Asymmetric Advantage via *Intelligent* Intelligence Information Technology (I3T)

Phillip Chudoba, J. Terry Simpson, and Christopher R. Gunderson

Abstract—**Traditionally, the US Navy/Marine Corps team has employed Sea Power to achieve asymmetric military advantage, i.e. deliver powerful, tactical blows, quickly, and in just the right places. Arguably, in terms of the current fight against non-state terrorists, the USN and USMC have lost that unique relevance. At the same time, adversaries have found an asymmetric advantage of their own. Namely, they use cutting edge Commercial-Off-the-Shelf Information Technology (COTS IT) for agile Command, Control, Communication, Computer and Intelligence (C4I) to outmaneuver Blue Force. Blue Force, by contrast, is hamstrung by brittle, archaic MILSPEC C3I kit, and by a crushing bureaucracy that resists refreshing the technology at anything approaching Internet speeds. Members of the US Marine Corps Intelligence Community, and US Navy C4I systems Acquisition Community, are fighting back. They have voluntarily reached across their stovepipe boundaries to join forces. Together, they are determined to re-establish USN/USMC tactical asymmetric advantage, in this case "Maritime Information Dominance", through mutually supportive Rapid Evolutionary Acquisition (REA) of game-changing IT capabilities. It's not about the technology per se; it's about using IT to give our warfighters the "information high ground." Accordingly, the REA approach is to adapt best practices demonstrated in observed success cases wherever those may occur in government or industry. Meanwhile, Congress has demanded that the Department of Defense, as an enterprise, fix its clearly broken IT acquisition processes. This paper concludes that the DoD can use this Naval Intelligence Capability Evolution (N-ICE) REA initiative as an exemplar for its broader IT acquisition transformation.**

***Index Terms*—2010 NDAA Section 804, IT Acquisition Reform, MIEA, N-ICE, MCISR-E, Intelligence, Surveillance, and Reconnaissance, ISR.**

Manuscript received January 31, 2011. This work was supported in part by the Joint Interoperability Test Command as part of the Naval Postgraduate School Netcentirc Certification Office Research Initiative.

Phillip Chudoba is the Assistant Director of Intelligence for the US Marine Corps. (e-mail: Phillip.Chudoba@usmc.mil).

J. Terry Simpson is the Principal Deputy for Intelligence at the Navy Program Executive Office for Command, Control, Communication, Computers and Intelligence (PEO C4I). (e-mail: terry.simpson@navy.mil)terry.simpson@navy.mil)

Christopher R. Gunderson is an Associate Professor of Information Science with the Naval Postgraduate School in Monterey CA (831 224 5182; email: cgunders@nps.edu)

I. Introduction

"**ASYMETRICAL** advantage" is the Holy Grail of warfare. Any military's combat objective is to exploit any and all tools and tactics – including dirty tricks -- to win the "high ground." That objective is exactly why the United States of America, from its very inception, established the Navy/Marine Corps team. From the beginning, a key US Military goal has been to take advantage of the inherent mobility of Sea Power to project a potent tactical punch right where it will hurt the enemy the most. That potent maritime punch has played a vital role in every major conflict between the United States and its adversaries from 1776 through the end of the Twentieth Century. Unfortunately, in the twenty-first century post-industrial "cyber" world, the Navy/Marine Corps team has not found the traction to apply its traditional formula for success.

Meanwhile, and even more unfortunately, the enemy has evolved and found a potent asymmetric advantage of its own. Adversaries ranging from low-budget, non-state terrorists to state-sponsored actors routinely apply COTS IT technology as a C4I force multiplier [1]. They use 3G or 4G as their version of the Global Information Grid. They use COTS software-defined radios, i.e. smart phones, as their version of the Joint Tactical Radio. Google Earth provides their Common Operating Picture (COP). These clever adversaries immediately harvest the benefits of upgrades to these various web-enabled/web-enabling capabilities. Strict radio discipline, and Operational Security (OPSEC) procedures, effectively cloaks their activity.

By contrast, the Blue Force coalition operates within brittle stovepipe communications networks wherein so-called "security" considerations prevent allies from sharing critical, perishable, information. Information collection and processing systems are typically either archaic legacy dinosaurs, or high tech, expensive, one-of-a-kind, stand-alone, stopgaps.

To be sure, Blue Force warriors use their equipment effectively. Further, some of the specialized military gear provides capability un-matched by COTS. We do not suggest that the enemy is winning. We do, however, suggest that Blue Force is unnecessarily fighting with one hand tied behind its back!

Two independently derived, but mutually supportive, plans within the DoN are aggressively addressing this issue: The Marine Corps Intelligence Surveillance, and Reconnaissance (ISR) Enterprise (MCISR-E) Roadmap [2], and the Maritime

ISR Enterprise ISR Acquisition (MIEA) implementation plan [3]. Both plans aim to implement a mandate for profound transformation in doctrine, organization, and equipment in response to a profoundly changing military threat, fiscal reality, and technological landscape. The mandate calls for increased operational agility with respect to cross-organizational information processing. Likewise, it calls for increased agility with respect to cross-organizational acquisition of Information Technology (IT.) That is, it calls for "Rapid Evolutionary Acquisition" (REA).

II. Business Case Analysis

A. Background

Success in any enterprise follows clear understanding of what industry calls a "value proposition" (VP), and implementation of an appropriate "business model" optimized accordingly. This truth holds for commercial for-profit enterprises, non-government not-for-profit enterprises, and government enterprises, including military enterprises. Indeed this simply is another way to say that a good leader understands what she or he is trying to accomplish, and will use available resources to best effect.

A Business Case Analysis (BCA) aims to objectively define the appropriate VP and suggest the associated business model. The BCA [4] for the Naval (i.e. USN + USMC) ISR Capability Evolution (N-ICE) REA process seeks to identify a cost-effective approach for establishing and governing an acquisition process that will address the objectives of MCISR-E.

Myriad Defense watchdog reports document general failure by the Defense Enterprise to implement IT acquisition transformations. (e.g. [5] [6]) The findings in all these reports are consistent regarding both issues with the "as is" legacy, and the desirable "to be" targeted end state. Namely, they agree that the "as is" legacy includes overly bureaucratic overly long serial processes, proprietary solutions, and budgets and requirements that are too big and continually expanding. Likewise, watchdog reports consistently agree that the "to be" target end state should include parallel "spiral" process, open modular design, and iterative customer-in-the-loop requirements development.

The issue has gotten so urgent that in Section 804 of the 2010 National Defense Authorization Act Congress has required the Department of Defense (DoD) to report its specific plan to fix its failed IT acquisition process.

Most of these reports, including DoD's response to Congress [7], lack specific guidance about how to bridge the "as-is"/"to-be" gap. That these successive reports have consistently reached the same conclusions over the past decade validates Einstein's observation: "The same thinking and processes that created the problem won't solve it."

Two recent reports that do provide some specific REA implementation guidance serve as key references for this BCA. One is the Maritime ISR Enterprise Acquisition Study (MIEA) Review) [3]. The other is the Association for Enterprise Information (AFEI) Industry Task Force Report on 2010 National Defense Appropriations Act (NDAA) Section 804 Industry Perspective on the Future of DoD IT Acquisition (TF 804 Report) [9].

The approach to the N-ICE BCA was to build on top of the body of watchdog reports in general, and the MIEA study and TF 804 report in particular. The BCA authors studied documentation of the exemplar REA processes enumerated above, and interviewed expert participants in those processes. They also interviewed Marine Corps Subject Matter Experts (SME) in Intelligence operations and supporting acquisition activities. The BCA socialized objectives and initial findings with senior leaders within the USMC and USN C4ISR community. Feedback from leadership contributed to the analysis of alternatives.

B. Measures of Success

Per well-established tenets of leadership and management, the BCA applies the following universal success factors as basis for its findings and recommendations.

1. ***You get what you measure; measure what matters.***
2. ***You get what you pay for; buy what matters.***
3. ***Empower good, well-trained, people to apply all your resources against your customers' most critical needs per #1 and #2 above***.

In keeping with those universal tenets, metrics for N-ICE will be based on "Value-of-Acquisition" (VoA) as a function of cost, performance, and schedule according to the following model.

> VoA = (normalized value-per-capability) X (#-of-capabilities-acquired) ÷ (discounted time-to-deliver-capability) ÷ (cost)

Note that in this model, the critical factor is "value." Given that the application domain is intelligence, value is most likely to be associated with the quality of collection, processing, and delivery of information. "Time" and "cost" either enhance or detract from basic value. If either "time" or "cost" grows to the point where VoA drops below some threshold value, it is time to walk away from sunk costs, and/or de-scope the effort, in order to get something useful in the warfighters hands in time to make a difference.

In order to most credibly define "value-per-capability" the BCA concludes that the N-ICE pilot project should immediately tackle the most critical tactical edge issues, e.g. countering IED emplacement; interdicting high value individuals; countering ambushes; etc. Definition of "information value" flows from analysis of the associated critical information transactions validated by operational SMEs. ***The key is to objectively link desired outcomes, such as "fewer casualties due to IED," to the specific classes of information transactions that enable them.***

C. Build on top of observed success

" 'Best practice', useful standards, and good architecture all follow repeated success on the ground. So, therefore, does good policy" [9]. Accordingly, the N-ICE BCA proposes

adapting non-theoretical processes that have demonstrably, successfully, and repeatedly executed aspects of REA. For example, the USAF Tactical Exploitation of National

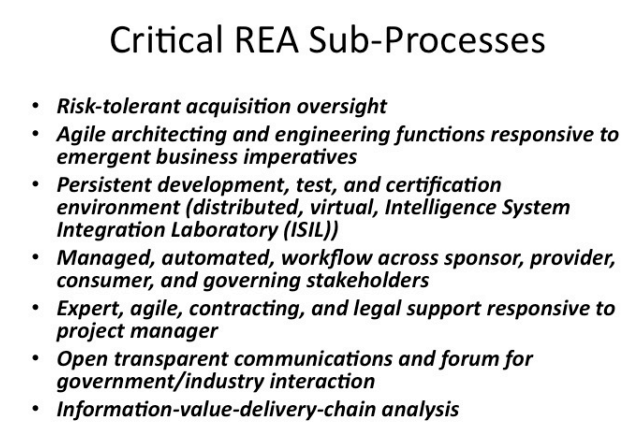

Figure 1: Study of successful exemplars of REA reveals this list of effective practices common among them

Capabilities (TENCAP) has an efficient, rigorous, collaborative process for rapidly developing and delivering small increments of new technology. The Special Operations Command is well known for its ability to find militarily useful COTS capability and rapidly insert it into operations. The Navy Acoustic Rapid COTS Insertion (ARCI) program is often cited for its continuous tech refresh across program lifecycle. In addition to studying those three exemplars, the BCA consulted a panel of industry experts to capture commercial best practice for REA.

The BCA distilled multiple critical success factors with respect to governance, management, engineering, acquisition, and operations that are common across all or most of the REA exemplars. Those success factors point to a number of sub-processes that are critical to success of REA. See figure 1.

D. Analysis of Alternatives

In order to properly frame the best management and governance structure for the N-ICE pilot initiative, the BCA considered the critical success factors distilled from exemplars, the associated necessary sub-processes, and the fiscal and political "facts of life" in the current Naval Intelligence acquisition landscape. That analysis delivered the boundary conditions for analysis of alternatives (AoA) listed in figure 2.

The AoA assumes that there are essentially three ways to manage a new activity: (1) assign it as additional duty to an existing organization; (2) create a "matrix organization" composed of part time resources from multiple disparate organizations: (3) create a "tiger team," i.e. a dedicated task force composed of individuals temporarily assigned full time to the new project.

Given that this N-ICE piloting activities will address USMC tactical ISR requirements supported by USN ISR infrastructure, the BCA identified two likely governance models:

1) **Standard acquisition governance model**: HQMC (I) as Naval Tactical ISR requirement sponsor; MCSC as acquisition authority and capability developer.

2) **TENCAP acquisition governance model**: HQMC (I) as Naval Tactical ISR requirements Executive Agent (EA); ASN RDA provides acquisition authority to a Naval ISR Portfolio manager, various capability providers are chosen for projects, competitively, per their particular skills.

Option 1) above represents status quo for developing and deploying USMC Intelligence Systems. Option 2) is the governance model commonly employed by various TENCAP offices and other special project offices designed to support rapid technology insertion.

The BCA AoA matrix matches each of the two potential governance models with each of the three staffing models to identify 6 alternative CoAs for managing the N-ICE pilot portfolio. The AoA then evaluated each potential CoA with respect to each of the five boundary conditions and assigned green, yellow, or red score.

Note that identifying dedicated staff for any project, especially a new start, inherently reduces risk. The TENCAP governance model is specifically designed to flatten bureaucracy associated with traditional governance inside large Systems Commands. Unlike traditional Systems Commands, the TENCAP process has an excellent track record for cross service/agency collaboration since its inception in the 1970s.

Significantly, neither the TENCAP nor traditional governance model has a history of success with respect to the "Partner with COTS industry" boundary condition. Hence the COTS industry outreach element of the project is high risk in any case.

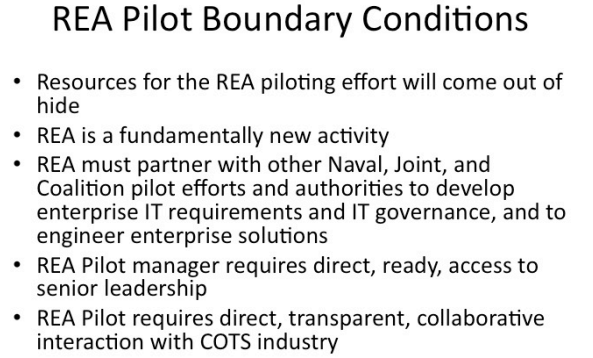

Fig. 2: N-ICE objectives and fiscal realities drive this list of pilot series boundary condition

Per figure 3, the AoA concluded that **the best CoA is to govern the N-ICE pilot portfolio with the TENCAP model.** Specifically, the HQMC Director of Intelligence should serve as the Executive Agent for Naval Tactical ISR N-ICE requirements. The PEO C4I Principal Deputy for Intelligence (PDI) should serve as N-ICE Portfolio Manager on behalf of ASN-RDA, reporting through DASN C4I&Space.

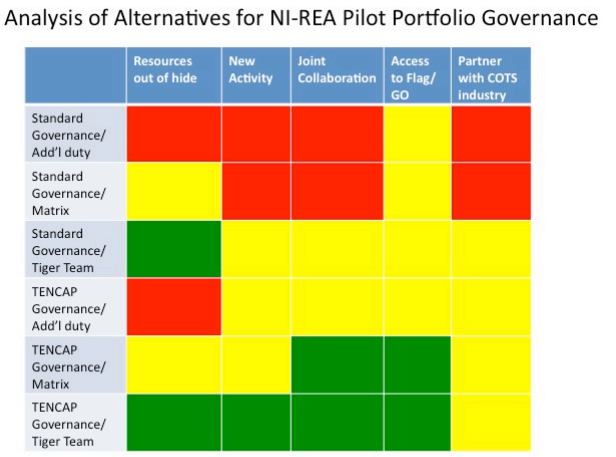

Fig. 3. Each governance model + staffing model was evaluated against each of the boundary conditions. Dedicated resources reduce risk. TENCAP model has track record of collaboration and agility. Interaction with COTS industry is new territory.

III. Critical Path and Plan of Action

A. Create an Enterprise Value-delivery Chain – Develop Value-Based Metrics and Automate the Acquisition Process

Today's acquisition process measures and incentivizes "compliance" and "size of program". Programs pass through each gate in the long serial process by delivering expensive, thick, static, paper artifacts that document compliance with hundreds of disparate and occasionally conflicting policies and standards. These compliance artifacts are largely redundant across multiple programs with similar parameters.

So called Earned Value Management (EVM) tracks costs and schedule but assumes the "value" is contractually well defined. However IT evolves so quickly, and IT-enabled capability is so inherently abstract, that it is impossible to define "stable requirements" in the traditional sense.

Applying waterfall development processes that are designed to deliver stable, well-defined "systems" to develop abstract rapidly evolving "capability" inevitably causes schedules to slip to the right and costs to go up. Meanwhile the value of the contractually specified deliverable decreases because it becomes archaic before it is deployed.

Recent policy changes recognize this issue and mandate that programs focus on "speed-to-capability." However, the industrial best practice is to focus on "time-to-value." "Capability" is not the same thing, necessarily, as "value." Industrial practice tends to discount value by a factor of 2 to 4 [per interviews with various industrial experts] in favor of delivering *something* the customer would value this year over delivering everything he wants next year. In any case, success requires understanding what the customer truly values. Achieving and maintaining that understanding in the rapidly evolving IT landscape demands that customers participate as literal partners with developers throughout capability lifecycles.

To address these issues in context with MCISR-E objectives, N-ICE team members have developed prototypes for a "Value-based Acquisition Framework" (VAF) [10] and Semantically Informed Dynamic Engineering of Capabilities and Requirements (SIDECAR) [11]

VAF is a series of parameterizations based on the traditional concept of "availability," e.g. system up time divided by total time, mission-ready aircraft divided by total aircraft, fully trained units divided by total units, etc. If you think about it, "availability" is really a simple ratio of value returned over total cost. Generally the Availability of Value in an Acquisition Portfolio = (normalized value-per-capability) x (# of capabilities delivered) ÷ (time-to-deliver discounted in favor of sooner) ÷ (cost).

VAF includes process-level efficiency metrics. Accelerating time to value depends on effective use of modularity, i.e. build-time interoperability of components. Build time interoperability is not about how many components you reuse; it is about effectively and efficiently composing *Informationally Interoperable* capability by re-combining "Value-off-the-Shelf." (VOTS).

SIDECAR is an automated, parallel, approach to eliminate the current serial paper-intensive engineering and documentation process. The idea is to link multiple complex databases that address policy, requirements, architecture, technology, and resources via cutting edge artificial intelligence. That complexity "under the hood" is hidden from the user but made useful through an intuitive GUI. Picture something like TurboTax for IT system engineers and acquisition professionals.

B. Define and Implement a Viable Business Model for Modular Open Systems Approach (MOSA)

DoD acquisition policy has, for sometime, required programs to leverage *MOSA*. That policy has clearly not resulted in the kind of rapid, Defense Enterprise-wide, plug and play, propagation of IT capability it envisioned.

The industrial best practice for MOSA is called Product Line Architecture (PLA). PLA provides detailed technical specifications for persistent modular IT "platforms." The platform then allows efficient re-use of components and enables lucrative time-to-value for multiple IT-enabled enterprises.

Apple iPhone, iPad, and iPod, and MacBooks all share the same PLA, for example. Google and Microsoft likewise specify their own versions of PLA. In industrial PLA "open" is obviously a relative term. However, in every case of effective PLA, "open" is described objectively and in great technical detail. That is not the case in most defense system architectures.

Carnegie Mellon University Software Engineering Institute (SEI) has reported several case studies and designed a methodology to [12] exploit PLA within government. Indeed, SEI has offered a training course in PLA for several years.

The reason the Defense Enterprise has not had much success with PLA, despite technical competence, is perhaps lack of commitment to the VP and business models that make PLA lucrative in industry.

For a consumer, the VP of PLA is access to a broad family of ever-evolving capabilities from several providers via the same shared infrastructure. For provider enterprises, the VP of PLA is preventing inefficient competition among enterprise member cost centers over choice of basic infrastructure. Instead, cost centers share the same open infrastructure and differentiate themselves through their unique higher order applications. The supporting general business model is open market "coopetition" within a self-selected ecosystem of providers and consumers.

The Defense Enterprise general business model is a mandated monopoly by cost center. Each cost center has a designated constituency of consumers and a budget. The VP for the provider enterprise in this model is ironclad control of resources by member monopolies. There is no central technical authority empowered, or competent, to specify a common PLA across programs. Neither is there incentive to create such an authority. Indeed, the VP for consumers is irrelevant. Consumers in the Defense Enterprise feel constrained by regulations, training, and/or culture to "shop" only from particular designated "Programs of Record."

The N-ICE team has addressed the issue of PLA VP and business model with a "value-off-the-shelf" (VOTS) Acquisition Strategy. In this sense, off-the-shelf means that the artifact is readily available, works right out of the box, and comes with lifecycle support. The "G" or "C" in GOTS and COTS are irrelevant. The VP for the program manager in the VOTS Acquisition Strategy is to buy down most of his or her risk (to cost, performance, and schedule) with pure off-the-shelf Firm-Fixed-Price commodities. VPs for other members of an open market ecosystem flow from that concept. See figure 4.

Value Off the Shelf (VOTS) Acquisition Strategy

- **Minimizes risk to cost, performance, and schedule with out-of-the-box functionality**
- **Puts operational customer community in a feedback loop inside the production process**
- **Makes the universally painful issues of certifying Interoperability and IA a "comes with" aspect of military Product Line Architecture**
- **Provides pre-approved plug-and-play transition platform for research sponsors**
- **Eliminates bureaucratic overhead for off-the-shelf product providers to robustly demonstrate compliance and value added and achieve pre-approved product status**
- **Leverages flexible contractual vehicles that do not lock in, or lock out, any reasonably qualified provider or consumer**
- **Includes marketing and outreach function to seek out fellow early adopter providers and consumers**

Fig. 4. By deliberately creating a customer-centric market that lowers barriers to entry to both providers and consumers, the Defense Enterprise can finally leverage the value proposition associated with Modular Open Systems Approach.

In the current Defense Acquisition model, "systems" are certified as is. Any change to the certified configuration mandates re-certification or waiver. Therefore, in order to make the VOTS model credible, generic plug-and-play components must inherit the various onerous approvals and certifications from the PLA itself. That is, the PLA must provide a high assurance modularization of the security and interoperability features, which can be invoked by generic components. Further, the various authorities such as JITC and the appropriate Designated Approval Authorities (DAA) must approve the modular approach to certification. Neither of these things has been done before, but the N-ICE team is making good progress on both. Indeed the Marine Corps Systems Command (MCSC) Rapid Prototyping (RapidPro) team has developed a prototype VOTS-based tactical Persistent ISR (PISR) PLA [13] planned for accreditation by second quarter FY12.

C. Create persistent, distributed, development, test, & certification environment

The VOTS Acquisition Strategy is just a variant of the well-established commercial "Apps Store" model. That model -- wherein a universe of third party providers can easily reach a universe of consumers and vice versa -- was flourishing among provider-consumer ecosystems all over the World Wide Web (WWW) long before iPhone burst onto the scene. In each case, as previously discussed, a catalyst is well-specified computer network infrastructure that is easy to navigate by providers and consumers alike.

One of the universal best practices among these "Apps Store" variants is a persistent, virtual, test & certification environment with low barrier to entry. A would be provider signs onto a web portal and registers as a developer. In so doing, he or she agrees to a particular intellectual property rights regime, certain technological standards, and rules of behavior. The developer receives a virtual development environment, Software Development Kits (SDK) and compliance guidance. When the app (or whatever) is ready, the developer submits it to the central authority (be that eBay, Amazon, Google, Apple, etc) for test and certification. Shortly, say days, later the app is either certified and deployed, or the developer receives guidance about how to fix it.

Various Defense Enterprise initiatives have attempted to duplicate this test and certification model. However success requires a well specified enterprise IT platform with embedded, objective, machine readable, interoperability and IA controls; easy continuous access to the platform by consumers; and a business model that allows providers to readily onboard their offerings and immediately receive compensation. None of the Defense Enterprise efforts to date have had any of those characteristics. The N-ICE team aims to be the first.

The prototype N-ICE test and certification infrastructure is called Open System Test Framework (OSTF). OSTF includes a reference implementation of PISR PLA within a service-oriented framework of test tools and mission models and simulations. Simulations are live, virtual, and constructive

representations of modeled warfighting scenarios. OSTF is designed, and has been demonstrated as, a virtual environment easily accessible over the Internet Protocol network of choice, including the open Internet itself.

Live simulations include frequent field exercises. The field environment includes realistic mock-ups of Afghanistan Forward Operating Bases (FOB).

Constructive simulations are official war game scenarios – including scoring metrics -- that were created for various DoD customers over the years using various legacy technologies. OSTF has "wrapped" these legacy simulations as web services. These simulation services can be discovered and invoked at will over the network.

OSTF *virtual simulations* compose "what if" netcentric architectural "mash ups" of various combinations of sensors and weapons. These simulations support the design analysis required to extend the physical architecture and accomplish the actual physical sensor-weapon mash ups.

D. Work with Industry to Form a VOTS "Mission Thread Marketplace"

Given its large investment and compelling mission, the Defense Enterprise should be able to influence the COTS IT market to evolve in directions that align with Defense priorities. Historically, government influences markets when it does two things well: (1) fund development of breakthrough infrastructure, e.g. Internet Protocol and Global Positioning System; and (2) reduce commercial risk through pragmatic certifications. In other words, the government provides raw new technology to the industrial base. Industry innovates within the boundary conditions provided by government. The more broadly and equitably the technology distribution, and the more pragmatic and unburdensome the certification requirements, the more quickly the market delivers ever-more valued capabilities.

Perhaps, members of the Defense acquisition community should stop thinking of themselves as a developers of IT capability, and start thinking like intelligent consumers and integrators of IT capability. For example, rather than designing its own middleware "stack", government should invest in tools and methods that allow pure COTS offerings to interoperate across a federated Defense IT Enterprise usefully "out-of-the-box". After all, vendors are not likely to invest to make their competitor's products portable within their proprietary architectures. Hence, interoperability, and certainly portability, is an inherently governmental concern.

The N-ICE project aims to apply this model of government-industry partnership via a project called "PISR PlugFest." Generally, a "plug fest" is an industrial best practice for demonstrating, rather than merely claiming, interoperability. In plug fests, compliance with standards is necessary, but not sufficient. Plug fests require solution providers to prove interoperability by actually configuring their offerings in the specified environment, against specified use cases and metrics, in run time. Typically, plug fests are sponsored by "dot org" collaboratives that represents provider and consumer common interests. The venue for a plug fest is usually a series of runtime demonstrations performed within a computer network laboratory. Over the course of the event, participants tweak their software per customer-defined value criteria and compete against each other. Interoperable "killer" apps that "wow" the operational community judges inevitably win the prizes.

PISR PlugFest will use OSTF as its demonstration environment, and the embedded instantiation of PISR PLA as its baseline "plug." "Judges" will include members of the tactical ISR community as well as certification authorities such as USMC DAA, NSA, and JITC. In preparation for the PISR PlugFest, government and industry experts will study critical mission threads. Together, they will refine the PISR PLA specification to align COTS state-of-the-art with military tactical priorities. The resulting SDKs, specifications, and evaluation criteria, will be provided to industry at large as "Government Furnished Equipment" (GFE.)

To provide the VP, N-ICE will recruit government offices to issue Broad Agency Announcements (BAA) inviting COTS IT industry to demonstrate required capability in runtime at the PISR PlugFest. Some vendors will win contracts from the BAAs. All vendor offerings that add value to mission thread objectives, and successfully configure with PISR PLA IA and IoP services, will earn "pre-approved net-ready product" status. N-ICE will establish convenient IDIQ, or similar, contract vehicles for pre-approved offerings. ***All members of the ecosystem get better time to value!***

E. Learn by Doing: Seed Portfolio of Multiple Small Pilot Projects

The N-ICE approach is to establish a temporary project office with mission to "learn how to fish" in order to "teach how to fish." Accordingly, the N-ICE initial pilot effort will deliver the following:

- A growing cadre of Naval Enterprise experts in REA, and a repository of effective REA practices and REA training resources
- A growing REA ecosystem of enlightened research sponsors, programs, vendors, and certification authorities
- Persistent governance model for a continuing N-ICE process
- Streamlined, increasingly automated, approaches to address the engineering, acquisition, and oversight requirements described in the JCIDS manual
- Credible, modular approaches to defining IA and Information Interoperability, and associated Certification & Accreditation (C&A)
- Boilerplate procurement language consistent with N-ICE, e.g. solicitation, source selection criteria, Service Level Agreements (SLA), contract language, Key Performance Parameters (KPP), etc.
- Recommended persistent governance and process model to support continuous IT acquisition improvement.

- Sustainable increments of improved Naval ISR capability readily available "off-the-shelf" as pre-approved products.

The N-ICE pilot will operate under an 18-36-month charter. HQMC Director of Intelligence, as part of his implementation of the MCISR-E Roadmap, serves as the mission requirements sponsor for a portfolio of IT projects that in some way support or are supported by tactical ISR.

The Principal Deputy for Intelligence (PDI) of Navy PEO C4I is an acquisition executive with mission to support the Naval Intelligence Community writ large. In particular he is charged with guiding implementation of the MIEA study recommendation. As such, he serves as the N-ICE pilot Portfolio Manager.

F. Empower a Cadre of Government Engineering and Acquisition Professionals "

"Sergeant, pick five of your best soldiers and TAKE THAT HILL!"

Clearly the best way to accomplish any critical task is to assign it to your best person, let that person hand pick a team, and free up the team from all other responsibilities. All good leaders know this to be true.

The N-ICE project will apply this tenet by hand picking a small elite team of proven professionals. Per the N-ICE BCA, the requisite skill sets are not necessarily those found in a traditional program office. The N-ICE "un-program office" will be staffed as follows:

- Acquisition Executive to serve as an IT portfolio manager. Projects will cross program lines.
- General Manager with CIO skills. In this case "CIO" is a technical person who understands how to manage an IT budget to add value to enterprise portfolio objectives.
- Chief Finance Officer (CFO). The CFO will be qualified and incentivized to allocate funds according to the emergent needs of the enterprise portfolio, and skills of the performers, rather than according to organizational convention.
- Chief Contract Officer (CCO). The CCO will understand the actual constraints of the FAR rather than the conservative conventional interpretations. He or she will work functionally for the General Manager and apply the full suite of contract options as appropriate for enterprise portfolio objectives.
- Chief of Marketing & Outreach (CMO). Achieving enterprise efficiencies requires dedicating resources to reaching across government and commercial stovepipes. The CMO will seek out forward leaning members of the IT provider and consumer communities and formulate mutual value propositions following a "Craig's List" approach to pragmatic match making.
- Chief COTS Architect (CCA). In this sense, "Chief Architect" is the expert engineer empowered and competent to decide and explain how the technical details will come together and deliver value. A "Chief *COTS* Architect" is particularly expert in how to leverage the commercial IT ecosystem.
- General Counsel with expertise in contract law and intellectual property. The GC will be incentivized to determine how to say "yes."
- Dedicated support from within the offices of JITC, appropriate DAAs Operational Test organizations. N-ICE will treat test and certification authorities as full partners throughout project lifecycle.

IV. Conclusions

When it comes to fixing IT acquisition, we members of the Defense Enterprise have all the policy we need to get our own houses in order. Per lessons of the past, new laws and regulations will not help until we "in the trenches" commit to new thinking and processes. We owe it to our front line warriors to get this done. The organizations represented by the authors are committed to do so. The N-ICE initiative is viable and scalable. HQMC Director of Intelligence is willing to serve as Executive Agent for partnering mission sponsors. The PEO C4I PDI is willing to serve as Portfolio manager for partnering projects that wish to share N-ICE efficiencies. Together, we can create center of mass and irresistible inertia in the right direction on behalf of the greater Defense IT Acquisition reform movement.

REFERENCES

[1] Gunderson, C. R. (2009). Netcentric Warfare Revisited. (Unpublished Article). Naval Postgraduate School, Monterey CA.

[2] Headquarters Marine Corps Director of Intelligence. (2010). Marine Corps ISR Enterprise Roadmap. Washington, DC

[3] Program Executive Office Command (PEO), Control, Communication, Computers and Intelligence (C4I). (2010) Maritime ISR Enterprise Acquisition Report. San Diego, CA.

[4] Headquarters Marine Corps Director of Intelligence. (2011). Naval ISR Enterprise Rapid Evolutionary Acquisition (N-ICE) Business Case Analysis. HQMC. Washington, DC..

[5] Defense Science Board. (2009). DoD Policies and Procedures for the Acquisition of Information Technology. Washington DC.

[6] National Research Counsel. (2010). Achieving Effective Acquisition of IT in the DoD. Washington, DC.

[7] Office of the Secretary of Defense. (2010). A New Approach for Delivering Information Technology Capabilities in the Department of Defense. Washington DC.

[8] Marine Corps Systems Command (MCSC) (2010). Persistent ISR Product Line Architecture Quality Attributes. Monterey CA.

[9] Association for Enterprise Interoperability. (2010). Industry Perspectives on the Future of DoD IT Acquisition. Arlington, VA.

[10] Naval Postgraduate School. (2009). Memorandum for the Record: Value-Based Acquisition Framework. Washington DC.

[11] CYCORP. (2010). SIDECAR: Semantically Informed, Dynamic Engineering of Capabilities and Requirements Phase 1 Report. Austin TX. Douglas Lenat.

[12] Carnegie Mellon University Software Engineering Institute http://www.sei.cmu.edu/productlines/

[13] MCSC. (2010). Persistent ISR Product Line Architecture version 1.0. Monterey CA