Abstract- Coalition Warrior Interoperability Demonstration 2008 (CWID 08), Interoperability Trial (IT) #5.64 “Trusted Enterprise Service Bus” (T-ESB) demonstrates a potentially quantum improvement in the government procurement model for information systems. Joint Interoperability Command (JITC) sponsored the World Wide Consortium for the Grid (W2COG) Institute (WI) to conduct IT 5.64. WI studied the requirements of the Multi-National Information Sharing (MNIS) program to distill the following objectives:

- “Flatten” coalition networks
- Enable data and service “discovery” via semantic interoperability
- Demonstrate rapid, adaptive, evolutionary acquisition compliant with the Federal Acquisition Regulations (FAR) and based on commercial best practice.

The general premise is that the government should “buy down” as much implementation risk as possible of its basic information-processing requirement with true COTS capability. An issue is that government requirements, especially military requirements, are typically more stringent than commercial requirements. Security and interoperability are especially critical. True COTS offerings rarely address the total government requirement. Accordingly, the IT 5.64 hypothesis is as follows:

*If the government (1) continuously develops and furnishes critical raw technology to the industrial base, and (2) simply publishes its use cases, objective selection criteria, and COTS competitive procurement budget in lieu of formal Engineering Development Model (EDM)-type solicitations; Then continuing industrial competition will generate pure COTS offerings that are ever more aligned with government requirements.*

To frame IT 5.64, the WI designed a government procurement consistent with this hypothesis. The IT 5.64 prototype capability is designed as a vendor team response to that hypothetical procurement. Hypothetical source selection depends on actual demonstration of value added in realistic mission simulations. WI used a combined Coalition Maritime Domain Awareness (MDA) and Maritime Interdiction Operation (MIO) mission thread as the basis of the solicitation. Stated government priorities are rapid deployment, demonstrated utility, continuous improvement, re-usability within and across program boundaries, and Information Assurance (IA). In this solicitation, “IA” refers to two broad objectives. One objective is assured methodology for managing risk with respect to the need-to-share vs. the need-to-protect information. The other is assured data strategy for both discovering valued information, and preventing information overload. The WI vendor team response was a prototype web service stack designed to (1) enhance “Information Processing Efficiency” (IPE), and (2) execute dynamic need-to-protect vs. need-to-share security policy. The prototype has a “Trusted-Enterprise Service Bus” at the server end, and a Trusted Command and Control (C2) Web Portal (TC2P) on the service consumer end. The web service stack includes: Protection Level 4 (PL4) government-furnished security services; Unmanned Aerial Vehicle (UAV) sensor services; and Intelligent Agents that provide a “Valued Information at the Right Time” (VIRT) service. The VIRT service issues a browser pop up message when geospatially enabled software agents detect pre-defined critical conditions of interest (CCI). Analysis of collaborative interaction among eight multi-national C2 watch standers shows an IPE for the T-ESB/TC2P that is at least 60%, and as much as two orders of magnitude more, efficient than the baseline capability. Analysis also suggests 36-69% value added through “need-to-share” services. The WI team used this analysis to craft a notional vendor response to the hypothetical solicitation. Vendor claims in the solicitation response are objective and supported by runtime demonstration and analysis. The hypothetical bid includes life cycle improvement,
guaranteed software currency, continuing customer outreach, streamlined C&A, and objectively defined “open” architecture. The methodology allows government to transform its myriad technology demonstration venues collectively into a competitive marketplace of such capability. The demonstration venues need not be limited to scheduled, formal, large scale events. Any properly configured and certified laboratory can participate. JITC, supported by the W2COG Institute, can assist interested participants perform the requisite configuration, and develop the necessary FAR-compliant documentation.

I. BACKGROUND

CWID is an annual event mandated by the Joint Chiefs of Staff (JCS) to focus cutting-edge information technology on information sharing requirements defined by combatant commanders. CWID addresses collaborative information exchange among coalition partners, military services, government agencies, first responders and U.S. combatant commanders. Each CWID event showcases myriad separately sponsored “interoperability trials” (IT) loosely interlinked through mission scenarios. CWID is one of many venues designed to accelerate fielding advanced technology to the DoD and Intelligence community. It, as do all the others, suffers from the lack of an efficient technology transition process. [1]

Multi-National Information Sharing (MNIS) is a Defense Information System Agency (DISA) program. MNIS objectives are to consolidate and sustain current multinational information sharing systems; standardize products and services solution sets; provide product improvements to meet essential required capabilities; provide enhancements to meet emerging war fighter requirements. The CENTCOM Regional Intelligence Exchange System (CENTRIX) Cross Enclave Requirement (CCER) is a subset of the MNIS program. The CCER mission is to “converge physically separated coalition war fighting networks to provide a common suite of information services to all Mission Partners with controlled access to Command and Control (C2) and Intelligence applications on a common network -- based on country trust and user role” [2]

World Wide Consortium for the Grid (W2COG) is a self-selecting collaborative community of experts from government, industry, and academia. The Office of the Secretary of Defense spawned the W2COG with a research grant in FY05. The W2COG mission is to advance “netcentricity” by applying the best Internet collaborative and business models, and by removing the traditional barriers to cross-stovepipe collaboration.

The W2COG Institute (WI) is a legally incorporated not-for-profit, non-government organization (NGO) chartered to manage the activities of the W2COG. The Joint Interoperability Test Command (JITC) has commissioned the WI to study government acquisition process in context with best industry practice. In particular, JITC wishes WI to propose test and certification models designed to accelerate fielding netcentric capability.

At the request of Deputy Director DISA, WI has studied the MNIS program mission and requirements. In particular, WI designed and executed CWID 08 IT #5.64 to address MNIS issues by achieving the following objectives:

- “Flatten” coalition networks
- Enable data and service “discovery” via semantic interoperability
- Demonstrate rapid, adaptive, evolutionary acquisition compliant with the Federal Acquisition Regulations (FAR) and based on commercial best practice.

“Flatten” means to use the same physical infrastructure to support networked private coalition enclaves. “Discovery” means that consumers can compose their own versions of “operating pictures” dynamically by selecting critical bits of information from the huge pool of data available on the network. Flattening networks and enabling discovery requires balancing the “need-to-share” and the “need-to-protect” information.

II. APPROACH

The premise of CWID 08 IT 5.64 is that the government should “buy down” as much implementation risk as possible of its basic information processing requirement with true COTS capability. That premise infers that the best way to harvest up-to-date and viable technology is by simply purchasing it as it becomes available on the market. An issue is that government requirements, especially military requirements, are typically more stringent than commercial requirements. Security and interoperability are especially critical. True COTS offerings rarely address the total government requirement. Accordingly, the IT 5.64 hypothesis is as follows:

If the government (1) continuously develops and furnishes critical raw technology to the industrial base, and (2) simply publishes its use cases, objective selection criteria, and COTS competitive procurement budget in lieu of formal Engineering Development Model (EDM)-type solicitations;

Then continuing industrial competition will generate pure COTS offerings that are ever more aligned with government requirements.
valued information, and preventing information overload.

If this hypothesis tests true, then the tasks of a Program Manager (PM) become as follows:

- Deploy the best available COTS architectures and products frequently
- Divest of legacy architectures just as frequently
- Document the COTS capability vs. total requirement gap
- Invest to develop technology to bridge the gap
- Iterate continuously

To succeed in these tasks, PMs need an objective framework to enforce policy and manage the myriad and evolving options around technology, architecture, license models, test & certification, contract vehicles, billable hours, etc. The WI team designed CWID IT 5.64 to (1) test the central hypothesis, and (2) collect data necessary to design such a framework. They assumed the following:

- Operationally expert customers must play a continuing hands-on role throughout acquisition lifecycle.
- Certification authorities such as NSA, DOT&E, JRTC, DAA, must partner to streamline the acquisition process.
- Efficient technology transfer from demonstration to operations is a primary objective
- Cross-program re-use of capability is a primary objective

**III. HYPOTHETICAL SOLICITATION**

The government will (hypothetically) begin to field this capability in the first quarter of FYXX. The Government strategy is to deploy best available off-the-shelf (OTS) capability and contract with material providers to continuously improve their OTS offerings, in context with emergent operational requirements, and in close partnership with the operational user community. Contract awards will depend on actual demonstration of value added in realistic mission simulations. Government priorities are demonstrated utility, rapid deployment, continuous improvement, re-usability within the network enterprise and across program boundaries, and Information Assurance (IA). In this solicitation, “IA” refers to two broad objectives. One is assured methodology for managing risk with respect to the need-to-protect vs. the need-to-share information. The other is assured data strategy for both discovering

**Procurement opportunity:**

The government (hypothetically) intends to field MNIS capability with as many generic off-the-shelf components as possible. In that sense the government intends that its MNIS program execution funds “seed” a market for universally useful components. Other government programs are likely to consume components that have been (hypothetically) validated and pre-approved for MNIS application.

1. $10M (hypothetically) budgeted for MNIS COTS procurement in 3Q FY(XX-1)
2. Between four and twelve Indefinite Delivery, Indefinite Quantity (IDIQ) contracts awarded (hypothetically), each with $100M/yr ceiling for FYXX-(XX+5). These IDIQ contracts will be reviewed annually. Renewal depends (hypothetically) on actual performance against source selection criteria.

**Assume:**

1. Multi-member international Coalition performs MDA and MIO command and control via Internet Protocol network.
2. Government furnished equipment (GFE)* includes the following:

- Information Assurance (IA) is a primary objective including
  - An assured approach to manage risk re: need-to-protect vs. need-to-share
  - An assured approach to “discover” valued information and to prevent information overload.
Government off the Shelf (GOTS) Meteorology and Oceanography (METOC) web services.

GOTS medium assurance (Protection Level (PL) 4) GOTS authentication (AuthN), i.e. single sign on (SSO), web service. This capability uses GOTS software and open SSO standards to allow separation of different levels of access at the same security classification on the same physical networks and/or devices.

GOTS medium assurance (PL4 target) GOTS dynamic authorization (AuthZ) web service. This capability allows creation and collapsing of coalition enclaves, i.e. different levels of access at the same security classification, on the same physical network and/or devices. Authorization is based on dynamic policy that considers identity, role, and emergent factors on the ground.

Streamlined early adopter net-ready assessment process per DISA Federated Development and Certification Environment (FDCE) pilot project. **

*Available at https://svn.metnet.navy.mil (This site has been enabled support user identification and authentication using DoD PKI. For more information on how to get a PKI certificate please visit https://infosec.navy.mil/PKI or contact the NAVY PKI Help Desk at 1-800-304-4636/DSN 588-4286 itac@infosec.navy.mil)

** See https://www.forge.mil (This site is under construction as of 12-19-08)

** Task:

The operational scenario includes a geographically distributed multinational Coalition Task Force (CTF). A known threat is that adversaries will attempt to smuggle weapons of mass destruction (WMD) into the West Coast of the US from the sea. The CTF Commander’s Intent makes “Maritime Domain Awareness” (MDA) to spot potential perpetuators a top priority. Likewise, Commander’s Intent makes “Maritime Interdiction Operations” (MIO) to neutralize perpetuators a top operational priority. To support Commander’s Intent, the government requires an assured information system to accomplish, at minimum, the following critical tasks.

1. Establish at least two private information-sharing enclaves on an Internet Protocol network with separation assured at Protection Level 4 (PL4)[3].

2. Add value to the following Maritime Domain Awareness (MDA)[4]/Maritime Interdiction Operations (MIO)[5] threat/mission scenario:

a. Threat CONOP is to pose as a US Merchant vessel by transmitting false information on Coast Guard Automated Information System (AIS). When threat vessel reaches three mile limit and is screened by heavy shipping and fishing traffic it stops transmitting, changes course for the nearest point of land, and increases speed. Threat CONOP includes attempts to use environment conditions such as low visibility, high seas, or degraded electro-magnetic propagation, to further mask threat vessel maneuvers.

b. Coalition task is to uncover deception and intercept threat vessel.

** Source selection criteria:

In context with the task above, the government will competitively select vendor offerings, and renew contracts, based on a numerical score of proposals. Slide presentations and white papers without substantiating objective run-time demonstrations are non-responsive. Government encourages creative
responses that optimize options associated with architecture, technology, license, test & certification, contract vehicles, and billable hours. The government will consider the value attributes listed below in its scoring algorithms. Some of these attributes may be given greater weight than others.

1. Objective run-time demonstration of:
   a. Enhanced probability of coalition members detecting a covert maritime threat
   b. Reduced detect-to-engage time for coalition Maritime Interdiction Operations (MIO)
   c. Assured risk management in balancing need-to-protect vs. need-to-share information across a military coalition
   d. Assured data strategy to prevent information overload in a coalition Command and Control (C2) environment

2. Credible “net-ready” assessment timeline including:
   a. PL4 Secret and Below Interoperability (SABI) Certification[6]
   b. (At least) Interim Authority to Operate (IATO)[7]
   c. Interoperability certification[8]
   d. NR-KPP assessment[9]
   e. Operational Test [10]

3. Lifecycle maintenance model including:
   a. Continuing currency of IT architecture
   b. Continuing customer connection.
   c. Cost
   d. Cross-program re-usability of IT architecture

IV. PROTOTYPE SPECIFICATION

In keeping with the premise for IT 5.64, vendors respond hypothetically to the hypothetical solicitation. A WI team led by QinetQ North American and Raytheon played the role of vendors. This WI team actually consulted with members of the MDA Community of Interest[11] to develop the following counter-threat mission thread.

1. Unmanned Aerial Vehicle (UAV) sensors monitor shipping traffic including AIS transponder signals.

2. Watch standers compose “User-Defined Operating Picture (UDOP)”\(^a\) for vicinity of threat vector using the following geospatially enabled services:
   a. Automated Information System (AIS) ship tracks
   b. Meteorology and Oceanography (METOC) warnings
   c. Processed UAV sensor data

3. Intelligent agents monitor UDOP and deliver “pop up” message when critical conditions of interest occur.

4. Assured web services manage single-sign-on authentication and authorization throughout.

5. Senior coalition watch officer establishes appropriate need-to-know vs. need-to-share procedures and executes coalition MIO to neutralize threat vessel.

To enable this mission thread, the WI team built a demonstration network based on a prototype service stack on a Red Hat LINUX Dell blade as follows:

1. COTS Automated Information System (AIS) ship track web service. Commercial ships report location, course, speed, flag, and other information via VHF transponder. 

2. Map rendering web service built with COTS open source “open GIS” tools.

\(^a\) User Defined Operating Picture (UDOP) is a refinement to the traditional concept of a Common Operating Picture (COP). The idea is that pictures should not be “common”. Rather users should tailor information content based on individual mission and preference.
3. GOTS Meteorology and Oceanography (METOC) warning overlays for GIS web services.

4. COTS Unmanned Aerial Vehicle (UAV) sensor web service. This capability allows an occasionally connected UAV sensor suite to federate with a C2 network across an open source “Tactical Service Bus”.

5. COTS Valued Information at the Right Time (VIRT) “smart push”[13] service. When various pre-defined critical conditions of interest (CCI) threshold values are exceeded this web service delivers a pop-up warning message.

6. Medium assurance (Protection Level (PL) 4) GOTS authentication (AuthN), i.e. single sign on (SSO), web service. This capability uses GOTS software and COTS open SSO standards to allow separation of different levels of access at the same security classification on the same physical networks and/or devices.

7. Medium assurance (PL4 target) GOTS dynamic policy authorization (AuthZ) web service. This capability allows consumers to create or collapse coalition enclaves, i.e. different levels of access at the same security classification, on the same physical network. Dynamic policy that considers attributes related to access control, such as: identity, role, and emergent factors on the ground determines authorization.

The IT 5.64 prototype architecture brokers service transactions across an open source “Trusted” Enterprise Service Bus (T-ESB). The prototype delivers capability to consumers via a “Trusted” C2 Web Portal (TC2P). “Trusted” means that T-ESB assures authentication and authorization at PL4. (See Figure: 1) “Assurance” means that the capability of interest, in this case security, is predictable. “Assurance” does not eliminate vulnerability, it minimizes and quantifies vulnerability. “T-ESB” refers to server-side “back end” activity. “TC2P” refers to the service consumer’s experience.

**Figure 1**: The Trusted ESB brokers information transactions, forcing a Protection Level (PL) 4 authentication and authorization sequence. The authorization depends on a policy provided by the service provider. When a certain individual, playing a certain role, under certain defined operational conditions, points a browser at a URL he either gets access or not. If access is denied the requestor simply receives a standard error message.
The T-ESB is agnostic of content. It simply brokers trusted transactions among a federation of service requestors and providers who accept the risk associated with the trust model. A military “coalition” is an example of such a “federation.” Here are the crucial components of a trusted transaction:

1. Requester’s identity credentials
2. Requester’s role credentials
3. Declared “need-to-share” condition
4. Provider’s authorization policy

These four components are independent. Credentials might be biometric, Public Key Infrastructure (PKI), Long Distance Access Code (LDAC), Personal Identification Number (PIN), user-id and password, IP addresses, etc. Authorization policy defines the acceptability of a particular credential format for any particular federation.

“Identity” refers to a unique individual. An individual’s attributes include things like nationality, security clearance, affiliation, rank, etc.

“Role” refers to a temporary function such as “watch stander”, “first responder”, “commander”, etc.

“Declared ‘need-to-share’ posture” refers to emergent conditions. Members of a coalition might agree to some pre-arranged set of events that warrant varying willingness to share information they consider sensitive. For example, they might be more willing to share sensitive information during a temporary emergency. When pre-defined events occur, an authorized watch stander might set an “emergency” condition across the coalition. When events indicate that normal conditions have returned, the watch stander re-sets “normal” policy.

“Provider’s authorization policy” refers to a pre-defined set of rules set by a service provider. These rules prescribe to whom and under what circumstances to grant access. The detail of any particular provider’s authorization policy is opaque to the T-ESB, and therefore to the consumer. The policy can be very dynamic and granular. For example if a Canadian military member, serving as a watch officer on a particular aircraft, under emergency conditions, may be granted access to an Australian web service. The same or different person, serving the same or different role, at the same or different location, under the same or different condition, might or might not be granted access.

Authorization policy governs the ability to set “need-to-share” conditions. Only authorized individuals serving in authorized roles under appropriate need-to-share conditions may set need-to-share conditions.

The WI team delivered the prototype as a lightweight “breadboard” designed in close consultation with multiple potential vendors of “production models”. Vendors agreed that if the government actually issued the hypothetical IT 5.64 solicitation they would respond with robust, life-cycle supported off-the-shelf bundles.

V. CWID 08 IT 5.64 SCENARIO

The IT 5.64 server was deployed at a single node, namely Hanscom Air Force Base. The CWID Coalition watch standers deployed to various internationally distributed sites. They registered their single-sign-on credentials, and consumed “authorized” web services transparently via Internet Explorer or Firefox web browsers. Authorization depended on national identity, mission role, and emergent situation. Therefore, the operating picture viewed at different Trusted C2 Portal nodes varied.

For demonstration purposes, IT 5.64 published arbitrary US security policy. Under this hypothetical policy, US AIS ship tracks are SECRET NOFORN. All other AIS ship tracks are SECRET REL. UAV sensor data is SECRET NOFORN. METOC littoral warnings are SECRET NOFORN. All other METOC warnings are SECRET REL. Accordingly, under “normal” security policy all coalition role players are authorized to view all SECRET REL data streams. No coalition role players are authorized to view any SECRET NOFORN data streams. Under hypothetical US National “emergency” security policy, specifically authorized coalition role players may view the SECRET NOFORN US AIS tracks and the SECRET NOFORN UAV sensor data, but not SECRET NOFORN METOC warnings. Under hypothetical US National “self-defense” security policy, specifically authorized coalition role players in imminent danger may view all SECRET NOFORN data streams. (See Figure: 2.)
Figure 2: Each nation would set its own granular dynamic policy based on a general set of agreed conditions and the specific operational scenario underway. In this case the US is (hypothetically) willing to share some NOFORN data with non-US coalition members under “emergency” conditions and even more under “self-defense” conditions. Which specific data to be released to which specific nation and which specific role player depends on tactical scenario.

WI programmed the intelligent agents with pre-defined critical conditions of interest and threshold values. As the CWID scenario unfolded, these geospatially-enabled agents monitored AIS tracks, METOC warnings, and UAV sensor data “looking for” suspicious activity. Accordingly, when an AIS track approached the 3 mile limit of the US West Coast, stopped squawking as a US merchant, changed course, and increased speed, the VIR service delivered a pop up message to appropriate CWID watch officer’s browser.

In response to this notification of an “emergency” situation, the watch officer immediately used a “point and click” menu to set “emergency” security policy. (See Figure: 3.) The tactical situation demanded that non-US coalition platforms interdict the threat. That situation constitutes a pre-defined “need-share” tactically significant NOFORN track and sensor data. In response, a US national watch stander used a point and click menu to authorize those specific non-US platforms emergency-level access to the C2 Portal.\(^b\)

\(^b\) This scenario used a human-in-the-loop to set the various need-to-share conditions and authorization policies. That function can be automated, adding more risk/benefit considerations.
In the course of the interdiction the intelligent agents “noticed” that a coalition interdiction platform was in imminent danger of entering a mine field depicted on a SECRET NOFORN METOC warning. Accordingly the VIRT service delivered a pop-up message. The alert message triggered a coalition watch officer to set “self defense” conditions. It also triggered a US national watch stander to authorize the endangered vessel to have “self-defense” level of access to the TC2P.

When the Interdiction vessel avoided the hazard and intercepted the threat vessel, the coalition watch officer re-set “normal” security policy.

VI. ANALYSIS

A. The Concept of “Information Processing Efficiency”

The WI team designed the Trusted Command and Control (C2) Portal as a collaborative “service.” By definition, a “service” must provide value as perceived by the consumer. To “information workers”, human processing time is a valuable commodity. It should be spent wisely. Military information workers, e.g. C2 watch standers, tend to be very busy managing multiple information sources. Their specialized jobs require them to spend most of their own human processing time independently. Collaboration is “expensive” because it spends multiple individuals’ processing time on the same collective task. Collaboration is only valued if it achieves important objectives not obtainable individually. More bluntly stated, effective communication minimizes confusion and accelerates speed-to-decision. Accordingly, a “budget” established for managing collaborative processing would prioritize “spending” time on actionable information. The

HQ US Navy SPAWAR has conducted an excellent body of research on the subject of effective collaborative information sharing process. Their approach is called Cross-domain Information Exchange Framework (CIEF).
budget would limit time spent on “overhead” like establishing “situational awareness.”

The WI team used this time budgeting principle to design the TC2P. There were two design objectives: (1) minimize over-all processing time required for collaboration; (2) maximize time spent processing actionable bits relative to time spent processing other bits. This approach is consistent with traditional military C2 Radio-Telephone “circuit discipline.” Circuit discipline does not permit distracting idle chat; it conserves bandwidth for priority traffic; it insists on unambiguous, concise, standard language.

The objective of a budget is to achieve efficient resource allocation. Conceptually, for example, one might define “Information Processing Efficiency” as “Utility of Information Consumed” divided by “Total Bits Processed”. An issue is how to define “utility” objectively. Different consumers will have different perceptions of utility. However, it is possible for subject matter experts (SME) to evaluate the value of some data types over others. One approach SMEs can use is to identify critical conditions of interest (CCI) associated with plans of action. Plans depend on assumed threshold values of CCI. When thresholds are exceeded, action is warranted. This is the approach many stock traders use. With stock trading, having the stock value information even one or two seconds in advance of others can be worth millions of dollars. These traders subscribe to various services that inform them when threshold values of CCI associated with their portfolios are exceeded. That is the time they buy or sell. In this example traders can literally determine the dollar “value” of specific timely information. In military domains the value metric may be more abstract, but the relatively greater value of actionable information remains clear.

The SMEs for this demonstration were the CWID role players. The role players were fully tasked to manage multiple disparate and overlapping events. Accordingly, they considered “relevant” information useful if it provided new situational awareness. However, they considered “actionable” information at least twice as useful. They considered “irrelevant” information useless because it distracted them from their critical functions. The role players defined “useful relevant information” as “new information pertaining to mission elements at times and places important to mission execution.” They defined “actionable information” as “information that forces unplanned action.” Role players considered all other information to be irrelevant.

Following this reasoning, we define “Total Bits Processed” as the sum of the Irrelevant Bits (IB), Relevant non-actionable Bits (RB), and Actionable Bits (AB) processed. We also introduce the notion of arbitrary information “Utility Unit” (uu) to quantify the relative usefulness of messages. Per the subjective preference of the SMEs, we assign a value of 1 uu to relevant useful messages, 2 uu to actionable messages, and 0 uu to irrelevant messages. We consider a bit of information added to browser view of an operating picture in terms of an overlay, pop-up, or track to be a “message”.

We hypothesize that TC2P will increase the overall processing efficiency of the CWID information system. The analytical approach is to count the messages processed during IT 5.64, and bin them according to relative utility. We can then calculate Information Processing Efficiency, at least notionally, using the following formula:

\[
IPE = \frac{\text{Utility of Information Processed}}{\text{Total Bits Processed}}
\]

\[
IPE = \left( w_{IB}(IB) + w_{RB}(RB) + w_{AB}(AB) \right) \div (IB + RB + AB)
\]

We consider a bit of “Information Processed” to be “Information Consumed” divided by “Total Bits Processed”.

\[w = \text{weighting factor, } w_{IB} = 0 \text{ uu, } w_{RB} = 1 \text{ uu, } w_{AB} = 2 \text{ uu} \]

\[IB = \text{Irrelevant Bits Processed} \]

\[RB = \text{Useful Relevant non-actionable Bits Processed} \]

\[AB = \text{Actionable Bits Processed} \]

\[B. \text{ Calculating the Information Processing Efficiency of the Trusted C2 Portal} \]

IT 5.64 scenario participants were as follows:

- 2 X Coalition command centers
- 3 X US command centers
- 1 X CA Aircraft
- 1 X NZ Ship
- 1 X NZ Aircraft

Uniformed military members played roles as coalition watch standers at each of these locations. These role players were involved in multiple independent or loosely coupled Interoperability Trials. They executed the IT 5.64 mission thread, with some variation, over a period of approximately two hour each eight hour day for nine days. The IT 5.64 mission thread called for collaborative activity, i.e. viewing the TC2P operating picture concurrently, three times. That collaborative activity required a total of about ten minutes. During each iteration of IT 5.64, the role players successfully detected and responded to the threat. The generic IT 5.64 mission thread, broken down message by message, is as follows:
1. Senior Coalition Operations Watch Officer tasks all participants to view the C2 Trusted Portal for situational awareness.
   a. Watch standers across the federation view eight messages (See Figure 4)
   b. Eight messages are relevant; i.e., all information is new, presented in mission context, and pertains to the area and time of interest.
   c. Zero messages are actionable, i.e., information provides useful situational awareness only.

Figure 4: Information is presented as web service messages. Under “normal” conditions this is typical of a message viewed by non-US coalition members. It consists of blue ship icons and METOC warning overlays presented on an open source map rendering tool. Clicking on icons opens windows with more information. Layers of data click on and off. NOFORN Littoral METOC data, US Ship Tracks, and UAV sensor data are withheld.

2. Senior watch officer receives VIRT (Valuable Information at the Right Time) alert message that CCI thresholds are exceeded. NOFORN UAV sensor data and NOFORN ship track data trip VIRT alert message.
   a. One watch stander views one message.
   b. One message is relevant
   c. One message is actionable, i.e., CCI exceed threshold value and force unplanned response.

3. VIRT Alert service message causes senior watch officer to order an interdiction. Mission requires CA and NZ assets. Security services allow senior watch officer to change policy to give CA & NZ assets
access to actionable NOFORN data. Senior watch officers tasks participants to view C2 Trusted Portal and issues tasking to CA and NZ assets.

a. Eight participating watch standers each view a message.  
b. Six messages are relevant. Two messages viewed by the coalition command centers without the NOFORN sensor and ship track data are irrelevant. They provide no new situational awareness.  
c. Six messages are actionable, i.e. six messages viewed by 3 US, 1CA, and 2NZ participants display CCI and exceeded threshold values in mission context. The message forces and enables unplanned action. Without the VIRT service and security services these actionable messages would not have been processed.

4. VIRT Alert service informs senior watch officer that NZ ship is in danger of entering minefield. Minefield warning is SECRET NOFORN.  
a. One watch stander views one message.  
b. One message is relevant  
c. One message is actionable, i.e. CCI exceed threshold values and force unplanned response.

Figure 5: The VIRT service informs the authorized watch stander that a US Merchant ship hit the three mile limit, stopped squawking, and tuned inland. He sees that the SS Black Pearl icon has changed from a ship to a skull and cross bones courtesy of NOFORN UAV sensor services. The NZ interdiction vessel is going to run into one of the SECRET NOFORN mine fields depicted with red icons. This situation calls for “self defense” need-to-share conditions. At the click of a mouse, and the refresh of a browser, the NZ ship views the danger.
5. Security policy allows senior watch officer to grant NZ ship access to NOFORN METOC warnings. Tasks participants to view C2 Trusted Portal. Issues tasking to NZ ship.
   a. Watch standers across the federation view eight messages. (See Figure: 5).
   b. The four messages viewed by the US participants and the NZ ship are relevant. The four messages viewed by participants without authorization to see NOFORN METOC warnings are irrelevant – they provide no new situational awareness.
   c. Four messages are actionable, i.e. four messages viewed by US and NZ ship provide CCI and exceeded thresholds in context that enables required unplanned action. Without VIRT service and security services these actionable messages would not have been processed.

Watch standers participating in IT 5.64 viewed a total of 34 web services messages each day. The TC2P message utility breaks out as 6 irrelevant, 16 relevant but not actionable, and 12 actionable messages. The notional Information Processing Efficiency is calculated below:

\[ IPE = (w_{IB}(IB) + w_{RB}(RB) + w_{AB}(AB)) + (IB + RB + AB) \]

\[ IPE_{TC2P} = (0uu(6) + 1uu(16) + 2uu(12)) + ((6) + (16) + (12)) = 1.18uu \]

What if the SMEs decide to consider actionable information that allows them to intercept WMD to be ten times more useful than situational awareness information? In that case, \( w_{AB} = 10 uu \) and the notional IPE for the IT 5.64 sequence calculates to 4.00uu.

C. Value Added by “Need-To-Share” Services

Consider steps three and five above. Note that without the TC2P security services -- or in this context, “need-to-share” services -- the messages viewed by the CA and NZ assets would not include the actionable NOFORN information. In other words, the sensor service would have provided critical information to US watch standers. The VIRT service would have alerted a US watch stader. However without a “need-to-share” service, the utility of the NOFORN information is diminished. In that case, four messages that were actionable with NOFORN information become irrelevant without it. The six messages viewed by US watch standers with the NOFORN data remain relevant, but are no longer actionable. The message utility breakout for this sequence becomes 10 irrelevant, 22 relevant but not actionable and 2 actionable messages. The IPE for that case is calculated below.

\[ IPE = (w_{IB}(IB) + w_{RB}(RB) + w_{AB}(AB)) + (IB + RB + AB) \]

\[ IPE_{TC2P\text{sans security services}} = (0uu(10) + 1uu(22) + 2uu(w)) + ((10) + (22) + (2)) = 0.76uu \]

The IPE without security services is 36% less efficient than IPE of the full TC2P service suite. If SMEs decide that information that allows intercept of WMD is ten times more useful than other relevant information, IPE for this case becomes 1.24uu – compared to 4.00uu is 69% less efficient than with need-to-share services.
D. Calculating Information Baseline Processing Efficiency

To provide a baseline comparison, we assume that basic CWID capability, without the TC2P, includes an AIS ship track “picture”. For this baseline case, we assume that the role players simply view the AIS picture three times – the same number of viewing as in the IT 5.64 scenario. This assumption is reasonable compared to typical coalition C2 Concepts of Operations (CONOPS). The message-by-message breakdown for this baseline case is as follows:

1. Senior coalition watch officer tasks all participants to view C2TP for situational awareness.
   a. Watch standers across the federation view eight messages
   b. Eight messages are relevant; i.e. all information is new, presented in mission context, and pertains to the area and time of interest.
   c. Zero messages are actionable, i.e. information provides useful situational awareness only.

2. Senior watch officer tasks all participants to view C2TP for situational awareness. The threat vessel has stopped “squawking” and has disappeared from the cluttered picture. Even if a busy watch stander notices, there is no means to locate the missing merchant vessel.
   a. Watch standers across the federation view eight messages
   b. Three messages are relevant. The messages viewed at US sites no longer include an icon representing the threat vessel – an indicator, if they notice, of a potential threat. Five messages are irrelevant. Without NOFORN ship tracks they do not provide new information.
   c. Zero messages are actionable.

3. Senior watch officer tasks all participants to view C2TP for situational awareness. By now, if the threat has not been detected and intercepted by other means it is too late.
   a. Watch standers across the federation view eight messages
   b. Eight messages are irrelevant.
   c. Zero messages are actionable.

In this baseline scenario watch standers viewed a total of 24 messages. 13 are irrelevant, 11 are relevant, and 0 are actionable. The IPE for this baseline case as calculated below is 0.46uu, which is 61% less efficient than the 1.18uu efficiency of the TC2P.

\[
IPE = (w_{IB}(IB) + w_{RB}(RB) + w_{AB}(AB)) / (IB + RB + AB)
\]

\[
IPE_{Baseline} = (0uu(13) + 1uu(11) + 2uu(0)) / ((13) + (11) + (0)) = 0.46uu
\]

A typical coalition C2 CONOP, without the benefit of automated software monitoring services, calls for human watch standers to view the operating picture frequently. In the baseline scenario above, if watch standers viewed the operating picture just once every 30 minutes, i.e. four times instead of three, the calculated IPE would be 0.34uu. Each time the eight busy watch standers view a low value message, the IPE decreases geometrically. Granted, some C2 “searches” would likely return relevant or even actionable information. However, each time the VIRT service “delivers” a message guaranteed to be useful, and the security services guarantee it can be shared usefully, the IPE increases exponentially. By this reasoning it is clear that TC2P services increase the
assurance that information processed by busy humans will be useful. This finding in no way implies that C2 watch standers should not “search” for information. Rather, it implies that smart push services -- designed to inform of known critical information elements -- can free up human processing time and provide insight for more intelligent searches. Consumers informed by these intelligent searches, may then add to or revise alert criteria in their VIRT service portfolios.

VII. RESPONSE TO THE HYPOTHETICAL SOLICITATION

Although the IT 5.64 analysis is notional, the approach is viable. It demonstrates that the “value” of information, and the value of sharing information, can be credibly quantified through analysis of critical information transactions. This mission level model approach can be modeled in digital formats [15]. SMEs can validate any particular architecture in run-time mission simulations using network performance test tools. The realistic objective outcome are suitable for comparing relative merits of competing architectures. A notional description of such an outcome is described below in context with the hypothetical MNIS solicitation.

“….. In context with the task above, the government will select vendor offerings, and renew contracts, competitively based on a numerical score of proposals. The government will consider slide presentations and white papers without substantiating objective run-time demonstrations as non-responsive. Government encourages creative responses that optimize options associated with architecture, technology, license, test & certification, contract vehicles, and billable hours. The government will consider the value attributes listed below in its scoring algorithms. Some of these attributes may be weighted more highly than others. “

1. Objective run-time demonstration of:

   a. Enhanced probability of coalition members detecting a covert maritime threat

   In the IT 5.64 mission model and simulation TC2P sensors services identified and “tagged” 100% of AIS tracks identified as US Merchant vessel that stop transmitting. VIRT services correlated 100% of tagged tracks against threat profile. M&S results showed 0 false alarms and 100% actual threats detected upon entering interdiction window.

   b. Reduced detect- to-engage time for coalition Maritime Interdiction Operations (MIO)

   In the IT 5.64 M&S, non-US assets were required to engage threat. TC2P need-to-share services allowed real-time transmission of essential NOFORN targeting data. The current process requires a minimum of sixty minutes processing time before releasing sanitized or re-classified information.

   c. Assured risk management in balancing need-to-protect vs. need-to-share information across a military coalition

   Government furnished authentication and authorization services, together with dynamic and granular security policy, provide mechanism for balancing need-to-protect vs. need-to-share. Capability is assured at Protection Level 4.

"The M&S supporting CWID IT 5.64 was conceptual and functional rather than rigorous and performance-based. Performance based SOA testing is an immature domain and a subject of WI research. The WI can help the government apply and improve existing best-of-breed SOA performance based testing and validation and verification to support an actual procurement.
d. Assured data strategy to prevent information overload in a coalition Command and Control environment

IT 5.64 M&S analysis shows that T-ESB/TC2P provides at least 60%, and as much as two orders of magnitude, greater Information Processing Efficiency as compared to the baseline capability. That analysis proves how VIRT services guarantee increased IPE and frees processing time to allow for better informed searches for information.

2. Credible “net-ready” assessment timeline including:
   a. PL4 Secret and Below Interoperability (SABI) Certification
   b. (At least) Interim Authority to Operate (IATO)

The WI team is working with NSA and an operational activity, Fleet Numerical METOC Center (FNMOC), and its Designated Approval Authority (DAA) to deploy the T-ESB (at SABI PL4) in FNMOC’s accredited environment under an existing ATO. The team is developing components of the T-ESB in context with the “Multiple Independent Levels of Security” (MILS) architecture and the Defense Information Assurance C&A Process (DIACAP) methodology [16]. An objective is to streamline the C&A process through, re-useable “type-certified” medium and high assurance web service component. This partnership delivered a PL4 SABI certification for an authentication component of the T-ESB in eighteen months. Thirty-six months is more typical. Target is C&A and updated ATO complete by 3rd Q FY09. MNIS DAA can leverage this on-going investment to accredit T-ESB in his/her chosen environment(s).

   c. Interoperability certification
   d. NR-KPP assessment
   e. Operational Test

The WI team has engaged with JITC and DISA regarding items 2.c. - 2.e. The WI team is performing as an early adopter in the Federated Development and Certification Environment Pilot (FDCE) project. That project aims to perform “net-ready assessment” in parallel with development. CWID 08 IT 5.64 was designed specifically to enable the FDCE concept. The Target to place T-ESB/TC2P on approved DISA approved products list by 4th Q FY09.

3. Lifecycle maintenance model including:
   a. Continuing currency of IT architecture

WI team bid includes quarterly software upgrades and a guarantee to install all applicable new standards within three months of their release. Using the methodology demonstrated in CWID 08 IT 5.64, the WI team will continuously evaluate new technology in context with government requirements. WI will propose timelines for intercepting new vectors and divesting legacy architecture -- and associated cost benefit analysis -- for government consideration.

   b. Continuing customer connection.

WI team bid includes a continuing customer outreach program, i.e., one three day visit per month to a site designated by the government. Visits will inform customers of detailed functionality and collect potential new use cases. WI team will also recruit and nurture a distributed “beta community” among the government customers. Input from the outreach and beta efforts will inform quarterly the software update cycle. WI team will maintain a 24 X 7 trouble desk and provide on-site technicians to resolve any trouble tickets still open after 72 hours.

   c. Cost
WI team (hypothetically) bids $10M/yr, renewable annually, to manage T-ESB/TC2P as a network service suite. Bid includes unlimited software licenses, all server-side hardware, and lifecycle support required to deliver capability described herein. Bid includes processing data flows from all discoverable sensor web services. Bid does not include delivery or maintenance of UAV or other sensor platforms.

Alternatively, WI team will negotiate professional services contract required to install and maintain this network service suite at designated government sites.

Alternatively, WI team will negotiate pricing for COTS T-ESB/TC2P appliance (pre-loaded server blades and shrink-wrapped client-side software) including lifecycle support as described here-in.

d. Cross-program re-usability of IT architecture

WI team will maintain all information technology delivered under this procurement as purely generic “off-the-shelf” commercial standard catalog offerings. WI will offer all capability under unlimited enterprise software licenses. WI team will maintain all furnished GOTS components, and any software developed at government expense, under Open Source Software (OSS) General Purpose License (GPL). WI team will honor any caveats or modifications to GPL required by the government.

VIII. CONCLUSIONS

The mock off-the-shelf procurement represented by CWID 08 IT 5.64 need not have been mock. Further, the procurement need not have been limited to IT 5.64. If the government had chosen to actually solicit vendor proposals against real procurement opportunities, CWID 08 could have delivered any number of real, pre-approved, supportable, off-the-shelf network capability upgrades. The methodology demonstrated by JITC in IT 5.64 literally allows government to transform its myriad technology demonstration venues collectively into a competitive market place of such capability. The demonstration venues need not be limited to scheduled, formal, large scale events. Any properly configured and certified laboratory can participate. JITC, supported by the W2COG Institute, can assist interested participants perform the requisite configuration, and develop the necessary FAR-compliant documentation.

REFERENCES


