REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-05-2012	FINAL	

Non-Traditional Intelligence, Reconnaissance, and Surveillance Electronic Intelligence for the Operational Electronic Warfare Officer

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Vande Griend, Nicholas A.

Paper Advisor (if Any): **N/A**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The military's decreasing budget and continued requirement to simultaneously wage war with two nation states, and maintain Defense Support to Civil Authorities in the homeland, necessitate a need to think creatively on how to provide a robust intelligence collection effort in a financially constrained era. The over tasking of ISR assets and the limited support they can provide in a contested environment make use of Non-Traditional Intelligence, Surveillance, and Reconnaissance (NTISR) capable platforms an attractive and affordable option to fill ISR gaps. To that end, the United States military must develop a means of tasking NTISR assets in the collection of theater electronic intelligence (ELINT) to provide Operational Commanders with a layered method to acquire actionable information to prepare, plan, and execute campaigns and major operations. ELINT providers in the NTISR community need to produce doctrine and a tasking concept to produce a viable method of getting ELINT to an Operational staff.

15. SUBJECT TERMS
Non-Traditional Intelligence, Reconnaissance, and Surveillance, NTISR, ELINT, operational, tasking

16. SECURITY CLASSIFICATION OF: Unclassified			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		27	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Non-Traditional Intelligence, Reconnaissance, and Surveillance Electronic Intelligence for the Operational Electronic Warfare Officer

by

Nicholas A. Vande Griend

LCDR/USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

04 May 2012

Contents Page

Paper Abstract

The military's decreasing budget, the continued requirement to simultaneously wage war with two nation states, and maintain Defense Support to Civil Authorities in the homeland, necessitate a need to think creatively on how to provide a robust intelligence collection effort in a financially constrained era. The over tasking of ISR assets and the limited support they can provide in a contested environment make use of Non-Traditional Intelligence, Surveillance, and Reconnaissance (NTISR) capable platforms an attractive and affordable option to fill ISR gaps. To that end, the United States military must develop a means of tasking NTISR assets in the collection of theater electronic intelligence (ELINT) to provide Operational Commanders with a layered method to acquire actionable information to prepare, plan, and execute campaigns and major operations. ELINT providers in the NTISR community need to produce doctrine and a tasking concept to produce a viable method of getting ELINT to an Operational staff.

Introduction

In Vietnam, the United States lost over 3,000 aircraft due largely to a robust North Vietnam air defense.[1] The United States struggled to deal with the multitude of SA-2 and SA-3 surface-to-air missile (SAM) systems that were able to move between numerous prepared sites and also by a contested air-air environment in which North Vietnamese Mig-21 fighters were used for air interdiction.[2] A massive number of anti-aircraft artillery (AAA) pieces, which accompanied the SAM's and the fighters, inflicted the majority of the casualties.[3] The common thread between all these systems was the use of the electromagnetic environment to detect, track, and fire on American aircraft. The United States adapted to North Vietnamese tactics with the introduction of jamming pods (mounted on F-105 aircraft), chaff clouds, and the Shrike anti-radiation missile.[4] The tactics and development of new technology would not have been achievable without the Electronic Intelligence (ELINT) provided by Intelligence, Surveillance, and Reconnaissance (ISR) assets which started collecting data on North Vietnamese systems before the conflict ever began.[5]

The United States has made many advances since Vietnam and continues to work to remove gaps in ISR coverage and achieve a persistent collection effort to support the needs of Combatant Commanders (CCDR).[6] To better meet the CCDR's needs, the United States military must develop a means of tasking Non-Traditional Intelligence, Surveillance, and Reconnaissance (NTISR) assets in the collection of theater ELINT to provide Operational Commanders with a layered method to acquire intelligence information. A collection effort that capitalizes on available resources will maximize the information available for the preparation, planning, and execution of campaigns and major operations. The military's

decreasing budget and continuing requirement to simultaneously wage war with two nation states, and maintain Defense Support to Civil Authorities in the homeland, necessitate a need to think creatively on how to provide robust intelligence collection in a financially constrained era.[7] Some innovative thinking that considers the need for intelligence planners to use all available means of collection to produce an intelligence picture, makes the use of NTISR capable aircraft and surface units an attractive and affordable option to fill ISR gaps.

Electronic Intelligence Definitions

A synopsis of the meaning of Electronic Intelligence (ELINT) should take place before continuing. ELINT is a subcomponent of Signals Intelligence (SIGINT), and defined as:

> *Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.*[8]

More simply put, ELINT consists of the signals that come from foreign equipment and are not associated with communications. ELINT is further subdivided into two categories, Operational ELINT (OpELINT) and Technical ELINT (TechELINT). TechELINT is electronic intelligence that provides fine granularity on a signal for analysis. This type of intelligence is primarily useful in determining an emitter's electronic characteristics and use for a weapon system, and in turn, to technological advances to counter the threat. TechELINT contains parametric data, which consists of the emitter's frequency, pulse width, scan type, pulse repetition frequency, and a host of other metrics. TechELINT also contains an emitter's location and other data used to identify systems and their potential manner of use and is useful in analyzing a potential adversary's capabilities.[9]

OpELINT provides specific emitters for incorporation into an Electronic Order of Battle (EOB) which provides a picture of how a potential adversary has integrated

information and weapon systems in the operational environment.[10] The EOB provides friendly forces information on the type of equipment present on the battlefield, which includes items such as Surface-to-Air Missile (SAM) and coastal surveillance RADARS, data links, Ground Controlled Intercept RADARS and other equipment. Operational Level Commanders use the EOB in conjunction with other intelligence sources to plan and prepare against tactics, techniques and procedures expected from a potential foe during hostilities.[11] NTISR systems are programmed to search for items contained in the EOB and require reprogramming when new information becomes available.

ISR & NTISR Sources

ISR platforms are national assets coordinated through the Defense Intelligence Agency (DIA) and controlled by the National Reconnaissance Office and USSTRATCOM. ISR assets come in a variety of forms and include a network of space based, Unmanned Aerial Systems (UAS), and manned platforms that work together to provide the detailed data required to produce an intelligence product. One challenge faced by the ISR community occurs when operating in an opposed environment where potential adversaries have developed long range weapons, jamming technology, and cybernetic warfare capability that inhibits their ability to collect.[12] Coverage gaps and the challenge of an opposed environment can be alleviated, to some extent, with NTISR platforms.

NTISR platforms are tactical in nature and include fighters, helicopters, surface ships, and ground based units. A universally accepted definition of NTISR remains to be seen, but the United States Air Force defines it as:

The concept of employing a sensor not usually used for ISR as part of an integrated collection plan developed at the operational level for pre-planned, on-call, ad hoc, and/or opportune collection.[13]

NTISR use in collection is limited, in part, due to the lack of a tasking construct that allows operational level staffs the ability to task and communicate with units that possess NTISR platforms. A combination of ISR and NTISR assets is essential to providing a layered collection effort needed by a CCDR or Joint Force Commander (JFC) to plan and execute operations.

Why do Operational Commanders need ELINT?

ELINT gathered supports the operational design of operational plans (OPLAN) by providing information for the employment of kinetic and non-kinetic means to support command and control warfare, fires, and protection. Operational Fires prepare the battle space for future operations and are accomplished in advance of the achievement of operational objectives.[14] ELINT provides information used in operational fires such as the Suppression of Enemy Air Defenses (SEAD) that reduce or eliminate the surface to air threat prior to follow-on strike operations.

In Operation Desert Storm, planners used ELINT to produce effects that had elements of both Command and Control Warfare (C2W) and Fires to significantly reduce the capability of the Iraqi IADS, called KARI (KARI is not an acronym but simply the word "Iraq" spelled backwards in French). In a multi-phased attack, coalition forces severely degraded KARI by first conducting strikes to eliminate the Command and Control aspects of the KARI system; and second by the employment of over 500 High Speed Anti-Radiation (HARM) missiles to reduce the SAM threat to follow-on strikes on key Iraqi military targets.[15] C2W and Operational Protection differ from Operational Fires in that they occur prior to hostilities and continue throughout a campaign.

Command and Control Warfare (C2W) involves the use of kinetic and non-kinetic fires to degrade or deny an enemy's ability to control the actions of his forces on the battlefield.[16] C2W is not limited to attacks on an adversary commanders ability to communicate, but is also used to interfere with information that could inform the decision making process. C2W, with respect to ELINT, includes attacks on systems that incorporate RADARS and data links used to provide information on the position and intent of friendly forces. C2W has a second order effect of offering a level of protection to friendly forces similar to Operational Protection.

Operational Protection refers to actions taken to "preserve the effectiveness and survivability" of friendly forces.[17] In Kosovo, ELINT was pivotal to operational protection for coalition aircraft. The Kosovo military learned lessons from the destruction of KARI during Operation Dessert Storm and protected SAM sites through routine movement and concealment. The Kosovo tactics prevented the destruction of their air defenses. The continued presence of the SAM threat, along with airspace restrictions, denied access to the area by ISR assets. In the absence of a robust ISR capability, F-16CJ aircraft protected coalition strike assets through SEAD and by rerouting strike assets around pop up SAM threats.[18]

The operational functions described rely heavily on good intelligence before hostilities begin and with real time information during hostilities. Today, however, intelligence requirements necessitate the continued deployment of ISR assets throughout the globe, significantly reducing their availability. In 2010 ADM Robert Willard, commander of United States Pacific Command (USPACOM), addressed the challenges by stating, "Effective ISR is essential to obtaining critical insights into the plans, capabilities, and intent

of our current and potential adversaries".[19] Additionally, he commented on the need to address "capability gaps, deployment of assets, and processing, exploitation, and dissemination of information to maximize situational awareness and warning".[20] NTISR adds an additional layer of support for obtaining intelligence and reducing the information gaps of which the Admiral spoke of, but only if we address the challenges that inhibit NTISR collection ability.

Operational Level ELINT Collection

Combatant Commanders also require intelligence products to develop OPLANs for use against a potential adversary at the outbreak of hostilities. OPLAN development begins with the Intelligence Division (J2) of the CCDR staff which uses intelligence information for the Joint Intelligence Preparation of the Operational Environment (JIPOE). The JIPOE process provides CCDR's with situational awareness on every aspect of an adversary's capability, to include use of the electromagnetic spectrum, in order to develop a Course of Action (COA) to counter the threat.

During this process, the CCDR determines additional information needs regarding the operational environment called the Commander's Critical Intelligence Requirements (CCIRs). CCIRs are broken into more specific information requirements known as Priority Intelligence Requirements (PIR) and Requests for Information (RFI). With respect to ELINT, the J2 Electronic Warfare Officer (EWO) has the responsibility to address the CCDR concerns.[21] Once the EWO identifies ELINT collection requirements required to fulfill the CCIR's, PIR's and RFI's the EWO will work with the J2 Collection Manager to develop a collection strategy and "optimize use of all available, capable, and suitable assets and resources."[22]

The collection manager pulls information by following four basic principles:

1. Identifying collection requirements to support CCRI, PIR, and RFI needs.

2. Prioritize the collection requirements.

3. Decide on applicable intelligence disciplines (some targets, such as a SAM site, may require combinations of intelligence like ELINT and IMINT).

4. Task assets that are immediately available to conduct priority tasking.[23]

The EWO and collection manager do not currently include NTISR assets when developing a collection strategy for ELINT. The absence of NTISR in this process is due to the lack of a tasking construct to request information and also to a lack of knowledge of what products NTISR assets are capable of providing.[24] A tasking construct is not the beginning of the process; however, a coherent doctrine must first support the construct. A lack of doctrine precludes operational staff from developing baseline knowledge of NTISR platforms and NTISR integration into the collection strategy. EWO's need a point of reference from which they can deviate in identifying collection assets and how to task them; doctrine will provide this baseline. Additionally, a lack of information on platform capability and availability make tasking NTISR assets nearly impossible. These challenges must be addressed so operational staff have a means to utilize the opportunities that present themselves when NTISR capable units enter their AOR.

The Path Ahead

Pressure on multi-sensor ISR platforms to perform IMINT roles limit their ability to participate in the SIGINT arena. In addition, foreign nations continue to study United States collection efforts and are working to deny that capability. Potential adversary advancements in electronic attack, space interdiction weapons, and cyber attack have produced an opposed

environment for space-based assets.[25] Adversary's development of electronic attack technology may inhibit the use of data links between ISR assets and a Distributed Common Ground System (DCGS). Additionally, their cybernetic warfare capability may prevent the use of ground processing stations or on collection assets.[26]

NTISR assets have the capability to EWO's meet intelligence collection needs to by filling the gaps caused by ISR overtasking and in opposed environments that deny safe passage to ISR assets. Increased integration and collaborating between the ISR and NTISR ELINT communities to produce a collection product need to address doctrine, a tasking concept, staffing, and training and education.

Doctrine

Doctrine is a critical start to the incorporation of NTISR assets into the collection process. Doctrine for NTISR operations currently does not exist in Joint or Service specific publications. The only doctrinal information available is in Air Force ISR doctrine which discusses the need for continued development of NTISR platforms and asserts that NTISR is an evolving activity that will become more valuable as a tasking construct becomes available.[27] Service specific doctrine needs to be written that represents the unique capabilities, limitations, and processes that a service intends to use for NTISR tasking. Service doctrines should parallel each other in terms of processes and planning and in turn feed Joint plan development.[28] Service specific doctrine that is aligned with joint doctrine will eliminate multiple, and differing, constructs that will confuse the intelligence community. Doctrine written by a joint forum with tactical, operational, and interagency representation will ensure all assets in the joint environment are working from a common

operating concept and will enhance a joint war fighting mindset. Doctrine should not be ELINT specific but contain information on all intelligence domains.

The principles of doctrine should define the nature of the NTISR mission and method of integration for the collected data at the operational and tactical levels. It should also address the need for coordination with the ISR community to produce a persistent collection effort and address lessons learned in Operation Iraqi Freedom and Enduring Freedom over the last decade. Furthermore, doctrine should provide a thorough explanation a Standard Operating Procedure (SOP) to task NTISR assets. ISR doctrine written by the United States Air Force provides a good template from which to begin. Detailed discussion of the full extent of what should be included in doctrine is the subject for another paper but at a minimum should include elements of ISR doctrine such as the principles, process, support, resources, benefits, and command relationships that represent the NTISR effort.[29]

Development of a Tasking Concept

A tasking construct is needed to provide operational level EWO's an avenue to obtain information from NTISR assets. Currently, theater EWO's do not task NTISR assets with collection responsibilities, and information on the electronic environment is reported based on what the tactical soldier/aviator/sailor deems relevant. For example, several hundred intercepts may occur during a mission in an EA-6B but only several will be reported based on what the aircrew deems relevant, which may not coincide with what an EWO desires to know. A tasking construct will allow EWO's to bridge that gap and have a vote in what emitters tactical assets search for and report. The two methods of tasking discussed are Direct Tasking and Indirect Tasking. Direct tasking infers direct control of a tactical asset while Indirect Tasking reflects an ad hoc method of obtaining intelligence information.

Direct Tasking via Component Commander – The direct tasking method introduced by Major David Gordon, in his research paper for the Air War College in 2009, involves the development of an NTISR tasking construct specific to the aviation environment.[30] Major Gordon's research in how NTISR aviation assets could be tasked in a joint theater led to his production of a tasking construct under the purview of the Joint Force Air Component Commander's (JFACC) Air and Space Operations Center (AOC). The overall theme was in the production of Imagery Intelligence (IMINT) but also has applicability in the ELINT arena.

Under the direct tasking construct, the AOC provides dedicated Air Tasking Order (ATO) assigned missions to NTISR aircraft with the assistance of NTISR LNO's. The ATO assigned tasking originates in the form of a Joint Tasking Air Strike Request (JTAR) from a unit requesting support for a particular mission. The JTAR provides details on the "who, what, when, where, and why" of the mission. Currently, Electronic Warfare (EW) aircraft also receive tasking through a JTAR, accompanied by an Electronic Attack request Form (EARF), from the Electronic Warfare Coordination Cell (EWCC) at the AOC. The EWCC prioritizes tasking and provides aviation EW units the EARF; which explains the portions of the electromagnetic spectrum targeted for exploitation and may provide an additional layer of jamming command and control.

The JTAR/EARF construct used for EW tasking at the AOC could also be used for NTISR ELINT collection. For the collection effort, however, the creation of an Electronic Surveillance Request Form (ESRF) that mimics information in an EARF needs to occur with the addition of the location and parametric specifics of the targeted emitters. EWCC personnel would coordinate with ISR planners to minimize duplication of effort and

maximize synchronicity. EWCC would then relay the assigned tasking via JTAR/ESRF to the supporting unit. Figure 1 provides a snapshot of information flow.

While this method is useful, it has several drawbacks to naval units due to its inability to take full advantage of the secondary nature of the NTISR role. Also, it involves direct tasking from a Component Commander which would be difficult during transit phases of a deployment and would also require similar constructs be developed by the Joint Force Maritime/Land Component Commanders (JFMCC/JFLCC). Lastly, it may require the movement of assets which may not be achievable for surface ships or land based units. An advantage of this method is that it can synchronize with ISR assets to some degree but synchronization becomes complex when one considers the coordination required between multiple Component Commanders and ISR planners.

In his article, Major Gordon asserts that Tactical Commanders may be resistant to "yielding control of their capabilities and resources" to other entities.[31] Resistance from tactical units might be overcome with a less intrusive tasking method which is well suited to ELINT collectors, who are only required to be within reception of a collection target. An indirect tasking method would allow for coordination with Operational level staff without the need for direct orders from a Component Commander.

Indirect Tasking via CCDR or JFC Staff – Indirect Tasking is a viable alternative to the Direct Tasking construct. Indirect tasking provides an ad hoc method of collection utilizing NTISR assets in a role that is less intrusive on a unit's primary mission and would cover collection from land, sea, and the air without the need for additional coordination through a JFACC, JFMCC, or JFLCC. The goal of this tasking construct is to provide theater EWO's an avenue to provide tactical aircraft, ships, and land based units a means to participate in the

collection effort without relocating assets or reassigning missions. To be more specific, it provides a means to perform a primary mission while onboard sensors perform the secondary mission of collecting information for the theater EWO.

An effective means to provide a conduit for the exchange of information between units providing input from throughout the globe is through the use of a SECRET Internet Protocol Router Network (SIPRNET) website. The SIPRNET is the preferred source for tactical users as information with a higher classification may be difficult to obtain since not all units have immediate access to computer terminals at the TOP SECRET level. Also, many tactical platforms do not have approval for the introduction of classifications higher than SECRET since it would require redefining hardware security classifications. A supplemental listing may be required on the Joint Worldwide Intelligence Communications System (JWICS) for units that possess a capability above the SECRET classification level.

The website should provide a one-stop-shop for access to operational level collection needs represented by an emitter listing broken down by regions within a CCDR's AOR. For example, USPACOM covers a massive area and includes several countries of interest to the United States. USPACOM's AOR would need to be broken down into separate regions that would each its own listing (regions such as US FORCES KOREA in PACOM's AOR are already well defined). The National Security Agency (NSA) has the lead for SIGINT information analysis, which makes it an ideal candidate to host a website that contains global links to CCDR/JFC emitter listings. NSA's National Security Operations Center (NSOC) Expeditionary Support Team (EST) has the responsibility to provide support to CCDRs, and as such, would have purview over the website.[32]

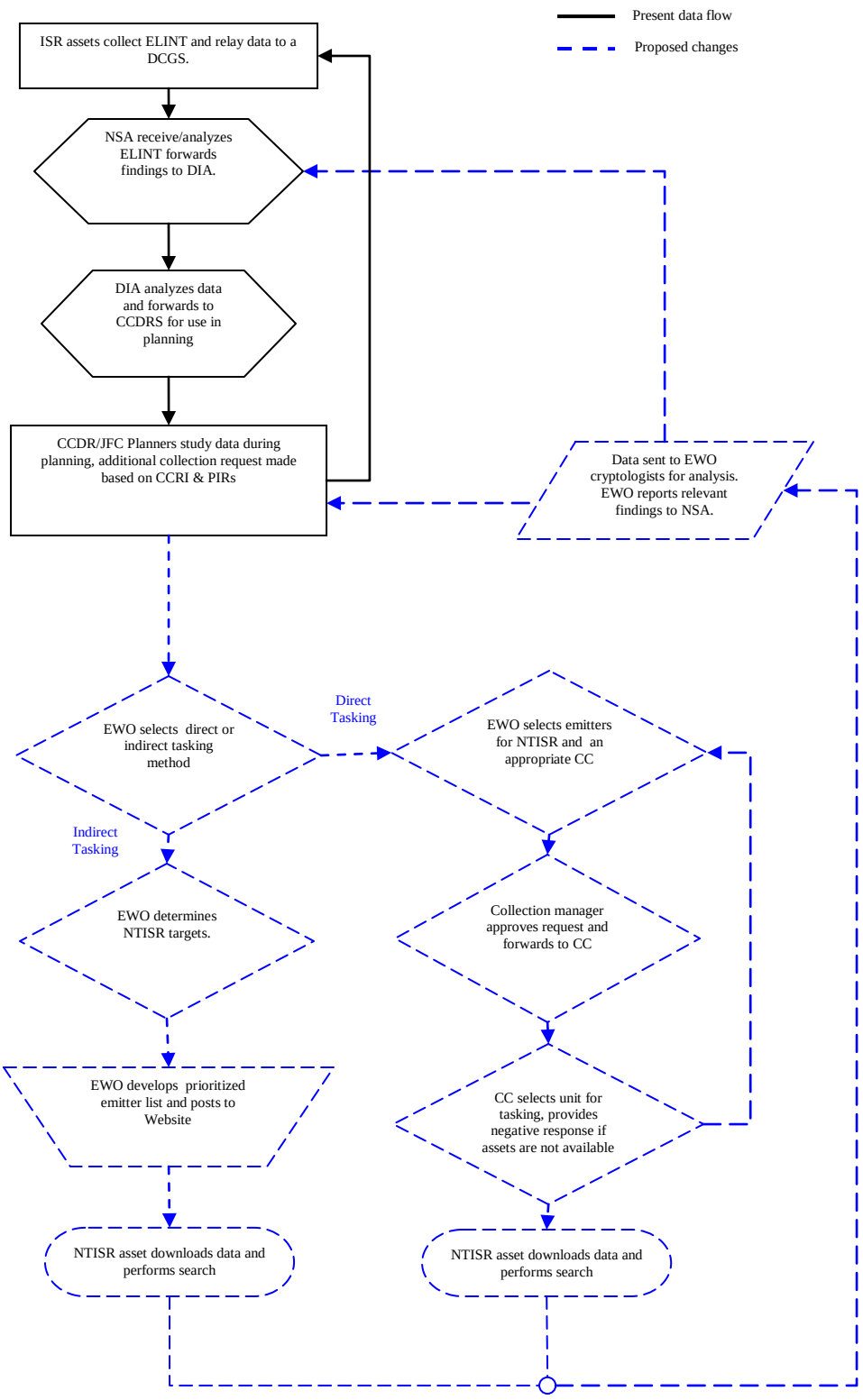

Figure 1: Tasking Construct Information Flow (created by the Author)

The data uploaded to website would be locally prepared by a JTF or CCDR EWO and provide a detailed listing of emitters that are of interest to the JTF. Tactical units then download the listing and prepare a mission load that supports the collection request. The listing provided would need to be tailored to NTISR collection abilities. EWO's cannot commit the characteristics of all NTISR platforms to memory and need a matrix of individual platform capabilities such as that depicted in Figure 2. The matrix provided in Figure 2 provides conveys a basic construct derived from the JFIRES spreadsheet provided to Joint Terminal Attack Controllers (JTAC), a more comprehensive set of metrics would need to be incorporated to provide greater fidelity on asset limitations. The capabilities matrix will aid EWO's in the matching the characteristics of a targeted emitter to a platform capable of meeting the collection requirement. The website would also have to contain point of contact information to allow NTISR capable units the means to communicate with the EWO. Figure 1 provides a quick look at the flow of information.

Capability and Communication Equipment								
Platform	**RCVR Type**	**Search Freq Rng**	**GEOLOC Capable**	**Manual Mod**	**Data Links**	**Comms**	**Freq Hopping**	**Secure Capable**
FFG	**SLQ-32**			**Y**	**4/11/16**	**UHF/VHF SATCOM**	**HQ II**	**KY-58**
CG	**SLQ-32**			**Y**	**4/11/16**	**UHF/VHF SATCOM**	**HQ II**	**KY-58**
E-2D	**ALQ-217**			**Y**	**4/11/16**	**UHF/VHF SATCOM**	**HQ II SINCGARS**	**KY-58**
EA-6B	**ALQ-218**			**Y**	**16**	**UHF/VHF**	**HQ II SINCGARS**	**KY-58**
F-16CJ	**HTS**			**N**	**16**	**UHF/VHF**	**HQ II SINCGARS**	**KY-58**
F-18E/F	**AN/ALR-67(V)3**			**N**	**16**	**UHF/VHF**	**HQ II SINCGARS**	**KY-58**

Figure 2: NTISR ELINT Capability Matrix[33]

Communication is essential; the EWO must know when assets are entering the theater and what capabilities they possess. Communication with the EWO should be provided to a

limited number of personnel to prevent a flood of communication that may overwhelm an EWO. For example, a Carrier Strike Group (CSG), with a mix of aircraft and surface ships, has many NTISR capable commands attached. Once the CSG enters the theater, only the CSG EWO embarked on the carrier would contact the Operational EWO and provide a listing of platforms, operating areas, and time on station in the AOR.

The Processing, Exploitation, and Dissemination (PED) process also requires a means to send collected data back to the EWO in a manner discernible to cryptologic technicians. NTISR assets possess a variety of post mission products but they might not support the EWO needs. To ensure information is relevant and accurate, the NTISR community needs to agree upon a commonly accepted method to provide feedback. Feedback would most likely be provided via Excel spreadsheet that contains operator narrative on the mission along with relevant parametric information tailored to the needs of cryptologists. The feedback should provide sufficient detail for analysis technicians at the staff headquarters and NSA. Feedback issues are also germane to the direct tasking method and need to be addressed in a similar fashion, the same feedback construct would most likely work for either method.

The benefits of this method is that it reduces staff workload to produce written orders to subordinate units and also eliminates the need for an LNO augmentation on a Component Commanders Staff, which in turn, reduces the burden on tactical units to provide personnel needed to accomplish the mission. This construct has the added advantage of using existing EW staff members and does not require the establishment of an Electronic Warfare Coordination Cell, which typically only exists during large scale conflicts and crisis situations. Additionally, it provides unexploited data to operational commanders from units transiting the area or participating in regional exercises. A major drawback to this method,

however, is that it does not help in producing a persistent ISR presence desired by theater commanders to eliminate gaps in coverage. The lack of synchronicity in terms of time and space are inherent in an ad hoc construct. This problem can be mitigated to some extent by including vulnerability windows where NTISR assets could provide gap coverage.

Education, Training, and Manning

To achieve effective program, proper training and education of Operational and Tactical level participants is vital to provide knowledge of the process and the limitations of NTISR units. EWO's will require detailed knowledge on how the process works and general knowledge of the hardware available in tactical NTISR assets. NTISR platform knowledge for the EWO is critical to manage expectations on the quantity and quality of information they will receive since not all collectors are created equal.

Tactical units also require training. Tactical operators do not share a consistent level of Electronic Intelligence knowledge needed to participate in the collection effort. For example, fighter assets have the collection capability but do not have knowledge on how they would fit in with a collection effort. Fighter units would need to designate a subject matter expert to conduct periodic unit level training and as a liaison to EWO's. Training would also include cryptologic technicians at both the Operational and Tactical levels, manning levels for technicians will also need to be addressed.

Manning is also an issue since many commands do not have the needed number of cryptologists to analyze data. Not all CCDR staffs are alike, for example, U.S. Africa Command (AFRICOM) does not have the personnel to facilitate a tasking construct for their AOR and would need increased cryptologists staffing. AFRICOM could also elect to rely on the staffs of other commands such as U.S. Sixth Fleet. Tactical units also need additional

staffing to facilitate the process. For example, Carrier Strike groups do not possess cryptologists staffing sufficient to provide support needed for ships in company and assigned squadrons. In email exchange LCDR Chris Bahner, EA-6B Naval Flight Officer, commented that "With today's systems it is quite possible that if the system was not set to alert the aircrew of a specific emitter, that it would be missed in flight. However the system will record and report the detections, classification and identification in the post [flight] processing. If you have a qualified ELINT processor (who is trained) look at all of the data, they can typically see everything they need to report."[34] LCDR Bahner's comments reflect the need to trained cryptologic technicians are available to analyze NTISR collected material.

Counter Argument

A tasking construct for NTISR assets is a cumbersome process that increases workloads at the Operational and Tactical levels with minimal benefits. ELINT gathered from NTISR assets is only desirable at the tactical level since it is time sensitive, already providing ELINT to the Operational level and limited in scope in terms of time and space.

ELINT from tactical assets has real time value; however, systems are becoming more mobile, making real-time information irrelevant at the operational level for long term planning. In addition, due to their tactical nature, NTISR assets are limited in terms of time and space. Tactical aircraft are severely limited in time on station due to fuel constraints, crew rest and maintenance requirements. Surface ships and land based units are limited in terms of space due to a limited line of site, which significantly reduces the probability of intercept.

Finally, the development of a tasking construct is not required since NTISR assets are already providing a service without the need of an additional layer of control. A feedback

mechanism is also not required since real time data can be transmitted via data link or UHF/VHF radios. In the Kosovo example presented earlier, the F-16CJ participated by providing Operational Protection by rerouting strike traffic based on ELINT intercepts. This is a textbook example of the use of NTISR aircraft that does not necessitate an additional tasking concept through an ATO.

Rebuttal

NTISR assets are tactical in nature and, therefore, collect tactical information. Over time, however, the information collected provides long term insights in how a potential adversary operates. NTISR products have long term value on mobile systems because they often return to prepared sites to operate. Placing an Operational level EWO in the tasking loop will ensure that units are searching for emitters that have operational value. Additionally, the presence of NTISR assets in the AOR will stimulate a potential adversary to turn systems on to gain situational awareness, which increases the probability of intercept of operationally significant information.[35] The NTISR collection is also valuable in detecting new or proliferated weapon systems and provide insight on how those systems will be used.

Aircraft do have a limited on station time compared to ISR assets but is offset to some extent by the multiple sorties tactical aircraft fly throughout the day. It is also true that surface ships and land-based units have a limited line of site horizon but collectively can supply valuable information over a wide space. For example, a Carrier Strike Group has multiple ships that can participate. Singularly, these ships may have a limited view of the battle space but collectively they can acquire information from a large area when dispersed throughout an area of interest.

Finally, NTISR assets are already providing information that is operationally significant. The goal of a tasking construct, however, is to provide a more robust collection effort by providing EWO's an avenue to actively task a unit with a requirement that fits the Operational Commanders needs. The examples provided reflect participation during hostilities; a tasking construct will enable participation during peace. The feedback portion of the construct can be partially supported by the use of data links or voice communications. However, this significantly increases operator workload which would require the collection effort to be a primary role. Additionally, data links lack parametric detail required for cryptologic analysis and link communication is often inhibited by line-of-site limitations imposed by topography or distance.

Conclusion

Tactical resources of Electronic Intelligence deploy throughout the globe and possess a capability to collect intelligence relevant to the Operational Commander. A construct, supported by doctrine, needs to be implemented to take full advantage of NTISR ELINT recourses in times of hostility, and during peace. Doctrine will provide EWO's a reference point to identify collection assets and how to task them; and a simple tasking construct will allow a virtually untapped NTISR resource to produce information that meets CCDR needs.

ISR assets continue to be task saturated and suffer from anti-access weapon systems evolving in potentially adversarial nation states. The need for a persistent presence will continue even after the Long War draws to a close in view of the fact that an over watch for weapons proliferations, terrorist activity, and rogue nation behavior will continue to be an issue. The utilization of NTISR assets can alleviate gaps in ISR coverage. Developing a

construct now will alleviate the time needed to train and educate the NTISR intelligence collection team before the outbreak of hostilities.

End Notes:

[1] John Andreas Olsen, *A History of Air Warfare* (Washington D.C.: Potomac Books Inc., 2010), 112.

[2] Ibid, 113.

[3] Ibid, 113.

[4] Ibid, 113.

[5] Richard L. Bernard, *The History of Electronic Intelligence* (Fort George G. Mead: Center for Cryptologic History, National Security Agency, 2009), 6.

[6] Admiral Robert F. Willard, *Statement before the Senate Armed Forces Committee*, March 24, 2010, 35

[7] Department of Defense (DOD), *Quadrennial Defense Review*, (Washington D.C.: Government Printing Office, 2010), 65.

[8] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, (Washington D.C.: Government Printing Office, 2010), 107.

[9] Bernard, *The History of Electronic Intelligence*, 1.

[10] National Security Agency, *Cryptologic Almanac 50th Anniversary series*, (http://www.nsa.gov/public_info/_files/crypto_almanac_50th/A_Brief_Look_at_ELINT_at_NSA.pdf), 16 December 2003, 1.

[11] Bernard, *The History of Electronic Intelligence*, 1.

[12] DOD, *Quadrennial Defense Review*, 34.

[13] United States Air Force, *NTISR Functional Concept*, January 2012 (www.intelink.sgov.gov/inteldocs/action.php?kt_path_info=ktcare.actions.document.view&fDocumentID=412103).

[14] Milan N. Vego, *Joint Operational Warfare Theory and Practice* (Newport, RI: U.S. Naval War College, 2009), VIII-59.

[15] Olsen, *A History of Air Warfare*, 183.

[16] Vego, *Joint Operational Warfare Theory and Practice*, VIII-45.

[17] Vego, *Joint Operational Warfare Theory and Practice*, VIII-95.

[18] Benjamin S. Lambeth, *NATO's Air War for Kosovo*, (Santa Monica, CA: RAND, 2001), 104.

[19] Admiral Willard, *Statement before the Senate Armed Forces Committee*, 35.

[20] Ibid, 35.

[21] Joint Publication (JP) 3-13.1, *Electronic Warfare*, (Washington D.C.: Government Printing Office, 2007), II-2.

[22] Ibid, III-9.

[23] Joint Publication (JP) 2-01. *Joint National Intelligence Support to Military Operations*, (Washington D.C.: Government Printing Office, 2012), III-15.

[24] LCDR Chris M. Bahner, email message to author, May 4, 2012.

[25] Department of Defense (DOD), *Quadrennial Defense Review*, 34.

[26] Ibid, 34.

[27] Air Force Doctrine Document (AFDD) 2-9, *Intelligence, Surveillance, and Reconnaissance Operations*, (Washington D.C.: Government Printing Office, 2007), 32.

[28] LCDR Chris M. Bahner, email message to author, May 4, 2012.

[29] AFDD 2-9, *Intelligence, Surveillance, and Reconnaissance Operations*, iii.

[30] Major David J. Gordon, *A Tasking Construct for Non-Traditional Intelligence, Surveillance, and Reconnaissance*, (Masters research report, Air Command and Staff College, Air University), www.dtic.mil/dtic/tr/fulltext/u2/a540123.pdf, April 2009, 9.

[31] Ibid, 21

[32] JP 2-01. *Joint National Intelligence Support to Military Operations*, A-22.

[33] Air, Land, Sea Application Center, *Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower https://ndls.nwdc.navy.mil/pdf_id/133026/3-09-2_(20_Dec_2007)_(NTTP).pdf#search="j fires"*, 2007, 69.

[34] LCDR Chris M. Bahner, email message to author, May 4, 2012.

[35] United States Air Force, *NTISR Functional Concept*, January 2012 (www.intelink.sgov.gov/inteldocs/action.php?kt_path_info=ktcare.actions.document.view&fDocumentID=412103, last modified January 2012.

Bibliography

Air Force Doctrine Document (AFDD) 2-9. *Intelligence, Surveillance, and Reconnaissance, Operations*, Washington D.C.: GPO, 2007.

Air Force Doctrine Document (AFDD) 2-5.1 *Electronic Warfare*, Washington D.C.: GPO, 2002.

Air Force Instruction 10-706, *Electronic Warfare (EW) Operations*, Washington D.C.: GPO 03 November 2010

Air Force brief, unclassified continent: *NTISR Functional Concept*, www.intelink.sgov.gov/inteldocs/action.php?kt_path_info=ktcare.actions.document.view&fDocumentID=412103, January 2012.

Richard L. Bernard, *The History of Electronic Intelligence*, Fort George G. Mead: Center for Cryptologic History, NSA, 2009.

Department of Defense (DoD). *Quadrennial Defense Review Report*, Washington D.C.: GPO, 2010.

Department of Defense (DoD). *Statement of Admiral Robert F. Willard, U.S. Navy, Commander U.S. Pacific Command, before the Senate Armed Services Committee on U.S. Pacific Command Posture*, Washington D.C.: GPO, 24 March 2010.

H. Streetly, Martin, "EW 101", The Journal of Electronic Defense", Gainesville FL:Naylor

LLC, February 2012.

Goodman, G. "Getting the Most from ISR Data." *The Journal of Electronic Defense* 30, no. 7, Gainesville FL:Naylor LLC, July 2007.

Gordon, David J. Major, *A Tasking Construct for Non-Traditional Intelligence, Surveillance, and Reconnaissance*, (Masters research report, Air Command and Staff College, Air University), www.dtic.mil/dtic/tr/fulltext/u2/a540123.pdf, April 2009.

Joint Publication (JP) 1-02, *Dictionary of Military and Associated Terms*, Washington D.C.: GPO, 2012.

Joint Publication (JP) 2-01. *Joint National Intelligence Support to Military Operations*, Washington D.C.: GPO, 2012.

Joint Publication (JP) 3-13.1. *Electronic Warfare*, Washington D.C.: GPO, 2007.

Joint Publication (JP) 3-51. *Joint Electronic Warfare Doctrine*, Washington D.C.: GPO, 2000.

Lambeth, Benjamin S., *NATO's Air War for Kosovo*, Santa Monica, CA: RAND, 2001.

National Security Agency, *Cryptologic Almanac 50th Anniversary series*, (http://www.nsa.gov/public_info/_files/crypto_almanac_50th/A_Brief_Look_at_ELINT_at_NSA.pdf), 16 December 2003.

Olsen, John Andreas, *A History of Air Warfare*, Washington D.C.: Potomac Books Inc., 2010.

Vego, Milan N., *Joint Operational Warfare Theory and Practice*, Newport, RI: U.S. Naval War College, 2009.