include government agencies, private firms, IGOs, NGOs, and even individuals in various informal communities of interest. Since their purpose is to address transnational issues and threats, trusted networks must be global in scope The overriding principal is that members of a trusted network must agree to share voluntarily their own information to be able to access the network's contents. In short, the network depends on mutual trust among its members.

Only the organizations that are members of the network have access to its information, and these organizations have access to all of the information in the network at all times. This means that trusted information is not open source information because it is not available to the public. Nor is trusted information classified information, since, its distribution is not restricted to the minimum number of people possible. In fact, distribution will be impossible to control, since members are free to use network information for any responsible purpose. Such uses would include use by a country's intelligence organizations. For example, in the United States, the IC could receive access to all or to selected network information from the U.S. government organization participating in the network. The IC could use this information as another

collection source, correlating it with various classified databases on the issue in question. At the same time, other national intelligence services might be using the trusted network information in the same or different ways.

Trusted information sharing systems will be increasingly important in the future as current transnational phenomena mature and new ones arise in response to increasing globalization and resource use. The IC will not be able to perform adaptive interpretations without them because it cannot procure the vast quantities of required information by itself. At the same time, the IC cannot be a member of these networks. Since effective networks depend on mutual trust among members, it will be essential that governments administer trusted networks using agencies that do not perform secret intelligence collection, conduct classified analysis, or produce classified products for very limited distribution. This rules out the use of the IC.

When trusted information is taken into account, a new conception of information flows comes into focus. This is outlined in Table 2. Blocks I, II, III, and IV are carried over unchanged from Table 1. They remain essential for solving traditional intelligence puzzles involving secrets. The new blocks of Table 2 give examples of ways that trusted information fits into the picture.

TABLE 2. New Information Flows for Solving Adaptive interpretations

Source ↓ / Recipient →		secret	**trusted**	open
secret		I. Intelligence about impending terrorist attack is derived from sensitive sources and methods, and then analyzed within traditional classified IC channels to produce a classified product to brief U.S. government officials.	**<u>Not applicable</u> Classified information does not migrate into trusted networks.**	III. Intelligence about impending terrorist attack to the U.S. homeland is derived from sensitive sources and methods, then sanitized and declassified for distribution to state and local law enforcement agencies.
trusted		**IC monitors trusted network containing global air travel information. Looks for correlations with IC's classified terrorist watchlist. Results remain classified.**	**Every member of a trusted network has access to all of the network's information all of the time.**	**Center for Disease Control monitors trusted network for global disease reporting. Issues warnings to American public when warranted.**
open		II. CNN reports that large scale civil war has begun in Iraq. IC seeks correlation using classified sources and methods All resulting products are secret, used to brief U.S. government officials.	**CNN reports the occurrence of several human Avian flu cases in Hong Kong. Center for Disease Control looks for additional evidence in trusted network.**	IV. CNN reports the occurrence of several human Avian flu cases in Hong Kong. Used by U.S. Center for Disease Control to issue travel advisories for Americans planning trips to China.

Trusted information networks will provide the kinds of information needed to construct adaptive interpretations concerning transnational issues and threats. However, if national intelligence organizations can't participate as members, how will they relate to trusted networks and the valuable information they contain?

IMPLICATIONS: WHAT IS INTELLIGENCE?

Liberal democracies tend to define intelligence in one of two ways. These are generally referred to as the American and British definitions of intelligence, although each represents an idealized view for purposes of discussion rather than an accurate depiction of each country's approach. As Philip H.J. Davies explains:

> In his 1996 *Intelligence Power in Peace and War*, British scholar and former intelligence officer Michael Herman tried to present the range of conceptualizations of intelligence as a spectrum, ranging from the broad definitions that approach intelligence primarily as "all-source analysis" (typified by [Sherman] Kent's view) to narrow interpretations that focus on intelligence collection, particularly covert collection. Herman notes in passing that the broader interpretations tend to be favored by US writers and narrow approaches by the British.[12]

Davies goes on to describe the American definition of intelligence:

> In current usage, "intelligence" in US parlance tends to refer to "finished" intelligence that has been put through the all-source analysis process and turned into a product that can provide advice and options for decision makers. Perhaps the classic US definition comes from a past edition of the Dictionary of United States Military Terms for Joint Usage, which states that intelligence is "the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or areas of operation which is immediately or potentially significant for planning." This definition includes the collection of raw information, but the end result does not become "intelligence" as such until it has been thoroughly analyzed. Hence, in the US context, intelligence production means analytical production.[13]

Regarding British practice:

> …, in British practice, raw intelligence moves straight into policymaking circles without passing through a separate, intervening analytical stage. This is not because there is no assessment process but because all-source analysis is subsumed by the civil service employees who, in their role as advisors to ministers of the crown, take ultimate responsibility for the policies and actions of their departments before Parliament. As a result, intelligence as such tends to refer more narrowly to those kinds of information not available from the "normal product" of departmental activity.[14]

Taken together, the concept of trusted information and the narrow British definition of intelligence offer a solution to the conundrum. Foreign government and private concerns are much more likely to cooperate with U.S. government departments and agencies that do not involve themselves in the business of discovering secrets. While all understand that some part of governments must perform this function, the important factor is to distance those agencies involved in espionage and other secret collection activities from those involved in open, mutual exchange of information through trusted networks. One way to do this is to reduce the scope of U.S. 'intelligence' to make it more closely resemble the British definition of intelligence while simultaneously constructing some U.S. government entity to serve as an interface for the country's participation in trusted networks.

A NEW U.S. GOVERNMENT INFORMATION ENTERPRISE

Under this new approach, the 'new' intelligence community (new IC) would retain those functions and activities associated with the collection of secrets. This would include:

- All secret collection activities, including human intelligence (Humint). This would include imagery intelligence, signals intelligence, measurement and signatures intelligence, and Humint. Humint should be conducted by case officers on a non-official cover basis so that other parts of the government such as the State and Commerce Departments can dissociate themselves from secret collection activities. Diplomats and trade attaches would still observe and report on developments in the countries where they were posted, but these activities are sufficiently time-honored as to be an exception to the rule.
- All covert action. These capabilities would be under the control of the National Clandestine Service.
- All defense-related intelligence activities. These activities would fall under the direct control of the Secretary of Defense to make it clear that it was part of the military establishment. Current Army, Navy, Marine Corps, Air Force, and Special Operations Command Intelligence organizations would remain essentially unchanged since they directly support their respective military branches.
- All counterintelligence activities. The FBI would continue to perform its counterintelligence function as well as its law enforcement role in apprehending terrorists.

If one were to conform to the strict British definition of intelligence, the current all-source analytic functions of the Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), and the State Department's Office of Intelligence and Research (INR) would be disestablished, then 'normalized' by incorporating their analysts and managers into analytic staffs in the Departments of Defense, State, and other departments as appropriate. With exception of the CIA, this is not really a change. The DIA is already in the Department of Defense, INR is in the State Department. The same holds true for analytic offices in the Treasury, Energy, and Homeland Security Departments. These normalized agencies would receive any secrets discovered by the new IC and would incorporate them into their analyses. In general, the rule would be to keep secret collection, processing and exploitation activities within the new IC and divest other activities into mainstream government departments as much as possible. Under the

new system, offices charges with analysis also would have access to information from trusted networks.

Outside of the new IC, an Office of Strategic Information (OSI) would constitute the U.S. component of trusted networks. The OSI would input U.S. information into the integrated global trusted information networks for legal activities such as shipping, air traffic, cargo movements, and passenger travel. Since these kinds of activities are generally not controversial and since the OSI was not involved in learning secrets, most countries and private entities would be willing to participate because of the system's clear benefits to commerce, travel, and security. Hopefully, as these Tier 1 activities became validated, Tier 2 activities (infectious disease reporting, arms transfers) and even Tier 3 activities (biopathogen developments) could be added to the list of trusted networks in which the United States was a trusted partner.

OSI networks would constitute an innovative collection source for the new IC. Integration of the large volume of information from Tier 1 networks alone – travel, finance, and trade, informaiton – could prove invaluable for analyzing both emerging and current transnational trends and issues. For example, Tier 1 integrated network analysis could provide information about terrorist plans, smuggling, and other kinds of illegal activity, particularly when combined with the new IC's secret collection efforts.

Identifying and integrating data on this scale will require data mining on a scale never before envisioned. While challenging, this is a blessing in disguise. Although all members of trusted networks have access to network information, none can approach the technological ability of the United States to exploit this data. Thus, successfully tapping into trusted network information will impart a significant asymmetrical advantage to the United Stares.

The OSI could not perform this function because the results of data mining would be classified, and the OSI must not deal in secret information if it is to preserve the trust of its network partners. Rather, the mining and integration of trusted network information would need to be performed by a part of the new IC. This would be a new agency devoted solely to this new collection method, perhaps a new CIA directorate or an entirely new agency, as long as it is not tied to any one cabinet department. The existence of this agency would be kept as secret as possible. The less attention drawn to the fact that the new IC is exploiting trusted network information the better.

Analysts in the various cabinet departments would seek to make sense of the raw intelligence provided from new IC collection activities – including trusted network analyses performed by the new data mining agency – and from Osint. The successful marriage of traditional secret collection activities, new trusted network data mining techniques, and Osint should give the United States a decided edge over its adversaries, both national and transnational ones.

SUMMARY AND CONCLUSIONS

This paper has proposed eight propositions that argue for a transformation in the U.S. intelligence enterprise.

Proposition 1. Transnational security issues are becoming increasingly important to international security. These types of potential threats tend to be diffused in nature and require preemptive rather than reactive action to counter successfully. The magnitude and nature of this challenge means that governments and private entities must be willing and able to share voluntarily large amounts of information.

Proposition 2. The traditional paradigm compares the intelligence process to solving a puzzle in which some pieces are secrets, some are mysteries, and some are found in open sources. Moreover, some pieces of the puzzle are always missing. While essential for dealing with traditional state-based security concerns, this model is not effective for addressing transnational threats.

Proposition 3. A new paradigm, called a complex solution, is needed to understand and deal with many transnational security threats. Adaptive interpretations are extremely complex puzzles for which virtually all pieces are available. While some of these threats (terrorism) still require the discovery of secrets and mysteries, others require the capability to process huge amounts of open information provided by many sources.

Proposition 4. Intelligence organizations need to solve puzzles and work adaptive interpretations simultaneously, which poses an apparent conundrum. Solving puzzles requires learning secrets, which engenders mistrust among foreign actors. Performing adaptive interpretations requires openness, which requires mutual trust among both foreign and domestic partners.

Proposition 5. The traditional paradigm rests on the view that all information is either secret or open. To preserve the sensitive sources and methods upon which the collection of secrets depends, the IC must maintain strict security practices. Thus, mandates to increase knowledge and information sharing tend to be accomplished through expanding secret information flows by increasing the number of persons with security clearances and the amount of secret information. This approach is unavoidable if the IC is to preserve its capability to employ the traditional paradigm.

Proposition 6. The new paradigm depends on a new view of information, one that includes a new category – trusted information – in addition to secret and open information. Trusted information is contained in trusted networks, which have many participants, including nonstate entities.

Proposition 7. The IC cannot be associated with trusted networks, because this would undermine the mutual trust needed to make trusted networks effective. However, the IC needs access to trusted information to perform adaptive interpretations in the new paradigm. The conundrum can be resolved by adopting a narrow definition of intelligence as secret intelligence only. This approach conforms to the traditional British understanding of intelligence. If intelligence only involves learning secrets, then other activities commonly associated with intelligence in America, such as analysis of a wide range of issues, become normal functions of government rather than intelligence. By casting the intelligence function as highly focused and distinct from the ‘normal’ operation of the U.S. government, foreign states and private firms should be more

inclined to cooperate with mainstream U.S. government agencies to provide trusted information necessary for performing adaptive interpretations.

Proposition 8. The U.S. intelligence community should be restructured so that it only includes secret collection activities and covert action capabilities. A new Office of Strategic Information (OSI) should be established to collect and process trusted information on a wide range of issues. Network partners would agree to share information because doing so would improve commerce and public safety in a number of open, legal, and accepted ways. The OSI would integrate and analyze network information to identify and analyze anomalies that might signal the start of an epidemic, an impending disaster, or a planned terrorist attack. It would forward such information to appropriate intelligence and law enforcement agencies, which could add value through their secret collection activities. However, all information in OSI-administered trusted networks would remain open and available to all partners, and the OSI would not use secret information from the intelligence community.

These eight propositions argue for a radical departure – a 'Revolution in Intelligence Affairs' or a radical 'transformation' – from current practices in the intelligence enterprise.[15] While the recommendations concerning the structure of the new U.S. information enterprise are preliminary and require further study, the general direction appears clear. The United States and other countries need to develop a new apparatus of government capable of integrating vast streams of information from a number of foreign and domestic sources if transnational threats are to be combated successfully. This information will have to be shared voluntarily since it is not collectable through traditional clandestine means. To accomplish such voluntary openness, developing ways to forge mutual trust are paramount. At the same time, however, it is vitally important to preserve the IC's ability to deal effectively with threats to U.S. security from traditional sources.

---

[1] This section is excerpted from William J. Lahneman, *The Future of Intelligence Analysis Project Final Report*, March 10, 2006, Center for International and Security Studies at Maryland. Study commissioned by the Office of the Director of National Intelligence. Available at www.cissm.umd.edu. John Steinbruner, CISSM's Director, drafted an earlier version of this section of the report.

[2] For an appreciation of the uncertainty surrounding how the world of 2020 might develop, see the alternative future scenarios in *Mapping the Global Future: Report of the National Intelligence Council's 2020 Project Based on Consultations With Nongovernment Experts Around the World* (Government Printing Office, December 2004). Available at http://www.cia.gov/nic/NIC_globaltrend2020.html.

[3] Frank Hoffman, 'Border Security: Closing the Ingenuity Gap', in Russell Howard et al (eds.) *Homeland Security and Terrorism: Readings and interpretations* (New York: McGraw-Hill, 2006) p.149.

[4] Jane A. Bullock et al, *Introduction to Homeland Security*, 2nd Ed. (Boston: Elsevier, 2006) p.66.

[5] A global system with this goal – the Register of Conventional Arms – already exists under United National sponsorship. However, many states do not participate. For more information, see http://disarmament.un.org/cab/register.html.

[6] For more information about the GOARN, see http://www.who.int/csr/outbreaknetwork/en/.

[7] There are three categories of classified material: 'Confidential,' 'Secret,' and 'Top Secret.' Confidential material contains information that, if disclosed to unauthorized parties, 'could be expected to cause damage to the national security.' Inadvertent disclosure of Secret material would cause 'serious damage,' while release of Top Secret material could cause 'exceptionally grave damage.' Quoted from Executive Order 13292 of March 25, 2003. Described in Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, D.C.: CQ Press, 2006) p.74. The Top Secret (TS) classification has a number of subcategories within it, which are denoted by code words. These subcategories pertain to 'sensitive compartmented information,' which means that the information is

associated with a particular sensitive project or operation to which only a small group of individuals have access. Individuals must meet two requirements before being given access to classified material. First, they must have the appropriate security clearance. A person is cleared for access to classified information following a background investigation during which security personnel research details of the person's life to see if there are any factors that might make him or her a security risk. Second, an individual must have a 'need to know' to be granted access to particular classified information. For instance, a person with a Top Secret clearance will only be granted access to the TS material that pertains to his or her current assignment. Access is revoked as soon as the person no longer has a need to know.

[8] Summary of *Intelligence Reform and Terrorism Prevention Act of 2004*, December 6, 2004, p.10.

[9] Ibid., p.9.

[10] Ibid., p.5-6.

[11] For example, if the CIA has recruited an agent who is a high official in the North Korean government, this agent would be a sensitive source. Similarly, a new technology that greatly improves U.S. ability to track submerged submarines would be an example of a sensitive method.

[12] Philip H.J. Davies, 'Ideas of Intelligence: Divergent National Concepts and Institutions', *Harvard International Review* 24/3 (September 2002) pp.62-67.

[13] Ibid.. pp.62-67.

[14] Ibid.. pp.62-67.

[15] For an argument that an RIA is occurring, see William J. Lahneman, 'Is a Revolution in Intelligence Affairs Occurring', *International Journal of Intelligence and Counterintelligence* 20/1 (Spring 2007), pp. 1-17.