BAE SYSTEMS

AN APPROACH TO REALIZING THE POTENTIAL OF INFORMATION OPERATIONS

Submitted by Gregory C. Crystal, Advanced Systems and Technology Division, BAE SYSTEMS Intelligence & Electronic Warfare Systems, MER15-2222, PO Box 868, Nashua, NH, 03061-0868, (603) 885-9573, fax (603) 885-3177, gregory.c.crystal@baesystems.com

ABSTRACT

The differing Service, Joint Staff, and defense agency interpretations and definitions of Information Operations (IO) arein fact fairly similar, but significant application differences can be easily noted. Coupled with continued stove-piping within domain areas, these operational differences and an unfocused IO defense-wide funding plan are creating difficulties in successfully implementing IO and will continue to make its potential benefits very difficult to realize in the future. The underlying purpose of Information Operations, regardless of which definition is used, is to enhance the decision making process of friendly forces while at the same time disrupting the enemy's decision making process. Some improvements in the friendly decision making process have occurred by the straightforward application of technology, but the full potential of IO has continued to be hampered by the difficulty of moving information between stove-pipes. Our approach to IO is to build a fully integrated system starting at the component level and is applied initially to the C4ISR functions of IO. Information Technology is the enabler for this to occur from the aperture to data links and displays. This paper will focus on the design of Intelligence, Surveillance, and Reconnaissance (ISR) multi-functional payloads using common modules, standard architectures, and standard interfaces to achieve dramatic improvements in the IO/OODA timeline.

INTRODUCTION:

We are a nation on the verge of a leap into the future, decisively engaged in fully transitioning to the Information Age of more, better, faster and smaller. Unfortunately, we have been on that precipice for years. In the early 1990's the continuing advances in computing and communications speed and capacity, powered by "Moore's Law," drove significant changes in the Department of Defense's view of the nature of future conflicts. The potential improvements in the decision making process, operational effectiveness and timelines, support function efficiency and timelines, etc. drove acceptance that future conflicts will occur not just on land, sea, space, or air, but also in the information realm. That realization was accompanied by the understanding that information is more that just a supporting resource, it is a critical asset which can be both a weapon and a target. The terms Information Superiority (IS) (or Dominance), Information Operations (IO), and Information Warfare (IW) were coined and sparked a continuing debate on military doctrine, organization, and operations, and inspired a so-called "Revolution in Military Affairs" (RMA). The scramble was now on within the military to define IS, IO, and IW; to determine who would be the leader; and how to realize the potential inherent in these advances due to Information Technology (IT). Initially, due to the strong influence of the intelligence community, the RMA was concerned with the restructuring and reorganization of the military to facilitate their control of the technology and its capabilities and to meet the increased requirements those capabilities would demand. There also was a scramble to capitalize

on the vast amounts of funding perceived to be available in this new arena. In the operational community the discussions generally focused on using IT to improve current operations processes such as Command and Control and targeting. Operationally, IT demonstrated great potential to affect the Observe, Orient, Decide, and Act decision cycle (the OODA Loop), decreasing friendly decision times while increasing those of our adversaries. Additionally, IT offered the possibility for new weapons and tools which could not only bring an adversary to its knees with drastically less resources on our part, but possibly the ability to stop a conflict even before it started. The resulting discussions, restructuring, reorganizations, maneuvering, and posturing continue today with only sporadic advances being made.

Whether you choose to accept the RMA or the potential deterrent capability of IO, Information Technologies is enhancing Operations, the OODA loop, and precision targeting on a daily basis. For example, more powerful, faster computer processors have been applied to decrease the processing time for signal analysis, to improve accuracy for geo-location, and to increase bandwidth for communications. We have seen numerous examples where the sensor to shooter network has been reduced from days to minutes and we have seen the production of the Air Tasking Order reduced from 72 to 12 hours. But the full potential of IO to dramatically improve US military operations, to decrease the number of personnel required, and to reduce the resources required is still in the future.

> "Information Operations [in Kosovo] was at once a great success…and perhaps the greatest failure of the war. Properly executed, IO could have halved the length of the campaign."
>
> (From "A view from the top," Admiral James O. Ellis, U.S. Navy, Commander-in-Chief, U.S. Naval Forces, Europe, Commander, Allied Forces Southern Europe, and Commander, Joint Task Force NOBIL ANVIL during Operation ALLIED FORCE.)

This paper will:

- Review current IO definitions and pertinent terminology.
- Describe the IO environment and offer some of the reasons why the potential of IO has not been achieved.
- Present an approach to achieve IO's potential for enhancing Information Superiority.

Perhaps, rather than being on the verge of a leap into the future or being embroiled in a Revolution in Military Affairs, we should consider that "Information Superiority is a journey, not a solution." as Mr. John Hamre stated in a recent speech.

INFORMATION SUPERIORITY AND INFORMATION OPERATIONS DEFINED:

The stated goal of the Department of Defense in all future military operations is "Full Spectrum Dominance." Joint Vision 2020 states that "the transformation of the joint force to reach full spectrum dominance rests upon Information Superiority." Joint Publication 1-02 defines Information Superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. As the enabler (focus) for the operational elements of Joint Vision 2020 (Full Dimension Protection, Precision Engagement, Focused Logistics, and Dominant Maneuver), Information Superiority's goal is to provide a competitive advantage by translating superior information into superior

knowledge and decisions to achieve decision superiority. As stated in JV 2020, "Information Superiority is created and sustained by the conduct of IO." JP 1-02 defines Information Operations as "actions taken to affect adversary information and information systems while defending ones own information and information systems." The USAF, in AFM 2-5, IO Doctrine, also defines Information Superiority as "the degree of dominance that allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition." This doctrine goes on to divide IS into Information Operations and its two major sub-elements: information-in-war and information warfare. The USAF stresses that "to achieve Information Superiority, our understanding of information operations must explicitly include two conceptually distinct but extremely interrelated pillars: information-in-war -- the "gain" and "exploit" aspects and information warfare -- the "attack" and "defend" aspects."

Unfortunately these definitions while clear, are very broad and can be interpreted to either cover very specific tasks or to encompass the entire scope of military operations depending on ones perspective and agenda. Further complicating the issue is the tendency during discussions for the participants to interpret the definitions depending on their perspectives and agenda or to focus on a specific type of capability rather than on the larger concept of Information Operations or Information Superiority. I.E. computer network attack, communications, Electronic Warfare, PSYOP, etc. -- rather than on the real objective of achieving Information Superiority. Also, the Joint Vision and the service documents don't explain how to achieve Information Superiority or how Information Operations fits into the operational picture.

The promise of information technology has been that we can bring all the assets and capabilities, regardless of definitions, together into an integrated, synergistic whole, an "Information Operations environment," that is much more capable, faster, and of lower cost than the individual pieces or capabilities. In practice, what this really means is that to achieve Information Superiority you must create that environment through actions (categorized as Information Operations) which integrate, manage, and affect information, information production, and information systems.

THE INFORMATION OPERATIONS ENVIRONMENT:

The multitude of existing definitions, joint, service, and those derived internally for business purposes obviously do not solve the basic question of determining how to achieve Information Superiority. As discussed above, to achieve IS an IO environment is required. To facilitate the discussion, a description of a fully realized information operations environment is provided.

In a perfect world, with Information Operations fully designed and integrated into the equipment, doctrine, concept of operations, etc., the commander, will fully understand the threat, the target set, and the political objectives. Using this total situational awareness and instant connectivity to his forces, he formulates his offensive operational objectives and gives instructions on what he wants to happen. Based on those orders, the machinery of command and operations takes over and it happens – the adversary is stopped, pushed back, destroyed, as appropriate. The collection plan, the maneuver plan, the airspace management plan, etc are formulated, the necessary data is collected and converted to knowledge, the correct targets are chosen, and the best possible means of affecting them (the most relevant to the objective) are applied. The successful execution of IO will provide Commanders at all levels with situational

awareness and a common relevant operating picture with additional information supplied on demand. This description carried out to any level of detail shows that the critical element in the IO environment is the information or knowledge derived from the raw data. The key to achieving the benefits of IO therefore starts with how that knowledge is developed.

Based on the potential afforded by the information revolution, the intent should therefore be to design, develop, and field a sufficient quantity of networked collection systems, that will provide an environment that brings all the varied pieces of technology into a cohesive whole with the capability to achieve Information Superiority. This integrated environment will host the service and agency operations and applications in a seamless manner. This environment will provide total awareness of all aspects of the operations, Command and Control, Intelligence, Logistics, Fire Support etc., supporting the JV 2020 operational concepts of Precision Engagement, Dominant Maneuver, Full Dimensional Protection and Focused Logistics. A fully integrated system of systems, built on the principles of IO will deliver timely, actionable knowledge to the commander not just data.

Whether creating knowledge about the adversary, our allies, or our own forces, the power of IO hinges on the efficient and timely collection, processing/analysis, storing, protection, and dissemination of data, information, and knowledge. The objective or goal of Information Superiority therefore is to obtain (collect) and apply (disseminate and use) valid (valid = true, useful) information faster and more efficiently, while reducing the adversary's ability to obtain and use valid information.

THE IMPEDIMENTS TO ACHIEVING THE POTENTIAL OF IO:

The first impediment to achieving the potential of IO concerns the budgeting and acquisition process. As stated above, Information Superiority requires the collection, processing/analysis, reporting, and dissemination of large volumes of accurate information or knowledge provided in a timely manner. The simplest way to produce this knowledge would be to field enough assets to provide the data and support necessary to complete the mission. Budget constraints and system development timelines have always severely restricted the number of sensors, weapons, supplies, and personnel available to a commander. This limitation has kept the C4ISR community from providing the necessary data to achieve Information Superiority in the past. However, the introduction of advanced Information Technology has offered the potential for a limited number of assets to perform the tasks of many. Automated decision aids and displays will allow one person to complete the tasks that currently are performed many. Improved sensors will gather more data, faster, with more accuracy. The services have made some progress toward IS by using more capable computers and processors within the structure of current systems, the equivalent of replacing a 386 processor with a Pentium III. But like putting a larger engine in a car with four flat tires, you can force it go faster, but it certainly won't be efficient and allow you to reduce the resources required. In fact it may require more. In other words, simply increasing power and speed will not achieve the full potential of IO.

Beyond the budgetary restraints, the second impediment to achieving the potential of IO is service organization structure combined with traditional system design. These impediments also limit advances in speed and efficiency. For example, in the ISR domain, the RF spectrum has been segregated by user, signal type, and use, hence the various "INTs" (SIGINT, MASINT etc.). This has resulted in both organizational and design impediments. Because the collection effort has been focused on specific segments of the spectrum, the components and systems have

generally been designed around custom hardware. Additionally, the US intelligence structures and reporting architectures, have evolved into "stovepipes," and become unresponsive or minimally responsive to the operational commanders. Information technology has afforded the opportunity for these systems to become more efficient by replacing processors and computers with more capable, faster chips. But because of the current organizational stovepipes, the internal command structures, the internally derived database structures, the security rules, etc., these systems and structures are greatly limited in their ability to achieve Information Superiority in the near future.

The sensor to shooter chain is an excellent example of this problem and a major focus area regarding improvements using advanced IT. In the sensor to shooter chain, the desire is for the sensor to respond directly to the shooter – the person who will employ a weapon, providing the necessary information, as it is required, in a useable format. However, unacceptable time delays have resulted due to the command structures, the reporting structures and formats, and system designs. Past and current sensors generally were designed to either collect all available data (target and non-target alike) on their respective section of the spectrum (ELINT, COMINT, IMINT, HSINT, etc.) or are designed to collect data about a single specific target. These sensors nominally have their own command and control, tasking, processing, and analysis chain, and the data collected by the individual sensors is in form and formats determined by the initial user/requestor, the intelligence organization. The collected data had to be processed through the intelligence structure, analyzed and reformatted before it could be delivered to the ultimate user. During recent demonstrations and Advanced Concept Technical Demonstrations (ACTD), improved sensors have been used to reduce the internal timelines and to increase system accuracy. During the ACTD, the organizational structures are broken down and the formatting and analysis impediments are overcome by force of command (when specific command attention is applied the normal restrictions disappear) and the use of custom designed interfaces. But outside of the ACTD, Information Superiority is still yet to be achieved due to the underlying organizational structure and the institutional nature of the military. In other words, to this stage of implementing Information Superiority, the focus has been on improving the process through emphasis on interoperability versus designing for mission flexibility or to accomplish the broader mission capabilities promised by IT.

ACHIEVING THE POTENTIAL OF INFORMATION OPERATION:

Ultimately, the real significance and value of Information Technology is to enhance the capabilities of military systems by eliminating time delays and information flow restrictions. As discussed, current budget constraints, system designs and organizational structures limit the possible improvements. Further improvements could be achieved by the introduction of an overarching IO concept, consistent guidelines, architectural standards, etc.

But since it is impractical to design and develop a single, overarching system due to the institutionalized nature of the current stovepipes, the forces of the future should be equipped with a fully integrated system of systems. This system of systems can not cobble a variety of systems together as current efforts do. The pieces of the system must be designed as part of an integrated whole from the start – e.g. ISR doesn't exist for itself, it provides Indications and Warning or targeting data, and therefore must be designed with the other parts (specifically the operations requirements) in mind. Designing for an integrated whole is not just designing the hardware systems, but integrating Information Operations concepts into how the force operates and is

supported. This includes the doctrine, C2, operations, intelligence, the airspace management system, logistics systems (supply), medical support system, etc.

An Integrated Design Approach:

Information Operations is the integration of all the components and systems within a single architecture and framework, the management of those components/systems, and management of the information they use or produce. An integrated IO force will produce a seamless system of systems, responsive and flexible to consistently meet the commanders changing information requirements. Any effort that improves the integration or information management processes and thereby makes the required information available more efficiently, rapidly, and/or accurately is an integral part in achieving the potential of IO. The integration of IO into future military operations will require a central acquisition authority with a broad vision of IO and authority over funding, personnel, acquisition, etc. Additionally, a designated component responsible for all managing all facets of military (and in some cases civilian) IO operations may be required. The likelihood of this occurring in this decade is very small. Since the current organizational and institutional structures which resist an overarching IO concept and architectural standards are so difficult to change, the design of hardware is the next logical area to pursue. The following describes an approach to designing ISR systems using common modules that are software re-programmable and reconfigurable, scaleable, and multi-functional.

Common Modules:

In today's modern environment of reduced budgets the trend is to use Commercial Off The Shelf (COTS) products whenever possible. This trend should reduce costs, increase reliability, and increase commonality. In the IO environment, specifically the ISR domain, COTS products have not yet achieved the computing capabilities required to process all the varied signal and data types. Custom hardware and software is still necessary to process the data. This has produced systems, such as the COMINT system depicted in Figure 1, which consist of multiple internal stovepiped sub-systems. These sub-systems often have similar processing cards and components performing the same functions within the separate stovepipes. But because the design did not plan for common modules there is no interaction between the stovepipes and the system pays a high cost in Size, Weight, and Power.

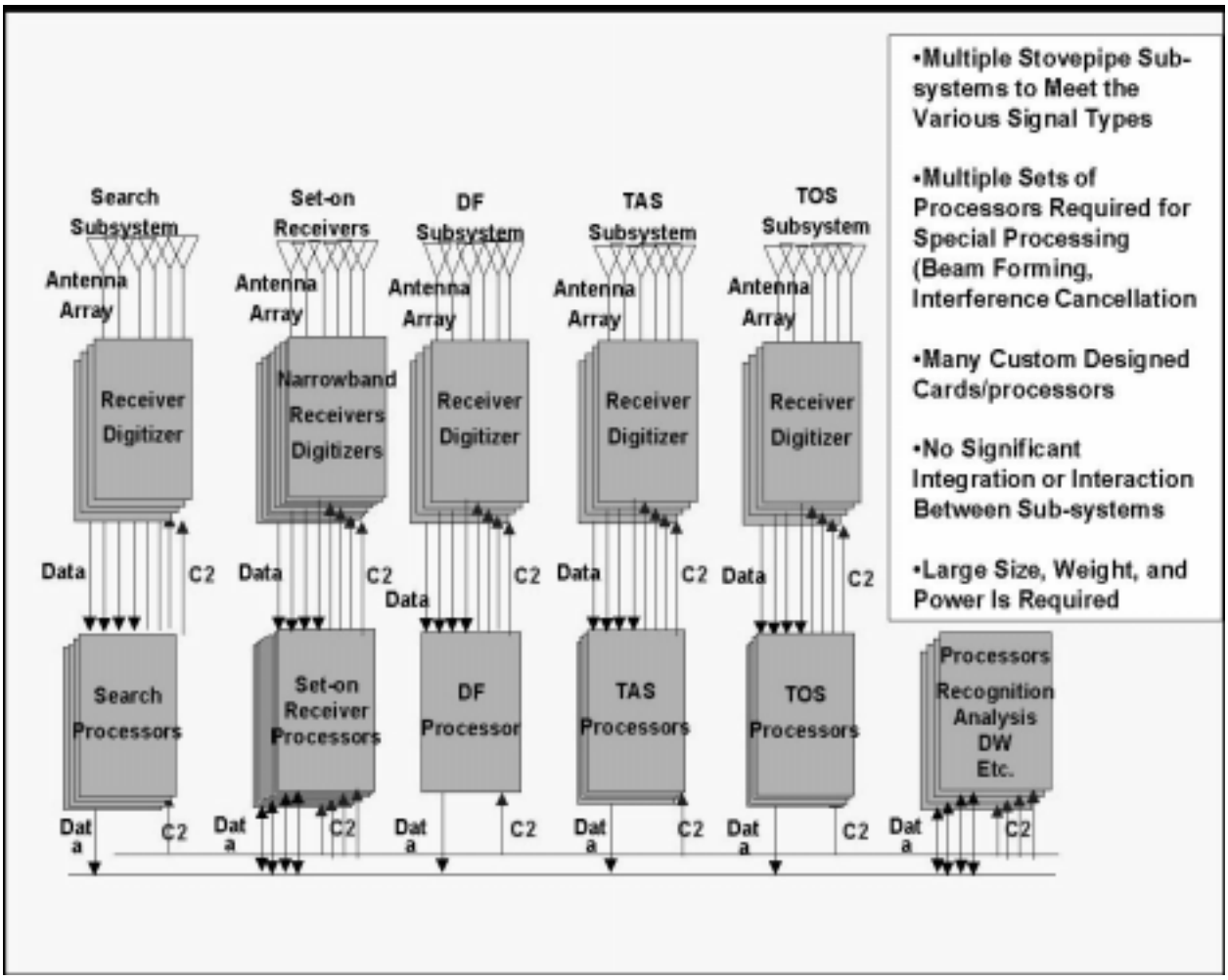

Figure 1. Current COMINT System.

However, the increasing power of COTS components and the further development of COTS products will facilitate the use of common modules, such as digital receivers, analog to digital converters, signal processors, etc., within the sub-system stovepipe and between stovepipes. By careful design attention (designing with the larger goal of non-specific function in mind), and the use of common modules throughout a design, a system can be designed so that the modules can be pooled, regrouped, or reassigned to perform more than one specific function. Using common modules a sub-system could perform as DF processing, signal recognition and analysis, or general-purpose tasks such as display and system management through software reprogramming as shown in figure 2.

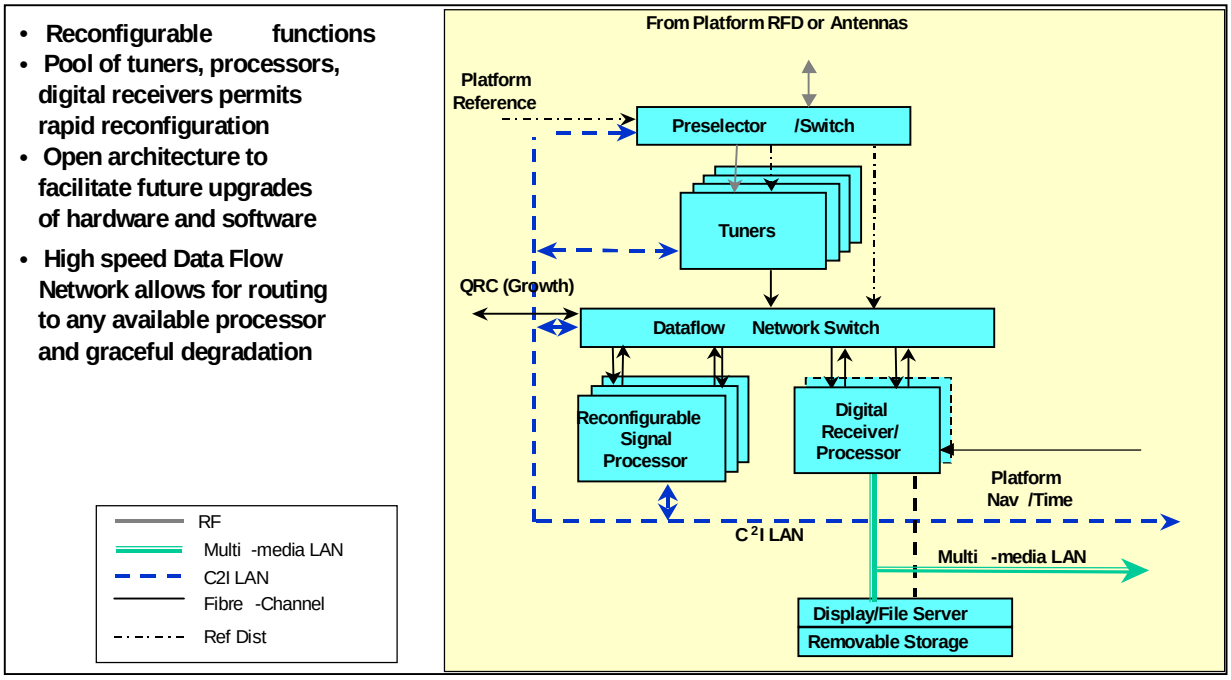

Figure 2. COMINT System using Common Modules

Multi-Function Payloads:

Multi-function payload designs take common modules and integrated design one step farther. Rather than just including several different systems within a payload package, multi-function ISR payloads build on common modules, standardized interfaces and architectures to integrate several of the "INT" sensor capabilities (COMINT, ELINT, SAR/MTI, EO/IR, Laser, HSI, MASINT, etc.) within a single payload. By using common modules, sensor sub-systems (such as the COMINT system described above) can be made more efficient, smaller, and lighter. The use of common modules, standard interfaces, and architecture standards also allows resources to be grouped (either by software or hardware) in a common pool, which can be used by any of the systems that need that same capability or use the same processes. For example, a COMINT system using digital signal processors and digital receiver/tuners and an ELINT system using digital signal processors and digital receiver/tuners could pool those resources as long as common modules and standard interfaces are used. These design efforts will require the adherence to use of Object Oriented methods and open architectures as found in the Joint Airborne SIGINT Architecture (JASA) found in the JASA Standards Handbook and the Joint Technical Architecture Handbook. Use of commonality and standards, can also allow designers to integrate between previously separate sensor platforms, and perhaps more importantly, integrate sensor functions and non-sensor functions within a platform.

Integration between the sensor functions and between sensors and non-sensor functions provide the benefit of deconfliction and facilitates interoperability, electro-magnetic interference reduction and automatic cross cueing between platforms. An integrated payload design will also take into account the fact that some functions may have to transmit in the same frequency band as it is sensing. This approach can be applied to many combinations of sensors (ELINT and SAR/MTI, COMINT and SAR/MTI, etc.) or combinations of sensors and non-sensors

(SIGINT/communications and/or SIGINT/jamming). For example, rather than building a COMINT system with its own antennas, RF distribution network, receivers, processors, and data network, and a separate ELINT system with many like elements, an integrated SIGINT payload system can be designed with many shared elements (as shown in figure 2). The transmission components can be integrated into the payload without conflicting with the SIGINT capability. By using an integrated design approach, the transmission functions can be interleaved in time, frequency, and space with the sensing functions so that the platforms own transmissions will not overwhelm its collection mission. This will mitigate or eliminate interference. Figure 3 is an example of combined SIGINT and transmission systems, which are closely coupled in time and frequency, and spatially compatible. In this case the transmission system could be used for

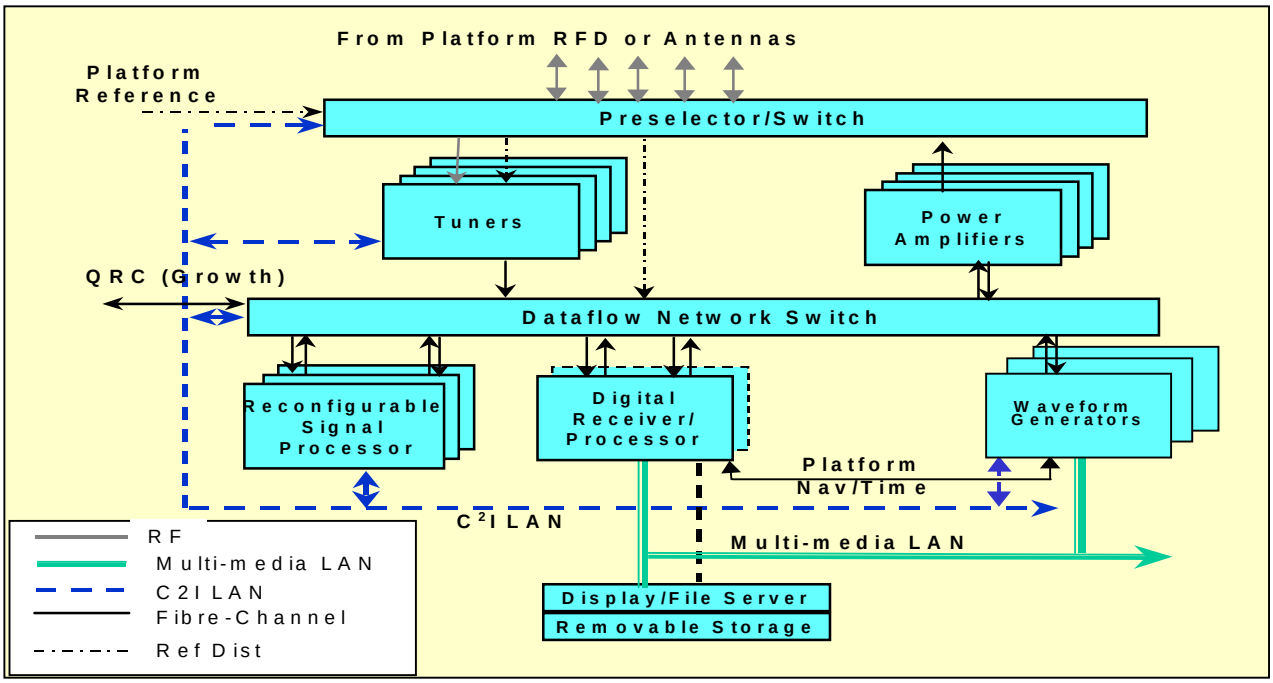

Figure 3. Integrated Combined Payload

communications, SAR/MTI, or jamming at different times during the mission. The waveform generator would be software programmable for the various waveforms. The power amplifiers and antennas may be different, but the other hardware elements could be the same. Depending on mission loading (tasks), large SWAP reductions can be achieved and mission tasks can be managed more efficiently using shared, reconfigurable assets such as pooled receivers, processors, antennas, etc. This could also be applied to the design of an integrated COMINT and Foliage Penetrating Radar payload. By designing for commonality, the number of processors, tuners, and even apertures may be reduced. These designs must take advantage of open industry standards to facilitate integration of multiple functions into common hardware elements. This, in turn, allows for the payload to be scaled to many different platforms as well as to be modularized with many different functions- a multi-function payload.

Anticipated Benefits:

The integrated design approach has multiple benefits. Systems designed for integrated Information Operations will reap substantial benefit in logistics efficiencies. This approach can also easily be seen to have benefits across the functional areas of IO and will move the military much closer to achieving Information Superiority.

Logistically, the integrated design and common hardware will allow modularity and scalability, will lower life cycle costs, and will reduce the Size Weight and Power (SWaP) of each payload. Additionally, multi-function payloads will reduce the total number of payload/platforms necessary to meet the commander's requirement for information. This can be achieved due to their ability to be software reprogrammed or reconfigured to perform multiple functions with limited hardware changes (antennas and apertures) and their ability to process and cross cue (using one sensor to cue another for additional information or more detailed information) within a payload. This will also have the effect of reducing the communications bandwidth requirements and equipment necessary to support the ISR operation. These more effective payloads/platforms should greatly reduce the logistics tail of a force designed for integrated IO.

Information Superiority will be easier to achieve by using multi-function payloads due to this type of system's greater flexibility in adjusting to rapidly changing IO requirements, the increased effectiveness of the individual payload, and the reduction in collection, processing and dissemination timelines. Platforms equipped with multifunction payloads, while on-station collecting data, will be able to reconfigure in seconds through software, rather than having to return to a central control point or base and swap out sensors. Additionally, a multi-function payload could be launched with less known intelligence (detailed intelligence is often required prior to launch so that the proper configuration can be selected and loaded) and be reconfigured once on-station based on the data received using a baseline configuration (a wide area/signal type). The payload could then be tailored using on board software tools to meet the environment, matching capabilities to priorities.

The effectiveness and efficiency of individual sensors would also be improved using this design approach. Improved resource management using pooled, common modules within a sensor, can increase computing power, processing speed, and processing capability available to accomplish signal tracking, beam forming, interference cancellation, and the other techniques necessary for signal interception and identification in the modern complex signal environment. Also, by using pooled resources to enable more thorough and complete processing at the reception point, the raw data from a single sensor type can be converted to information closer to the point of interception and less data has to be transmitted back to an analysis point. Only that data necessary to reduce ambiguities or necessary for the commander to make his decision would have to be passed, greatly reducing the bandwidth requirements and increasing responsiveness, accuracy, and timeliness.

Multi-function sensor payloads, programmed to intercept distinctive signatures in the communications environment, could immediately cross cue and reconfigure to intercept radar signals, confirming the target identity without having to use additional resources. For instance, by integrating wide area sensors or broad band sensors with narrow field of view or specialized frequency sensors, automatic cueing would reduce the need for huge amounts of reconnaissance data or imagery down to simple text based reconnaissance reports combined with a small image of the detected target and facilitate rapid location and identification of targets. By integrating a

high resolution Mid Wave IR imager and a Long Wave IR hyperspectral cuer into a "Dual Mode Sensor" one can share an aperture and simultaneously collect data from a wide area in parallel. The cuer operates at relatively low resolution. As a cuer, the hyperspectral sensor attacks the data problem from two approaches. First, it's ability to find targets based on their spectral signature triggers the extraction of "chips" of MWIR imagery from the high-resolution sensor which are centered on the detected target and its immediate surrounds. Second, the hyperspectral sensor identifies the background type (e.g., grass, oak tree, pine tree, roads) and these features are added to the image chip as text files providing context for the target. Additional annotation of the image chip includes Time, Date, Latitude, Longitude, the hyperspectral target ID etc. This annotated image can be transmitted at low rates over secure, Omni directional UHF links in NITFS-2.X format. The product, when fused with other data becomes part of a map of the battlefield with high-resolution cut-ins for targets and supporting annotation in standard IPIR formats.

This cross cueing within the same platform, between similar and dissimilar sensors, can generate even more synergy when integrated multi-function sensor payloads (in the above case, a Dual Mode Hyperspectral imager) are integrated with other collection suites or a network of sensors that includes other intelligence areas, such as even wider area SIGINT (COMINT and/or ELINT) disciplines. These sensors will have the broadest coverage and would cue a multi-function payload to scan suspect areas that need additional collection. The annotation of the resultant images can now include the additional ID symbols from the relevant INTs. Use of information derived from past looks at the AOR via All Source can be used to identify enemy intent and high value targets found in the battlespace. Cross- cueing and integration of this nature will greatly reduce the time and resources necessary for correlation/fusion and will improve situational awareness. The end result of this process would potentially be finalized knowledge – the identity and location of the high payoff targets.

CONCLUSION:

Information Superiority, achieved through Information Operation, can be a valuable combat multiplier. The integrated multi-function payload design approach, using common modules, will greatly increase the US military's capability to successfully execute Information Operations. By using standard architectures and interfaces, common modules can be pooled to increase computing power, processing power and speed, and to allow reconfiguration and cross cueing to reduce timelines and assets required, while still increasing responsiveness and flexibility. The use of an integrated multi-function payload design approach will greatly enhance commander's ability to make the right decision at the right time in any environment across the full spectrum of combat.