Building an Integrated Intelligence Network: Challenges and Opportunities

Dr. Pete Rustan
Director, Ground Enterprise Directorate
National Reconnaissance Office
Chantilly, Virginia

Our adversaries, ranging from nation states to terrorist groups, take full advantage of information available on the internet and have deployed many networks to conduct their operations. In today's information technology (IT) world, we must fight their networks with an intelligence network much more powerful than anything available to them. People often state it takes a network to fight a network; but I contend it takes much more than that, it takes a more powerful and fully integrated network, with increased access, enhanced content, and reduced timelines. The National Reconnaissance Office's (NRO) vision is a fully integrated Department of Defense/Intelligence Community (DoD/IC) network, where information is virtual, assured, available on demand, and globally accessible to authorized users empowered with the tools and services necessary to generate tailored, timely, trusted, and actionable intelligence products. This architecture must operate as efficiently as the best commercial IT and knowledge service networks, and enable authorized users to receive, task, and query trusted information on-demand to improve the speed and execution of decisions from anywhere in the world. This article describes the challenges the NRO faces as we develop information products and services for use across the DoD and IC that ride on this powerful network with accurate and timely intelligence information on any problem of interest. Additionally, this article describes the tremendous opportunities available as we build this integrated intelligence network.

Over the past 48 years, the NRO has been known as the premier acquirer and operator of the nation's space reconnaissance capabilities. However, in today's world, the NRO also needs to work with our partners in the DoD and the IC to add more value to the data the NRO collects and provides to warfighters and intelligence analysts. While the NRO must maintain and continue to build on its expertise in system acquisition and operational excellence, it must also transform itself into a world class provider of information products and services. To start this transformation, the NRO must work with the National Geospatial Agency (NGA) and the National Security Agency (NSA) to build an integrated and scalable ground architecture capable of fusing overhead geospatial intelligence and signals intelligence with air and ground based collectors, as well as integrating other sources of information. This NRO, NGA, and NSA collaboration will provide new information products and services through an enhanced multi-intelligence (multi-INT) framework that is not possible using today's business model. In addition, we must build on our information assurance capabilities to securely share data with our mission partners and users. Our business should leverage the streamlined business practices used by the expanding commercial information technology/information services (IT/IS) industry, including the implementation of a service oriented architecture (SOA), migrating our infrastructure to commercial-like data centers, and capitalize on economies of scale by leveraging system commonality.

Challenges and Opportunities

Figure 1 illustrates some of the major challenges facing the community, and a rough estimate of the percentage of effort

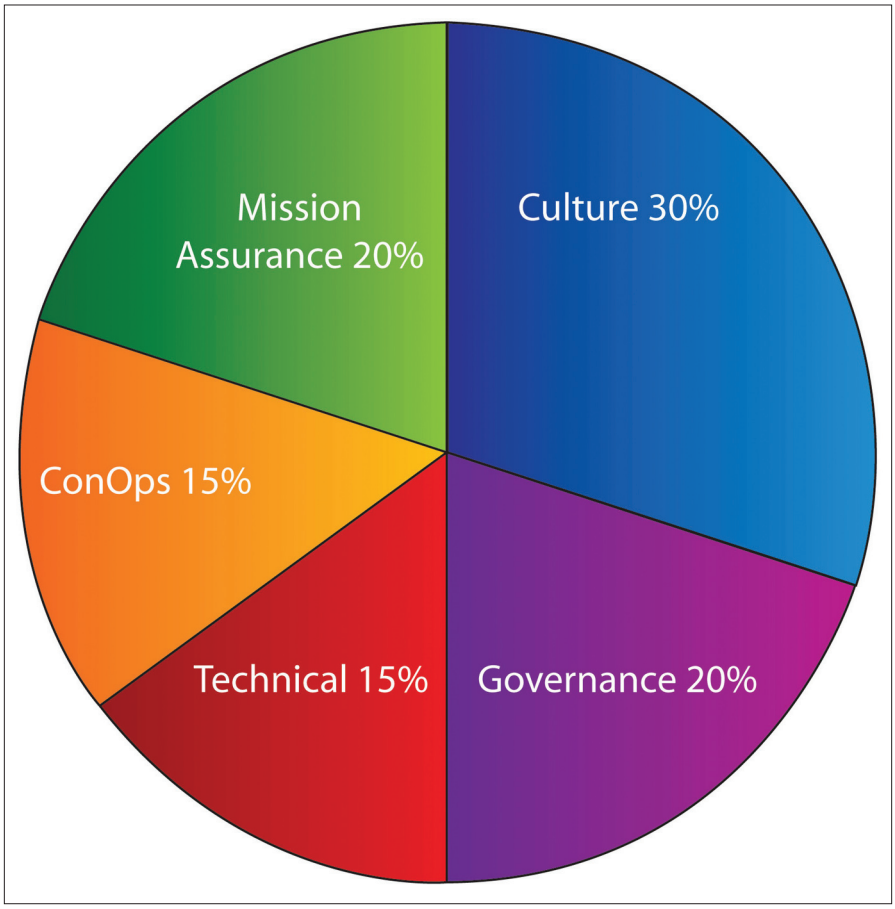

Figure 1. Challenges facing the Department of Defense/Intelligence Community in building a fully integrated intelligence network.

required for each category. Next, we will discuss these challenges and the potential opportunities available to solve these problems.

Cultural Challenge – 30 Percent

There are two aspects of the cultural challenge. The first deals with the need to adopt commercial business practices, the second relates to information sharing. Global geopolitical challenges, when coupled with the ever expanding capabilities of the commercial IT market, demand a completely new approach to solving present and future intelligence challenges. Unfortunately, the largest and most established government organizations offer the strongest resistance to change because they have become highly bureaucratic, generally following processes established prior to the advent of the internet. Human nature is such that people often get attached to existing procedures and do not change their approach, even when the problem or circumstances surrounding the initial conditions have changed significantly. There is also potential risk in change because one cannot predict the intended and unintended consequences of the new methods being proposed. As a result, our bureaucratic organizations have become very risk averse. We have established a multitude of processes that require inordinate amounts of time to execute (even for small tasks) and we have become unwilling to tolerate any changes.

The recapitalization cycle for successful IT businesses is measured in months, not years, and we must adopt their streamlined business practices into our acquisition strategies. A significant barrier is the amount of existing infrastructure that has been built up over many years. It would seem much easier to build a brand new system from scratch to achieve a given set of capabilities than to evolve a legacy system. Legacy systems generally have a number of unique and highly customized designs focused on solving very specific problems. They are difficult to modify and generally limit the government to a small group of contractors, or even a single contractor, who can perform the work required to make them interoperable. Unfortunately, the upfront costs associated with a "clean slate" approach are often too high in the near term, and the risk to existing operations threaten their approval even though their successful implementation would result in increased capabilities and long-term lower costs.

We must also embrace the open standards that are being widely accepted throughout the IT/IS industry to enable us to become more flexible and agile in our responses. Open standards give us access to a broader commercial industry base and should also reduce the overhead associated with test and integration as compared to traditional customized solutions. Finally, we must move away from one-of-a-kind, monolithic acquisitions that required years, if not decades, to build with no margin for error. The future of space acquisition must be based on larger constellations of smaller, cheaper platforms, that plug into modular ground systems (acquired separately from the satellites) using the latest commercial IT developments.

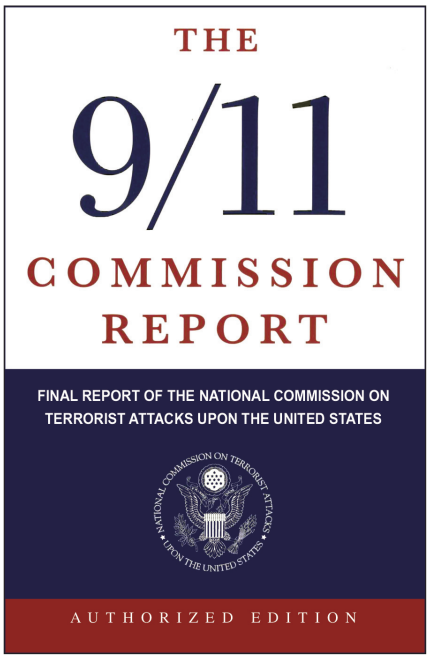

Figure 2. The 9/11 Commission Report.

Information sharing is another cultural change that must be addressed. The terrorist attacks on 11 September 2001 forced us to begin the process of breaking down cultural barriers within the DoD and the IC, and sparked the beginning of a fundamental transformation to meet the changing threat environment. The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) proposed sweeping changes to the IC. The 108th Congress passed several of the proposals, referred to today as the Intelligence Reform and Terrorism Prevention Action of 2004, that were signed into law by President George W. Bush. In October 2005, the director of National Intelligence (DNI) published the nation's first National Intelligence Strategy (NIS). The strategy called for integrating domestic and foreign US intelligence and aimed at eliminating gaps in our understanding of threats to our national security, bringing more depth and accuracy to intelligence analysis, and ensuring US resources are used to define future capabilities as well as present results.

Today, the military services and IC organizations do not work as a fully integrated entity and do not have effective mechanisms for making all data available to each other using standard formats. Many policy barriers still exist within the DoD and IC restricting the disclosure of classified information based on a "need to know" philosophy. These policies must migrate to a "responsibility to share" mindset to support the prosecution of a much more agile enemy and to allow us to take advantage of the information sharing technologies that we have become so familiar with on the Internet. From my perspective, the most important capability we must have to address present challenges is an integrated intelligence network. So far, our established culture has prevented the DoD and IC from building a unified network with the ability to deliver fused information products and services from various collectors directly to our user community.

Unfortunately, the largest and most established government organizations offer the strongest resistance to change because they have become highly bureaucratic, generally following processes established prior to the advent of the internet.

If we can address these cultural problems, we will deliver enhanced information products and services based on multiple collectors over an interoperable network to yield far greater intelligence. Users should be able to make improvements to existing intelligence products and create new ones with the knowledge that the available information is assured and secure. We should work with the users to build interactive tools and services, accessible through common interfaces, to tailor multi-INT information to meet their specific needs. Each system and information stream produced by the DoD and IC should become a data feed accessible by authorized users.

Governance Challenge – 20 Percent

DoD and IC agencies are tied to their functional managerial roles that were established by policies written when we faced a different enemy and when we did not have access to the information technologies available today. These organizations will have to shed outdated roles to create a virtual enterprise. Breaking existing functional relationships are difficult without strong leadership and direct guidance from the president and the National Security Council. To break the governance barriers, new sets of governing rules will have to be provided.

To improve mission performance, expand information sharing, and reduce the cost of ownership, the IC and the DoD have created the Integrated Intelligence Architecture Leadership Board (IIALB). The IIALB provides a forum to jointly evaluate and structure solutions to network interoperability problems. A DoD-IC Joint Technical Board (JTB), reporting to the IIALB, manages and coordinates solutions to the identified and prioritized interoperability needs. The JTB applies a business model to determine the optimal level of federated versus unified execution as well as the resulting and appropriate governance model. The IIALB governance body should provide effective management to ensure every piece of information is discoverable and accessible in real-time.

Mission Assurance Challenge – 20 Percent

Users must know that the data has not been altered, modified, or tampered with in any way and that the information provided is from a trusted source. Making security transparent to the customers, without system performance degradation and complexity, is an enormous challenge but vital to delivering trusted information to the users. Integrating security mechanisms into the integrated ground architecture and providing them as a service will preclude providers from having to develop and implement unique solutions. A cohesive and deliberate approach to security and mission assurance is fundamental to addressing the customers' needs.

Technical Challenge – 15 Percent

Intelligence analysts, warfighters, policymakers, and other decision makers require on-demand access to information products and services with assured content. Our objectives, milestones, and performance metrics are all designed to fulfill that fundamental need in the community. That need applies to a wide range of intelligence problems, including but not limited to:

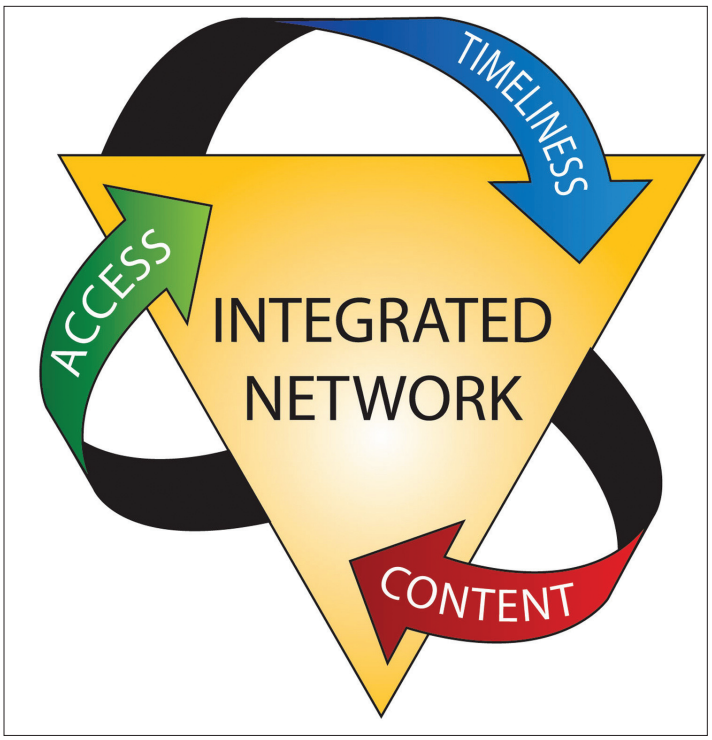

Figure 3. Improvement Focus Areas.

- monitoring weapons of mass destruction
- countering the threat of improvised explosive devices
- global war on terror
- combat search and rescue support
- high value target location and tracking
- drug interdiction and ship tracking
- missile launch detection
- weapon and space system performance characterization
- strategic indications and warning

Our technical challenge is to ACT (access, content, timeliness) by building an integrated and interoperable DoD/IC network, providing expanded access, enhanced content, and reduced timeliness:

Access. Users, regardless of their role, require relevant data and information to be readily available. Common, user-friendly interfaces that simplify their ability to produce, discover, acquire, understand, and use intelligence, regardless of its data sources or types, are critical to operational success. Our approach is to work with our partners to post all information products and services at the earliest point of consumability instead of only delivering those information products and services to individuals that request the information.

Content. Users will always demand continuously improving information content, from both new and existing information products and services. Improved performance characteristics such as better geolocation, improved product quality, and data fusion across all collection platforms are central to our intelligence needs. Analysts must also be able to combine real-time information with information collected in the past to determine strategic and tactical changes.

Timeliness. Users demand the information they need, when they need it, and have little patience for delays resulting from

disparate systems and dissemination mechanisms. While the specific requirements for different user groups vary, a war fighter's decision timeline may be dramatically shorter than an analyst tracking a strategic threat. The bottom line is that users need their information on their timelines.

To make ACT a reality we must integrate our ground infrastructure. The mission processing, mission management, and command and control areas have to be optimized to ensure that every new or existing operational system complies with a common set of standards to facilitate multi-mission tasking and data integration. Where necessary, we will migrate legacy systems to new common standards. We will take advantage of commonalities in existing systems and systems in development to eliminate redundancy and maximize interoperability. We will no longer build customized ground systems tailored to specific spacecraft; instead, we will acquire ground systems as an enterprise using the best available commercial technologies for future systems.

We must enable dissemination of data to our forces in the field to the "last tactical mile." This will require a two pronged approach where we continuously enhance the speed and capacity of the networks while investigating data format changes that allow data streaming in real-time over low bandwidth communications.

Overcoming these technical challenges will enable a fundamental shift in how intelligence is collected, processed, disseminated, and exploited. It will require a complete transformation of our ground architecture, without the disruption of current operations, and the development of new, multi-INT information products and services. Fortunately, there are no technical miracles needed to fulfill these needs.

Concept of Operations Challenge – 15 Percent

Our end state will be an IC enterprise that operates as efficiently as the best commercial IT and knowledge service companies, enabling authorized users to receive, task, and query trusted information on-demand to improve the speed and execution of decisions from anywhere in the world. Our intelligence network must be designed to anticipate mission needs for information by making the complete spectrum of sources of information seamlessly fused and available to the users. Our concept of operations will encourage new collaboration opportunities with improved analytic practices. It will operate like the best commercial IT networks, using common standards and cost-effective enterprise-wide IT services. It will provide users with common administrative and operational services accessible through a common desktop operating across multiple security levels based on the user's credentials.

Implementing the Vision

Figure 4 shows five key enablers to implementing this vision: SOA, Distributed Common Ground System-IC (DCGS-IC), network consolidation, data centers, and economies of scale. The adoption of SOA is one of the largest trends in commercial markets today. SOAs foster innovation and agile development by focusing on the service provided and not on the specific implementation behind the service. This enables service managers to modify a service to enhance the user's experience without changing the fundamental service provided. The implementation of SOA is directly tied to the use of open standards that enable us to evolve away from customized solutions and foster greater access to information than ever before.

DCGS-IC is a collaborative SOA effort to share data, information, intelligence, and services across the IC in a net-centric manner consistent with the emerging DoD DCGS and Joint Intelligence Operations Command (JIOC) enterprises. It is designed to meet the community requirement for information at the earliest point of consumability, ensuring the unique data and services provided by the NRO are interoperable, discoverable, accessible, and usable by the DoD and IC. Our desired network should leverage the large DoD investment in developing the architecture, standards, documentation, and tools for the defense industrial base. The attributes we are striving to achieve with our implementation are:

- common core services and infrastructure

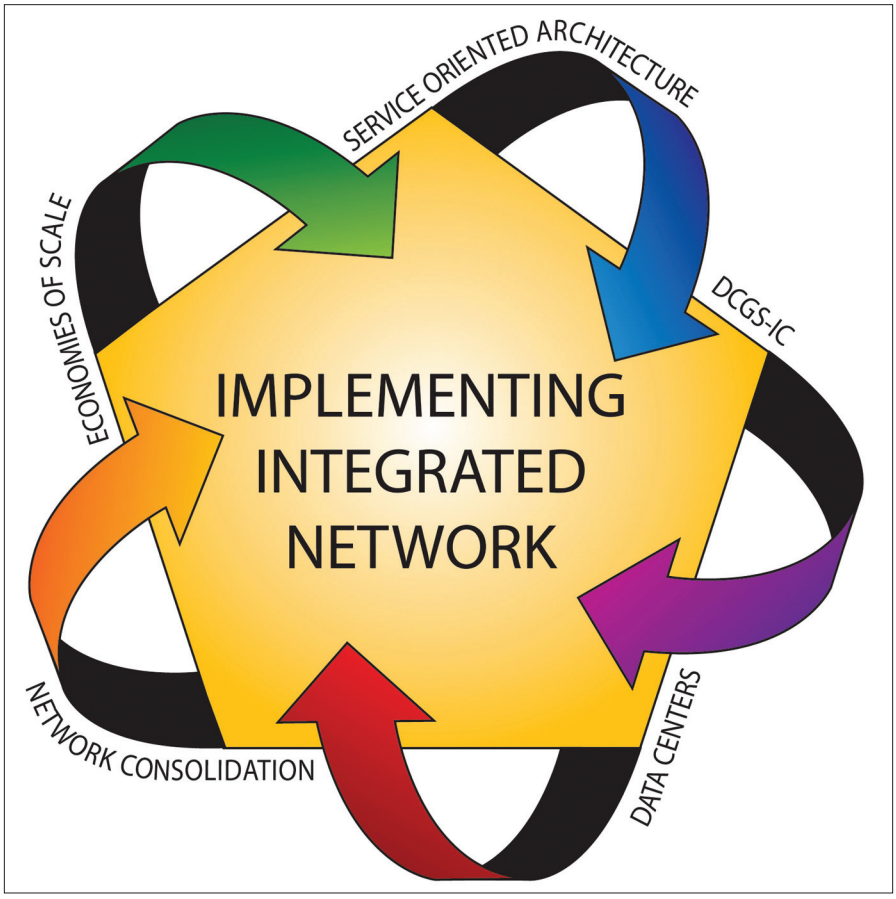

Figure 4. Five Key Enablers for Implementing the Vision.

… we can leverage economies of scale by developing integrated mission management, mission processing, and command and control. We should no longer build a specific ground system for each spacecraft, but build a basic, common architecture for new systems to "plug into" with minimum customization.

- re-use of services
- single query access to multiple intelligence sources
- delivery of unique, net-enabled value added IC services
- ubiquitous, common-standard visualization interface
- discoverable data and services
- global situational awareness
- rapid acquisition and transition of new capabilities
- use of "live/real" data for testing

Network consolidation is essential to the success of our SOA efforts. It is also in line with DNI and the chairman, Joint Chiefs of Staffs' strategic guidance to establish a single information environment across the community. We are engaging with the DNI chief information officer and our mission partners to enable community collaboration across a peered federation of DoD and IC enterprise frameworks. There are two essential steps. First, NRO, NGA, and NSA should work together as one entity operating on one network. Then, all available intelligence, whether from the DoD intelligence organizations or the IC, should be integrated into the same network.

A growing trend in the commercial IT market is the use of data centers. Data centers provide extraordinary opportunity for integration of mission data and applications, effective tipping and cueing, multi-INT data fusion, and hardware and software cost savings by capitalizing on mission commonality. Data centers can also provide a common repository for mission data archiving. By merging our data into master data repositories across agencies, we can ensure the pedigree of our data and provide our customers with a flexible platform capable of meeting their needs.

Finally, we can leverage economies of scale by developing integrated mission management, mission processing, and command and control. We should no longer build a specific ground system for each spacecraft, but build a basic, common architecture for new systems to "plug into" with minimum customization. Depending on the model being used, one can demonstrate that between 50 percent and 80 percent of the mission management, mission processing, and command and control are the same regardless of the specific spacecraft mission. Consolidating these functions using data centers and operating the spacecraft using SOA should provide economies of scale.

Summary

This article describes the capabilities that could be available to the DoD and IC if we build an integrated interoperable intelligence network. It addresses challenges and opportunities, including culture, governance, mission assurance, technical, and concept of operations. It also presents the next steps required to achieve this vision. That is, accelerating the development of SOA, DCGS-IC, network consolidation, data centers, and benefiting from economies of scale to achieve the best value proposition.

The author encourages collaborative developments between the various IC agencies and the DoD to build information products and services based on data collected from multi-INT sensors. We must proceed with a sense of urgency since today's problems cannot be addressed effectively unless these information products and services are made available on an integrated and interoperable intelligence network that is more powerful than anything available to the enemy. To prevent future attacks on the US and our allies, we must take immediate action to build this kind of integrated intelligence network.

Dr. Pete Rustan (BSEE and MSEE, Illinois Institute of Technology, Chicago; PhD, Electrical Engineering, University of Florida) is the first director, Ground Enterprise Directorate (D/GED), National Reconnaissance Office (NRO), after serving as the NRO's director of Advanced Systems and Technology for over four years.

Dr. Rustan served a 26 year career in the United States Air Force, where he distinguished himself in the management of seven spacecraft development programs that used advanced technologies and implemented the "faster, cheaper, and better" approach to acquiring space systems. He was the mission manager for the Clementine spacecraft, which mapped the surface of the moon and obtained more than 1.8 million images using 11 spectral bands. The construction and testing of the Clementine mission took just 22 months from concept to launch and cost only $80 million. The Clementine mission demonstrated for the first time that a fairly sophisticated spacecraft with six cameras could be built on a shortened schedule. Of scientific note, Clementine's radar returns strongly suggested the presence of ice on the moon's South Pole.

During his last tour of duty in the military, which was coincidentally at the NRO, Dr. Rustan promoted and demonstrated that NRO mission objectives could be met by building a constellation of smaller and cheaper systems. Dr. Rustan remains an advocate for rapid prototyping and selecting the best value proposition that addresses our intelligence needs.

Dr. Rustan has received many national and international awards, including the Aviation Week and Space Technology Laureate and Hall of Fame, the Disney Discovery Award for Technological Innovation, the National Space Club Astronautics Engineer Award, the NASA Outstanding Leadership Medal, and was featured by *Space News* in their Top 100 in Space 1989–2004.