LEADERSHIP FOR A NETWORKED WORLD PROGRAM/EXECUTIVE EDUCATION
John F. Kennedy School of Government
Harvard University
Case 07-2007

Maritime Domain Awareness[1]

A Case Study in Cross-Boundary Information Sharing Among the United States Navy, Coast Guard, and Department of Transportation

> *"Cutters may be rendered an instrument of useful information concerning the coast, inlets, bays and rivers of the United States, and it will be particularly acceptable if the officers improve the opportunities they have in making such observations and experiences in respect to the objects …reporting the result from time to time to the Treasury." Alexander Hamilton, 1791 letter of instruction to the commanding officers of the Revenue cutters, the forerunners of the United States Coast Guard*

In November 2005, Mike Krieger was in Colorado Springs to brief an Air Force team on space situational awareness when he found himself instead surrounded by a Coast Guard Admiral and a sea of senior sailors, soldiers, airmen, and marines who wanted to hear what he had to say about oceans and everything that moved there.

Two years earlier senior representatives of departments and agencies who touched what insiders called "the maritime domain" had gathered in a summit at the White House to carve up responsibility for "awareness" of any and all ships, cargos and crews as they moved on the seas of the world, or the rivers and lakes of America. After years of difficulty sharing data – perhaps information was lost or guarded somewhere in a bureaucracy, or caught in a conflict between intelligence and law enforcement agencies, or lacked interoperability and the means to be shared, or became a casualty of intra-agency rivalry, mistrust and orneriness -- at this meeting, on this day, Secretaries Rumsfeld of Defense and Ridge of Homeland Security wanted to know, this: How would all agencies of government deploy their vast capabilities to create cross-domain maritime awareness, and ultimately, safety, for the nation, its ports, and legitimate maritime commerce?

The choices were many but constrained. With two conflicts raging in Iraq and Afghanistan, agencies guarded their budgets closely. Admiral Joseph Nimmich of the United States Coast Guard reflected on the circumstances.

---

[1] This case was written by Zachary Tumin, Executive Director, Leadership for a Networked World Program.

"Whenever you're dealing with inter-agency efforts, as a new concept comes out, there's a great deal of concern and trepidation. 'What is this going to do to me?'," he observed. "But especially then, in a very tightly constrained budget environment, it was hard to expect that agencies would spend money on something other than what was planned for, let alone give over authority to an inter-agency group to spend it for them."

It did not assuage fears that the concept of *maritime domain awareness* was itself vague. "Is it," Nimmich asked, "seeing everything everywhere all the time, or is it what do I really need to see, and when, so that I'm not overwhelming myself?"

Much depended on the definition of the problem. For as vaguely defined at it was, providers were tempted to offer a wide range of solutions. "You've got people who go from the extreme of, 'We need a new $100 billion dollar space surveillance system to 'Hey, this could be far less technically difficult that we think.'"

The reality of the problem was apparent, and significant. "Not only did 9/11 show that we have a problem with airplanes," Mike Krieger observed. Krieger was Director of Information Policy for the Department of Defense's Chief Information Officer. "But we were not tracking merchant ships as they came to the docks. All DoD ever tracked was Navy ships, friendly and enemy. I think they figured out we really needed to start looking at maritime domain awareness and, really, the merchant sector was where the biggest threat was."

"Most of all," Joe Nimmich said, "we needed a concept of operations to define what we were going to try to accomplish, and where the biggest return on any investment would be."

John Shea, who would soon lead the MDA COI technical effort, offered up the bureaucratic "begats" in his own 80-slide Powerpoint deck of 12 April 2007, "MDA Data Sharing COI Information Brief":

> "The MDA Summit of 7 May 2004 created the Senior Steering Group (SSG) which oversaw the writing of the NSPD-41/HSPD-13, Maritime Security Policy, (released December 2004) which directed the writing of the National Strategy Maritime Security (NSMS) and the eight supporting plans, one of which was the National Plan to Achieve MDA (NPA MDA). Chapter IV, page 18, tasks the Maritime Security Policy Coordinating Committee (MSPCC) to establish the MDA-IT, co-chaired by DOD and DHS. [Summing up, the] MDA Summit begat the SSG which begat the NSPD-41/HSPD-13 (MSP) which begat the NSMS and eight plans, including the GMII, the MOTR and the NPA MDA, which begat the MDA-IT."

If the bureaucratic moves were maze-like, the technical challenges of creating a unified view of the maritime domain were no less so. In fact, the range of national surveillance capability and awareness was extraordinary. There existed a complex web of sophisticated space-based observation posts, sea-borne radio telemetry, and land-based human intelligence that ultimately "saw" nearly every vessel – every object – that moved above, through, and under the seas, and knew much about their cargos and crews. Whether from deep space or deep ocean, somewhere, someone was tracking movement, looking to better understand the situation in the domain and manage its risks.

Civilian communities of shippers and brokers, for example, were particularly interested in the status of their cargos, ships and crews as a business concern. They used shipboard *automated identification systems* ("AIS") to beam and track ship, crew and cargo data on all large ocean-going vessels.[2]

Border control communities – US Customs, Coast Guard, and Immigration officers among them – scanned for signs that a vessel or a person that was approaching the United States posed a risk. Traditionally, they used a combination of AIS, radar, visual, and physical patrols to understand the domain.

Naval and Coast Guard operations communities were concerned with the risk to their vessels on the open seas and ports. They used the Global Command and Control System - Marine to track other vessels.[3]

Intelligence communities were concerned not just with asset protection domestically and abroad, but with homeland security. They used "national technical means" -- satellites and sensors -- to scan the globe to systematically discern legitimate

---

[2] The **Automatic Identification System** (**AIS**) is a system used by ships and Vessel Traffic Services principally for identification and locating vessels. AIS helps to resolve the difficulty of identifying ships when not in sight (e.g. in fog, at distance, etc.) by providing a means for ships to exchange identification, position, course, speed, and other ship data with all other nearby ships and VTS stations. It works by integrating a standardized VHF transceiver system with an electronic navigation system, such as a LORAN-C or Global Positioning System receiver, and other navigational sensors on board ship (gyrocompass, rate of turn indicator, etc.). The International Maritime Organization's (IMO) International Convention for the Safety of Life at Sea (SOLAS) requires AIS to be fitted aboard international voyaging ships of 300 or more gross tonnage, and all passenger ships regardless of size. It is estimated that more than 40,000 ships currently carry AIS class A equipment. (www.wikipedia.org)

[3] **Global Command and Control System** (**GCCS**, pronounced "GEEKS") is a system of Command, Control, Communications, Computers, and Intelligence (C4I) systems and applications. Although GCCS is the Department of Defense (DOD) Command and Control (C2) system of record, there are GCCS variants fielded by the US Army (GCCS-A), the US Air Force (GCCS-AF), and the US Navy/Marine Corps (GCCS-M) and Joint Command Centers (GCCS-J) . GCCS was developed to replace the Worldwide Military Command and Control System (WWMCCS). GCCS is an automated system designed to support situational awareness, crisis action planning and other mission areas, and is intended to be the C4I system that supports the warfighter from the foxhole to the command post.

ocean, river and lake-going traffic from the few vessels that perhaps posed some risk to the nation or its interests.

There was one rather large problem: none of the many systems in use tracking cargos, conveyances or people, whether civilian or military, could "talk" to each other – even when carried on the same network -- whether to see or display the other's data.

"As an example," John Macaluso recounted, "HSIN -- the Homeland Security Information Network – might project a map of, say, New York Harbor." Macaluso is a Captain in the United States Coast Guard and Program Manager of its Research and Development efforts. "If something's happening in New York, all the other watch centers can click and get that same map. Before the COI approached them, the map had icons that would link them to detailed data on port infrastructure -- who owned a dock, or a wharf. But at the time, the map of New York Harbor had no information on which ***ships*** were in the harbor. While planned, it had not yet been implemented."

The MDA-IT – or implementation team – convened in late fall 2006 in Colorado Springs to map out a concept of operations, or "CONOPS", for the maritime domain initiative. How would it go forward to implement its charter? The MDA-IT was co-chaired by Rear Admiral Joseph Nimmich of the United States Coast Guard's Domain Awareness Directorate, representing the Department of Homeland Security, and Army Brigadier General Frederick Rudesheim of Joint Staff J-5 Policy Directorate, representing the Department of Defense.

Mike Krieger was scheduled to be last briefer up after three days of MDA-IT sessions. He was in Colorado Springs on other business – to meet with the Command and Control Space Situational "Community of Interest," one of the first "COIs" he'd helped establish under charter from the Department of Defense's Chief Information Officer, and Secretary of Defense. It would be easy to add the MDA-IT sessions to his itinerary. All Krieger had to do now was brief the MDA-IT on his community of interest charter, take a few questions, and get back to Washington.

Krieger might not have guessed it at the time, but within the year some members of this same group and he would demonstrate to US Navy and US Coast Guard admirals alike a view of the world's maritime traffic that streamed four complex data feeds to three different types of display terminals, at far less cost and complexity than current systems required. They would demonstrate and offer a view of the maritime domain that no admiral, no ship driver, and no intelligence chieftain had, in the history of world maritime navigation or warfare, ever had before.

For now, though, Krieger's job was to brief the MDA-IT at the most general level on the mission of the COI initiative. He'd had some luck with the Space Command

Community of Interest, and could share some lessons learned, as it was one of the first COIs "stood up" by Krieger in response to two foundational DoD policy documents.

The first document had been signed by then DoD CIO John P. Steinbit on May 9, 2003. It required that the Department of Defense make available as much data as possible to as many people as possible in a "net-centric strategy."

> This DoD Net-Centric Data Strategy outlines the vision for managing data in this net-centric environment. Net-centricity compels a shift to a "many-to-many" exchange of data, enabling many users and applications to leverage the same data—extending beyond the previous focus on standardized, predefined, point-to-point interfaces. Hence, the net-centric data objectives are to ensure that all data are visible, available, and usable—when needed and where needed—to accelerate decision cycles. In a net-centric environment, unanticipated but authorized users or applications can find and use data more quickly. One of the CIO's goals is to populate the network with all data (intelligence, nonintelligence, raw, and processed) and to change the paradigm to "post before processing"—allowing authorized users and applications access to data without wait time for processing, exploitation, and dissemination. Users and applications will post all data to "shared" spaces, increasing the amount of Enterprise and community data while minimizing private user or application data. All posted data will have associated metadata (i.e., data about data) to enable users and applications to discover, and evaluate the utility of, shared data.

Further, Steinbit's directive introduced the concept of "Community of Interest" as a vehicle through which the Department could realize the net-centric strategy.

> The strategy also introduces management of data within communities of interest (COIs) rather than standardizing data elements across the Department. COI is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange.

Krieger knew the brief well. "Steinbit said you have to make the data ***visible*** – that means it has to be discoverable. If you can find it, it has to be ***accessible*** so that everybody who's authorized can access it. And, then, you have to make it ***understandable***, so that there is a common vocabulary for communities, so that when you discover the data, and access it, you actually recognize what the data is. And then, you have to make it ***trusted***, so that people have comfort with sharing and using data knowing who will use it and where it came from. It hast to be ***interoperable***, so that everyone can use it. Lastly, the final thing is it has to be ***governable*** – we're doing something that is inherently joint and there is some governance required."

The other document, signed in 2004 by Paul Wolfowitz, then Deputy Secretary of Defense, directed that the Department, in fact, "stand up" the Communities of Interest:

> 4.7. Semantic and structural agreements for data sharing shall be promoted through communities (e.g., communities of interest (COIs)), consisting of data users (producers and consumers) and system developers, in accordance with reference (b).

"That basically said, 'Ok, go implement the strategy. Form communities of interest to address the information sharing problem, and go make your data visible, accessible, understandable, trusted and governable,'" Krieger said. "So from that point we were looking for communities with sufficient interest in leadership to start making this work."

"That," observed Krieger, "was the basis of this transformation in 2003-4 – from 'need to know,' to 'need to share'.

As last briefer up on the last day of the three day MDA-IT kick-off, Krieger followed a Joint Staff officer who previewed an 18-month work plan to produce the MDA-IT CONOPS.

"I gave them a pretty standard brief," he said, "first on the net-centric data strategy, and then how we were trying to establish communities of interest that had information sharing problems," Krieger said.

The COI concept appealed to some. "When you do a COI," Krieger said, "you scope your problem to something that you can actually deliver a solution to within nine to twelve months, and from that solution you keep building. If you go to the COI thing and do a pilot you can inform the CONOPS before it's even finished. I told them I was on that path -- I wanted a community to get together, identify a problem, scope it, and go *do* something in nine months. And I think it's what got them excited."

Admiral Joe Nimmich, one of the two MDA-IT co-chairs, approached Krieger after the session and indicated he would be willing to be the DHS sponsor for the MDA COI.

"What Mike presented," Nimmich observed, "was pretty simplistic. It came down to, in an interagency environment, how do we get people to agree to a schema and define data so that no one has to change anything they have done, and we can allow people into our databases with the right controls on it – without abandoning our legacy systems or investing in new ones?"

"This resonated with me," Nimmich continued, "because I knew my problem was to start 'knowing what I knew', rather trying for a new acquisition in an environment where it was going to be rejected out of hand due to budgets."

Nimmich also liked the speed and clarity of Krieger's suggestion. The interagency CONOPS was causing conflict and confusion, as the agencies had different images of it. It would take a lot of "inside the beltway" bureaucratic alignment, and a lot of time. "Trying to get agreement on what the concept of operations would in fact entail was itself going to be an awful lot of work," Nimmich observed.

"Krieger said, 'I can help you start sharing information fast,'" Nimmich recalled. "The CONOPS and the COI were both talking about the same thing – data management – just approaching it differently. I felt we could do both, and our only challenge would be how to link them together."

As the November meetings closed, Nimmich and his MDA-IT co-chair affirmed their support for the continued CONOPS development. The MDA-IT in fact adopted the CONOPS approach.

But Nimmich's commitment to the MDA COI also gave Krieger one of the two sponsors he needed to launch the MDA COI. Rather unexpectedly, Krieger left Colorado Springs in November 2005 with a new COI poised for development, and in the Coast Guard's Joe Nimmich, a senior-most DHS executive as its foundational sponsor.

* * *

That left Krieger with the need to find appropriate senior-most DoD sponsorship for the MDA COI. The new US Northern Command (NORTHCOM) was the obvious place to look, having been established shortly after the Al Qaeda attacks on New York and Washington in 2001. With headquarters at Peterson Air Force Base in Colorado Springs, NORTHCOM had regional command responsibility for North America and for collaborating with DHS on homeland security.

To entice interest, Krieger could dangle technical support – two staff members for six months to support any needed technical development, plus some minimal funding. But what really mattered to Krieger was finding the right executive – one who would have passion for the overall effort, and stature to help navigate it.

"My job is to get people to lead it, and for me to be the best 'wingman' in town," Krieger said. "But you do need flag level support to break down the barriers initially."

As often as not he might strike out, and would move on. "If they don't show any interest, which happens 50% of the time, I just go on and find somebody else. When you're trying to transform a department, it's not worth pushing people. They have to want it."

With Nimmich's help, within weeks Krieger had worked his way up the NORTHCOM chain of command through the J3 and J4 and J5's. Ultimately, in a meeting with staff and NORTHCOM "J6" (then) Rear Admiral Nancy E. Brown, Krieger secured a treasured asset: Brown's assent to serve as the DoD MDA COI sponsor. NORTHCOM's commander, Navy Admiral Timothy J. Keating – who himself faced a staggering post-Katrina problem to "know what he knew" throughout the NORTHCOM domain -- had directed Brown to assess the MDA COI opportunity, having caught wind of it through Pentagon channels.

"It was an area that I was particularly interested in," recalled Brown. "We had been doing basic work in trying to figure out what kind of common operational picture the commander needed, where we could get the feeds, and how we could blend all of the areas into one picture. This played right along with that requirement."

As NORTHCOM Director of Architectures and Integration, Nancy Brown represented a significant win of stature for the MDA COI initiative. "I got a combatant commander. That works for the Secretary in DoD," observed Krieger. "And I got the combatant commander responsible for homeland defense in DoD willing to say, 'I'm the right combatant commander, I'm worried about maritime domain awareness, and I'll be the co-sponsor.'"

"I knew that Mike needed someone who was interested, could dedicate some resources to it, and keep it on track," Brown recalled. "It was a 'plus' from everyone's perspective. We all needed this and rather than pursue it alone, it made a lot more sense to pursue it as a group."

The matter of governance had still to be squared away, principally the outstanding issue of how the MDA-IT and the MDA COI would co-exist. With Nimmich wearing hats in both camps-- as MDA-IT co-chair and MDA COI sponsor – by January 2006 all met and concurred that MDA-IT and MDA COI would co-exist, pursue their destinations separately, but in concert with overlapping teams, keep the other informed, but not slow the other down. It was a low-friction resolution that suited all. Nimmich, in turn persuaded USCG Rear Admiral Ronald T. Hewitt to take up the reins as MDA COI co-chair with Navy Rear Admiral Brown.

Having brought DoD and DHS together within the COI framework, Krieger set about navigating the MDA COI's first operational steps, focusing now on convening a launch of the MDA COI at NORTHCOM facilities, back in Colorado Springs, in February, 2006.

* * *

Framing the Issue

"The concept of a community is you get people together to solve an information sharing problem. The problem," Krieger said, "is coming ***up*** with a problem. And that's what I said: the first thing they have to do is to tell me what information sharing problem is here that we have got to solve, because you cannot do a community unless you have a problem to solve. And you solve it," Krieger said, "by exposing your data."

The Problem

"We call it "'IFF for Ships'." Likening the maritime Automated Identification System ("AIS") to the two channel interrogation system required by the Federal Aviation Administration of all aircraft in US airspace, to "identify friend or foe".[4] "It's required of all ships three hundred gross tons and above," Krieger explained. "They have to install an AIS device connected to a UHF transmitter that broadcasts information about who they are, where they are going, what their speed is, what their direction is, and what cargo they have. They just broadcast it steadily, and anybody can interrogate them. Countries use AIS around coast lines to identify the ships that are going past them."

The Navy was already hard at work installing AIS receivers under the maritime domain awareness campaign. "The Chief of Naval Operations ['CNO'] told Andrew Cox's guys at C4I in San Diego that they had to immediately ramp up and do an AIS receiver system for Navy ships," Krieger said. Cox was Deputy Program Executive Officer of the Navy's Command, Control, Communications, Computers and Intelligence efforts, commonly known as "C4I". "He wanted to know where all Navy ships were, and have any Navy ship interrogate any ship anywhere, anytime. So, C4I was working hard to just solve the Navy problem. But Andrew saw that it is not just a Navy problem. It is really Navy, and it is industry, and commercial ships."

Frank Petroski of MITRE Corporation saw the same landscape. "The Navy has a system to track the position of Navy vessels; the Coast Guard has the AIS system which goes on all commercial ships and sends out information on registry, country of origin, manifest information. There are intelligence sources that allow basically position

---

[4] "The need to be able to identify aircraft more easily and reliably led to another wartime radar development, the Identification Friend or Foe (IFF) system, which had been created as a means of positively identifying friendly aircraft from enemy. This system, which became known in civil use as Secondary Surveillance Radar (SSR) or in the USA as the Air Traffic Control Radar Beacon System (ATCRBS), relies on a piece of equipment aboard the aircraft known as a 'transponder'. The transponder is a radio receiver and transmitter which receives on one frequency (1030 MHz) and transmits on another (1090 MHz). The target aircraft's transponder replies to signals from an interrogator (usually, but not necessarily, a ground station co-located with a primary radar) by transmitting a coded reply signal containing the requested information." www.wikipedia.org.

reporting on ships that do not have transponders. The whole issue is how do I collect all that up for those different sources and get it in a display that I can understand?"[5]

"None of these three had any plans to share information with each other," Krieger observed. "The problem we have is to take these three databases, advertise that they are out there, and publish their information. Anybody who is authorized ought to be able to get any information from any of these databases. That is what we have to do for this community," he explained.

A fourth database was soon discovered and acquired: the US Department of Transportation's Volpe Center data base (NAVEUR MSSIS). "They stumbled across our community, and said, "Gee, if we can publish information and then use your information, that is good for us. That was appealing to Volpe, and they came in."

Thus, the initial problem was framed: how to get all the data producers who collected information - Navy, Coast Guard, and Department of Transportation - to agree on how they would standardize and share the data that they each independently acquired and produced on the AIS net. Nimmich felt that the AIS would be the right place to start as it was relatively new, had a well-defined data stream, and as yet, not much customization by individual users.

"Each of us is collecting a certain kind of information over AIS," Nimmich observed. "Just by bringing it all together, I will multiply in one picture all of the AIS signals so that in any part of the world, depending on whose picking up the traffic, you can see what we all know – from each of our different signals. Domestically," he explained, "most of it is being picked up by the Coast Guard. But globally, most of it is being picky up by Navy vessels or other partner vessels as in the case of the Volpe system. Can we publish what we pick up to those other users? "

"We wanted a good win to show that this could be done," observed Nimmich. "To 'know what we already know', expand our pictures by looking at what everybody else brought in, and not invest a lot of money up front."

* * *

[5] Initially identified 3 AIS Data Producers – currently 4:

- **Navy AIS RDC Shipboard program**
- **Coast Guard Operations System Center (R&D Center Experimental Network – will become NAIS)**
- **NMIC/ONI – Automatic Maritime Reporting System (AMRS)**
- **DOT / Volpe Center – NAVEUR MSSIS data**

The Work Proceeds: February and Beyond

John Shea, who would become project manager for the MDA COI pilot went to Colorado Springs. As Technical Director for C4I, his boss was interested in seeing whether the directive to standup the Navy's own AIS system could somehow be housed within the MDA COI.

> "So we all trudge out to Colorado Springs and we go to some contractor's office and all the suits are there -- they smell money in the water. But what they hear is, 'We have no money. There's no funding for this. This is all sweat equity. What we need are some working groups – one for data management, one a pilot working group, and one called Joint Services and Implementation. Here's a sign-up roster. Anybody who is interested in signing up, here it is: let's get to work.' There are about one hundred and twenty five people in the morning session. By the afternoon session, there were fifty, and on the sign-up sheets, there were ten. The contractors and the working capital fund organizations are looking for money. When there's no money, they're like, "Goodbye.'"

The financing stratagem was in fact purposeful, and one of several guiding principles that Krieger observed in establishing COIs.

First, the participants should pay their own way – they were gaining value and should pay to acquire it. "My theory," related Krieger, "is that doing this does not require a lot of resources, and we should not earmark resources. I am not giving anyone money."

As they would ordinarily pay to establish a new point-to-point connection for any new user coming onto their networks, instead they would pay to publish and advertise their data. "That is one of our selling points," Krieger said. "We are spending your money by making you show your data. I do not want to give you money. I want you to re-spend the way that you are doing things."

Which they did. "The total cost is about a million dollars," Krieger related. "I actually took some CIO money and paid the Department of Transportation, because it was a good target and they said they did not have any money to publish. But the Coast Guard paid to publish and advertise their data, the Navy paid to do theirs, and ONI paid to do theirs. NORTHCOM contributed resources for the Navy to serve as the COI project manager. We were in business."

"We basically had the major programs that held the data build up the web services interfaces as part of their program, "recalled Frank Petroski. "The usual way to do this is

you just have some side group go off and build the interface one-off, but that cannot be sustainable. In this case, we actually had to lean back on the program managers to commit some resources to make this happen. But really, it's just a couple of hundred thousand dollars, and just an issue of moving that up on the priority list."

Nimmich saw the problem as actually far more difficult, and as a job for the executive sponsor. "Money is always a challenge, and when that's the case, you have to set an example and put your money where your mouth is. Starting late in the Federal fiscal year," he said, "people are looking to dump money rather than lose it. But we started in the January or February timeframe, and it was much harder to convince people at that point in the calendar to give up funds. I had some resources that I could reprogram, which I did. It helps convince people that this is the right place to invest their money as well."

Krieger's second mantra was: "This is not hard." Each agency knew how to establish point-to-point connections to its proprietary databases. It was easy to add a server outside, and it was easy to push the data to the outside server – in the agreed-upon vocabulary of the community. Publishing the service on the Internet, making it discoverable, advertising it, letting people subscribe to it as a web service was well know technology. "It is very easy using XML to wrap the data and publish it as a web service," observed Krieger. It turns out not to be hard."

A third mantra was, "Leverage and reuse existing capability and infrastructure." In fact, most of the "publish" and "subscribe" infrastructure and know-how was already in place and available in the DoD IT enterprise, as the Net-Centric Enterprise Services program Early Capability Baseline (ECB) Federated Search, security and messaging services.

Frank Petroski explained. "There were a number of enterprise capabilities that people could just write on top of -- an existing DISA enterprise service bus on the net that was an enterprise resource they could just plug right into. It did not have to be procured from scratch – bought, installed, or trained on."

A fourth mantra was to advance the overall net-centric capability of the Navy. "We were not supposed to go out and build new capabilities," Krieger observed. Utilizing the NCES program ECB services was the core of the net-centric strategy and would need to be featured in any build.

Fifth, "Leave a trail behind showing the way." The MDA COI initiative should demonstrate reusable steps and technologies, document them, and leave them in place for further development and use.

Sixth, fly with authorization but below bureaucracy. The fact that it was low cost and a non-acquisition program would let the service development fly somewhat under the typical oversight radar and move quickly. Krieger in fact positioned this as "risk mitigation for acquisition programs," further softening its profile. "Once we put the capability in," he said, "we're going to leave the capability under an interim authority to operate as we formally get it certified and accredit it with full authority."

Seventh, partner with a community, create ownership as early as possible, spin off, and move on. "My goal is to get this thing started, be their wingman, and then back out of it and monitor it," said Krieger." I don't want the credit. I want to be behind the scenes pushing, making sure they're doing it the right way. But I want them to get all the credit within DoD."

The MDA COI ratified the problem assessment, and authorized operations with the goal of delivering a service on the Internet nine months later, in October. "There were plenty of skeptics," Krieger recalled. "People out of their comfort zone. But I drove it hard, and it was well-supported by the two Admirals. They came up with a plan, and said, basically, 'Let's go do it.'"

The Political Challenges

Nimmich might add an eighth mantra: show how the innovation solves the problems of potential investors. "Start out with understanding what the other services interests are and how this addresses them," he advised.

In this instance, the Navy was wary of MDA investment as it appeared to be weighted to benefit the "domestic" side, covering the coast lines, rather than to benefit the Navy mission, or "the away game". And it would certainly not build new ships or planes, which was the Navy priority. "All they could see here initially," one observer said, "was at the end of the day a bill that did not necessarily answer their mail."

By keeping the up-front investment small, however, the bar to involvement was lowered.

For her part, Rear Admiral Nancy Brown helped pursue the Navy's broad interests, wrap them in the banner of collaboration, and secure the Navy's share of financial investment. "Navy folks were very anxious to participate," she recalled. "They saw the COI effort as a way to leverage additional resources to do some things they might not be able to do on their own. The Coast Guard had a pretty robust database of information about merchant and commercial shipping. The Navy did not have access to that. By joining the COI, they would – and faster and more easily than had they had to figure it out on their own. We did not even know what was in their database until the Colorado meeting."

Even so, the idea of collaboration rankled some. “Why don’t we just do this ourselves?” one commander in the audience asked in sidebar. Admiral Brown was seen to turn around and reply, “Because this is a shared effort and that’s how it will be.”

“Yes, Ma’am,” came the answer, and that door was shut.

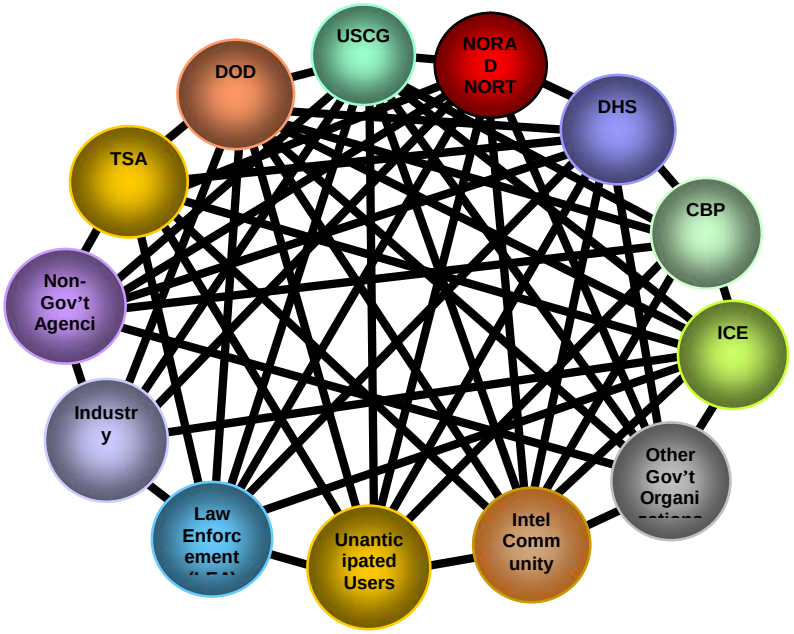
But the stakes were still high, as much would have to be proved – that this system could address the Navy’s global information challenge -- before any further investment could be contemplated.

The Technical Challenges

“It turns out the web services technology is relatively straightforward,” Frank Petroski observed. “In all of the times we have done this that part has not been hard. The technology is pretty straightforward. There are a lot of folks around who understand it. It is very easy to find them and get them on the project.”

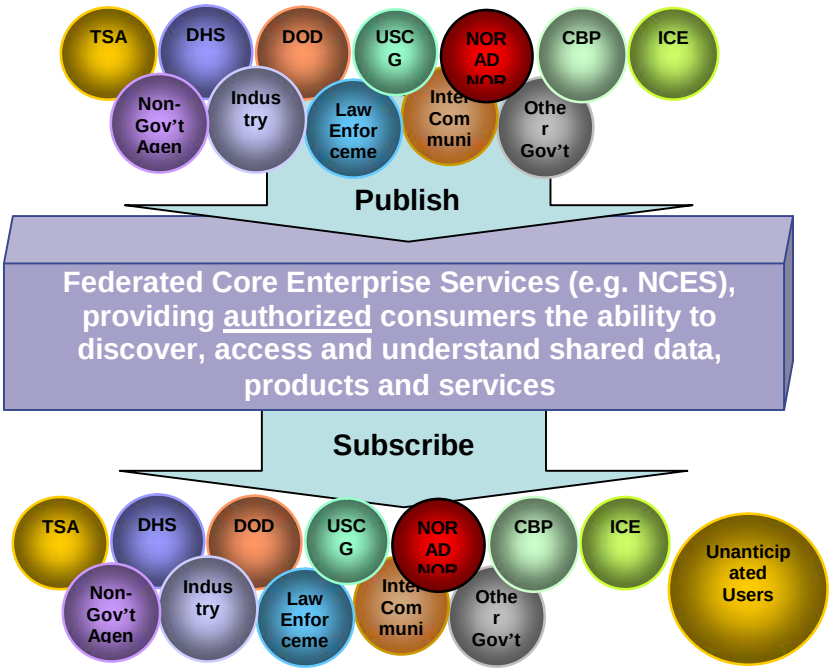
What was hard was breaking the old habit of doing point-to-point any time a new user came on, and data owners’ “discomfort” with just publishing the data and having people subscribe to. Mike Krieger explained:

> “That is the way we have done it for years. Whenever we want to share data we identify the two users, right? We come up with a proprietary away to do it, pay a system integrator to do another proprietary point to point –- the best example of that is the common operational picture (COP) of the GCCS system. It has something like a hundred and fifty point-to-points. As soon as we publish one point-to-point somebody else decides they need the data and yet ***another*** point to point. It is the “n-squared” problem. And for every point-to-point there is another translation required of the enterprise, which is how we get killed financially, because we always ***have*** to translate, and we never resource the translation or the management of the translator. Our theory, here, was: ‘Let us avoid the n-square problem altogether by agreeing on a common vocabulary and publishing the data and making it discoverable.”



Then N-Square Problem of Point-to-Point

To address the N-Square problem, the doctrine of net centricity proposed a different schema – one that would use a core enterprise services like the NCES ECB services to give authorized users the ability to discover, access and understand shared data, products and services. It would purposefully decouple data from providers and make data available to consumers, to increase agility, extensibility, and responsiveness.



Frank Petroski explained. "The beauty is going forward. I can now add a data source by modifying it to publish in the community vocabulary (I have to add only one new interface). In the new approach, all existing subscribers can now see and use the new data. In the old way, as I add more systems and displays, I have the n-squared problem of interfaces. Operations research describes this as reducing the problem from O(N**2) to O(N)."

Acceptance

But decoupling data created issues for the owners of the data. One of the cardinal rules of data sharing in the intelligence environment, for example, is "use no data without the owner's consent." The same challenge would apply to MDA COI – even for corporate suppliers of shipping data.

"All shipping companies have and use AIS," John Macaluso explained. "They know where their ships are at any given minute. That's unclassified information, but its competition-sensitive information. So while they might like to share with the Federal government, they don't want to share with their competitors, because firms are operating on thin margins and every little bit of information helps."

"So when we say to a shipping company, 'Give us all the up-to-the-minute location of all your vessels worldwide,'" Macaluso observed, 'They want assurance that that data would be handled properly."

Security and access – for both classified and unclassified data – would be a major issue to address.

Certification and Accreditation

The touted virtue of net centricity was its extensibility – rather than being locked and fixed into a bevy of expensive point-to-point connections, it could accommodate virtually limitless numbers of unanticipated users. These might be users, for example, who came forward in the midst of a crisis to search for data they'd never needed before. "Your point-to-point systems will give you the information you know you need to have," Macaluso observed. "In a crisis situation, you have unanticipated data needs, and you can't search on information that you didn't know you needed ahead of time."

Net-centricity promised that at any time authorized unanticipated users could subscribe to the service. But this ran counter to current methods to "accredit" systems for service. Federal requirements mandated that new systems be "certified" before they could be integrated into existing ones, so that access control – who is seeing data, and where it is going -- is clearly understood and defined. Systems accreditation is classically based on the highly controlled access that point-to-point connections confer. The process is long, but point-to-point connections in fact facilitate it.

Net centricity throws a wrench in the works. Macaluso could hear the push back even now. "Someone comes selling net centricity to a watch center, and they will hear, 'Hey, great, but you've got to make sure that when I integrate your capability into my watch floor that I don't blow my own certification and accreditation and have to start over."

"One advantage of point-to-point is that data protection is well understood," related Macaluso. "On the other hand, when you put your data out on an enterprise service bus, you expose it to unanticipated authorized users. Although this is exactly what you *want* with net-centricity, it's also what you *get*. It makes publishers nervous unless you can give them assurances that their data will only be seen by users with the proper credentials."

Vocabulary

The hard part too, was reconciling diverse naming conventions used by multiple systems and interfaces to multiple "clients". Frank Petroski explained by way of example. "The Navy has a system that they use for situational awareness that publishes in a legacy format. But they can't publish more broadly – to more

users -- in their own format. The Coast Guard is using a client that was built by the Air Force that consumes data in a different format. So both the Navy and the Coast Guard have really nice tools with a lot of port information, for example, that they consume and publish, but only in their own formats."

"The real challenge here," said Petroski "tends to be the social challenge of agreeing on the vocabulary. The key is simplicity – we agree on the idea of "vessel" and avoid going too deep on "sub-types". Once you get the common vocabulary, the rest of the benefits accrue pretty quickly."[6] But the MDA COI would need to reconcile the multiple data bases of its partners and arrive at a series of common naming conventions.

The MDA COI authorized a go forward effort, named John Shea as project manager, and established three teams – data management, pilot development, and implementation – to address five challenges facing the community:

> *First*, agree to a common business process and information exchange vocabulary that described it.
>
> *Second,* figure out the interfaces from individual databases to a common enterprise "bus" so that the data, once normalized across business processes and vocabularies, could become available via the enterprise "bus"
>
> *Third*, publish the data off the bus so that users around the world could "subscribe" to the service
>
> *Fourth*, give access where authorized and appropriate
>
> *Fifth*, make it available in formats that subscribers could use.

The data management group delivered a common vocabulary and schema within the agreed-upon 60 days. But the problem was still huge. How best to scope it down to something manageable, provable and valuable?

---

[6] The classic in-industry joke that is told to illustrate the potential confusion of different meanings for like terms, and the importance of agreeing on a common vocabulary: "Secure the Building!" What does it mean?

- Navy: "Turn off the lights and lock the doors."
- Army: "Surround the building, occupy, and control entry."
- Marines: "Call in close air support, assault with small team, neutralize occupants, fortify and hold at all costs until properly relieved. SEMPER FI!" and…
- Air Force: "Take out a three-year lease with option to buy."

As technical director for the Navy's C4I effort, Shea was already under way implementing the militarized version of AIS requested of C4I by the Chief of Naval Operations.

"As technical director I get inundated with articles and mandates and initiatives on net centricity and the God's work that this has been doing, trying to roll out Net Centric Enterprise Services," Shea recalled. "And up pops this formation of the MDA data sharing community of interest."

If this worked, it might save Shea a lot of time and trouble. "We were the low hanging fruit sensor that could be used to exploit an MDA case for data sharing," explained Shea. He was blunt. "I signed up for this for the simple reason that I wanted to find out if DISA's NCES, the huge monolithic promise of net centricity of the future, was the real deal, or a bunch of bull."

"Spiral One [the first phase of MDA]", Shea observed, "went right to the heart of the matter of NCES. Could I discover the existence of data by using federated search, and could I then access and understand what I just discovered? These are the basic principles of DoD directive 8320.2, and its companion 87320.2G, the implementation guide."

Shea thought about the problem. "I was given some thirteen year old kids with four hundred pound brains to help me on this and I'm a guy in my early sixties who has had lots of failure in my life, so I can usually determine what works and what doesn't," Shea said. "We decided, 'Ok, what's going to be our baseline use cases here?"[7]

Shea's group decided on two, one for "discovery", and one for "access and understand", and they were unusual in their simplicity. "In net centricity you don't have to have a complicated kind of operational use case which typically drives out contradictions," Shea explained. "What you really want is real black and white use case."

He explained "discovery".

"You have, first of all," he said, "a data provider. Let us take the case of the US Coast Guard. They have an internal representation of their data – in other words, they

[7] In software engineering and systems engineering, a **use case** is a technique for capturing functional requirements of systems and systems-of-systems. According to Bittner and Spence, "Use cases, stated simply, allow description of sequences of events that, taken together, lead to a system doing something useful" [1]. Each use case provides one or more **scenarios** that convey how the system should interact with the users called **actors** to achieve a specific business goal or function. Use case actors may be end users or other systems. Use cases typically avoid technical jargon, preferring instead the language of the end user or *domain expert*. (www.wikipedia.org)

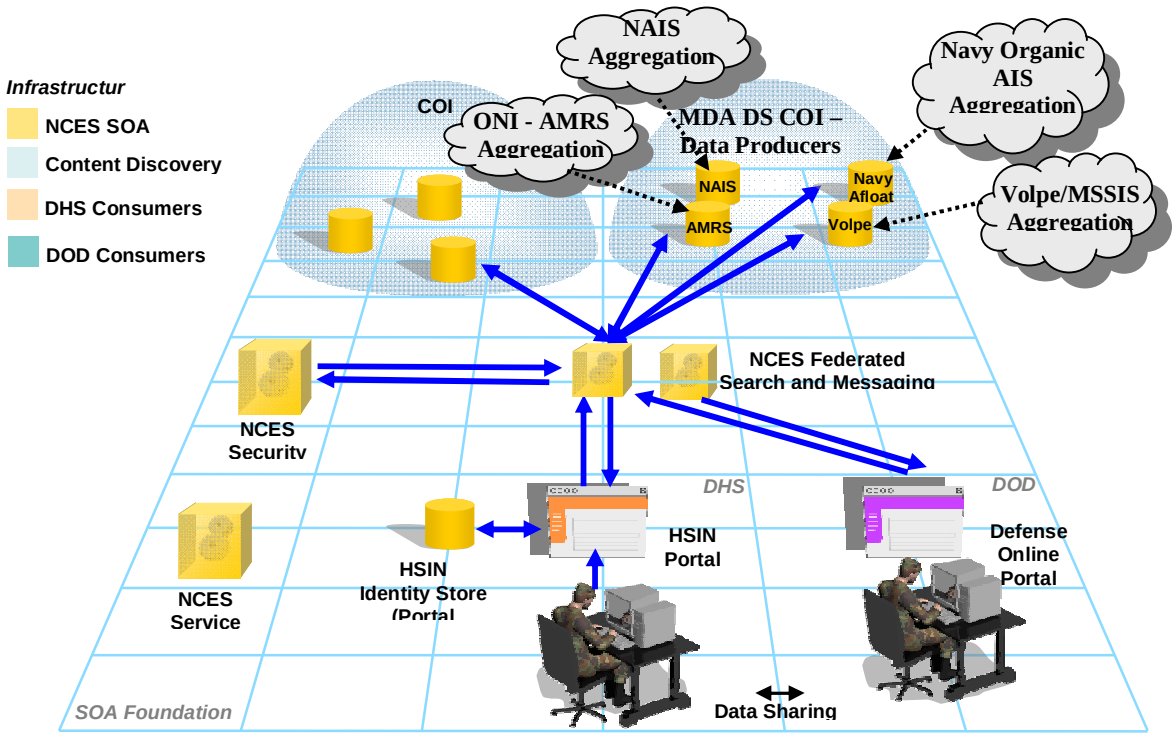
store it, maintain it, manipulate it in a certain way. What we wanted them to do was to create an external representation of that data mapped to a community of interest vocabulary, create a metadata representation of it, and publish that metadata in a catalogue. When we searched for the metadata over the NCES Federated Search and Messaging Service, we wanted to learn, could we find it? Yes, or no? That was 'discovery.'"

The second use case was for "access and understand."

"If I'm a consumer, and I want to find the existence of, say, AIS data, I likely have a viewing platform that I use. Maybe its Google Earth, or IMAP, which is the Homeland Security enterprise viewer. Could we write a translation of our vocabulary into the commonly used viewing platforms? Again," said Shea, "an extremely bounded problem, simple in the extreme. Either we can view the data in our viewers, or we can't."

For the purposes of the use case, driving the community agreement on the vocabulary would be critical. It was scaled for speedy resolution. Four data providers had to agree, for example, on a common definition of "vessel" – and do it with within two months.

> Early on we said, 'We really need a community vocabulary and schema.' We knew the guys over in the data management working group and we said, "Hey, for us to be successful in this thing, you need to deliver to us by the 17th of May a working, no "bull" schema that we can run with." And they said, "OK." And I said, 'The problem set is vessel as a conveyance.' You've got to describe that. We're not worried about cargo, we're not worried about people, the Navy's job is really to build superior knowledge about vessels. And so they went off and did their thing. What we gave them was our use cases in a schematic that they could understand, you know, a cartoon that they could understand and apply to their work.



"In complex vocabulary builds," Frank Petroski of MITRE explained, "you end up trying to get to a place where you can compromise – getting to the common places that achieve the most interoperability, without trying to get every last detail out. There are always arguments aimed at making their side of the implementation easier – making the schema look as much like their existing data set as possible -- not necessarily what is best at the enterprise level."

In this instance, however, simplicity worked well. "We were trying to come up with a scheme that is as simple as possible –simple in the extreme. For us, the question was, how do you define what a vessel is and report on the classic elements of position, time, and various attributes for the purposes of the use case?" The work accelerated further as such concepts were well-defined by previous international standards bodies and UN classifications.

The data management working group turned over the vocabulary and the schema in mid-May 2006, as promised. Shea's developers went to work to prove out the use cases. They elected to publish to channels tied to geographical areas of interest, rather than to catalogues, as a better way to offer the data.

By June 2006, developers were ready to demonstrate to Shea proof of the first use case, "discovery." "I was in San Diego and we were doing a telecom," he recalled. "The

team was over in Roslyn. We went to the DISA GES portal, accessed federated search, and typed in the word "MDA". After a couple of seconds, it came back with the metadata that we had constructed to expose the US Coast Guard. "Holy ***," he exclaimed, "that's what I want!"

Work proceeded. By October, Shea was ready to give a preliminary demonstration that proved both use cases. By December, the proof was ready for the highest levels of the Navy and Coast Guard.

"Naval officers are used to working the command and control tools called GCCS-M – Global Command and Control System - Maritime. It's very cryptic and sparse on information. What we showed them using Google maps as a platform were new points of data which they'd never seen before on GCCS-M. We showed a display from Singapore harbor taken from an onboard US Navy AIS sensor. On its own, it showed 500 tracks [ships]. With the new IS data being organically collected and injected into the mix, it went to 1500 tracks."

"That," said Nimmich "was a watershed event."

"Remember," said Shea, "what a ship driver wants. What the ship driver is definitely afraid of is the things that he doesn't know. He wants information. What surrounds me? What kinds of ships? Oh there's a liquid natural gas ship coming by or there's a ship loaded with sulfites, or, a ship that's on the "bad ship" list -- all that information wasn't available to them on a timely basis or at all prior to AIS coming on their ships. And even with AIS, without integration, they couldn't see it. This way, its' published back to NCES ECB services, and shared to all other people who have authorization to look at it. If I'm a ship a hundred miles away, I can see what's going on. Any one ship's information would only stay on the ship. We showed them a way of not only enhancing the information of situational awareness, but how to share that situational awareness with the world."

"This helps me," Vice Admiral Mark J. Edwards told Nimmich. Edwards was Deputy Chief of Naval Operations for Communication Networks. "It's what I have been trying to get to. This can give me a netted Navy."

Edwards was heard to ask Vice Admiral Robert Papp, Coast Guard Chief of Staff, "Is the Coast Guard interested in this?" Papp's reply was, "Vitally interested."

As the Admirals left the room, Shea lingered. An uncertain future lay ahead. With new offers of financing on the table, how would this scale as it moved to production models? What issues of reliability would arise? How would security and access be addressed in a hybrid system that combined sensitive national intelligence, competition-sensitive data, and otherwise unclassified data? With new data streaming in, how would

information "overload" be managed? As it moved from a single COI to global reach, from lab bench to the field, how would it be governed, and by whom?

"When you look at the number of vessels that are out there," Admiral Nancy Brown observed, "it will overwhelm anybody. The real purpose of maritime domain awareness is to gain an understanding among all the ships, crews and cargos of who out there from among the 99% of commercial folks doing business with no intent to harm or injure anybody, is suspicious – whose signature doesn't match where they say they're supposed to be and where AIS says the are? The Coast Guard is concerned about that when you come into port. The Navy is concerned about that on the high seas. That's the information we all need to know."