

The Many Faces of Collaboration Interoperability

Diane Boettcher

Director of Knowledge Management, SRA, International

diane_boettcher@sra.com

Abstract

Collaboration interoperability has many technical challenges, but these are only one aspect of true interoperability. If we are to reach the goals of Network Centric Warfare, we must address all of the various faces of interoperability. The people, processes and technology offer a diverse, interdependent set of challenges, all of which impact our ability to successfully collaborate in a robust online environment. The challenges range from a diverse user group, to major cultural barriers and from security procedures to simple data interoperability. The technical challenges should not be minimized, with areas of standards compliance and cross-domain solutions having the greatest potential. Many of these problems are not new, but simply look new. These challenges will require training in the new processes. Other challenges will require a change in attitude and culture to properly address.

1. Introduction

The Department of Defense (DoD) has been struggling with online collaboration tool interoperability since the late 1990s. Nearly as soon as these tools were introduced into the warfighting environment, their lack of interoperability has caused consternation and difficulty [1]. Action officers and watch officers alike often require at least five different tools to reach all of the commands and people with whom they need to collaborate. The Information Technology departments must work to maintain all of these tools; some of which require conflicting browser or network settings.

Several attempts have been made to address this challenge, starting in 1999. Working groups have been formed, contracts have been issued, and standards have been explored. All of these efforts have met only minimal success. And while the technical challenges remain, other interoperability challenges remain largely unaddressed.

True, robust collaboration has many aspects of interoperability. The challenges surrounding the people and process issues are as important, and are potentially more difficult than the technical issues. This paper will examine the often overlapping, inter-related issues and make recommendations for their resolution.

2. People issues

Collaboration is ultimately a human endeavor. Data exchange accomplished by machines is important and necessary to Net-Centric Warfare, as identified in the 1990s [2]. Such exchanges, however, are not fundamentally collaboration. Collaboration requires people to be involved in the process. While many definitions of collaboration exist, all definitions speak to multiple users working together to create a product. Without a product, the interaction is simply a conversation. The product might be a white paper, a briefing, a decision or increased shared awareness of the situation. Without more than one person, the event is simply work.

2.1. Familiarization and training

People inherently dislike and seek to avoid change. More than most, busy people are reluctant to move beyond their tried and true methods of getting the job done. The staffs at the Regional and Functional Combatant Commands, such as Special Operations Command and Central Command, are some of the busiest. They are, quite literally, in the midst of war. As we move closer to the fight, down to the tactical levels of war, the people are nearly overwhelmed. The tactical warfighters are therefore less willing to try new things, new collaboration tools or new processes. Any new method or process must solve a problem that is causing immediate pain and trouble.

This is not to imply that our combat troops are not innovative. Quite to the contrary, we have some of the most intelligent and creative people in the

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 21 MAY 2008		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE The Many Faces of Collaboration Interoperability				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) SRA, International				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES AFCEA-GMU C4I Center Symposium "Critical Issues In C4I" 20-21 May 2008, George Mason University, Fairfax, Virginia Campus, The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 30	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

world working for and with the DoD. However, they understand the potential cost of failure of new methods. Any new tool or process must not only improve their situation, but must do so by a factor that overcomes the cost of training and lack of familiarity. As much as the warfighter would appreciate using only one tool to collaborate, if she is forced to learn a new tool or new process, she is unlikely to move from what has proven successful in the past.

The use of collaboration tools has not yet made it into the schoolhouses of most of our military. While some collaborative tools are in use, such as Command Post of the Future (CPOF), few courses focus on effective online collaboration. Tactical Training Group, Pacific, does include fairly extensive coverage of chat rooms, naming conventions, chat protocol and room use in their work-ups. This training focus remains sadly missing in most courses. So our Sailors, Marines, Airmen, Soldiers and Coast Guardsmen enter the warfighting staffs, rotate into country or arrive on station with widely varying degrees of familiarity and skill in the tools that are provided. If they encounter difficulty in using robust online collaborative tools, they will fall back on what they know – the phone, e-mail and Video Teleconferences (VTCs).

The wide diversity of familiarity comes from the diverse background of military members. A mobilized Navy Reservist may fly planes for a living and never use a computer, not even at home. Alternatively, an infantryman may have built a Linux lab in his basement. Demographically, about 65% of the active duty force is under the age of 26. Many of our young recruits can be considered Digital Natives, but many may also come from the other side of the Digital Divide. Those on the downside of the digital divide often don't have computers in their high schools and are growing up in the half of American homes that do not have broadband access.

While it isn't always about the technology, it's important to note that no one in these groups has a high tolerance for technical difficulties with their collaborative tools. Those who understand the technology expect their tools at work to run as easily and seamlessly as Google and Skype. They regularly IM, text and Skype their friends and family. They have no concerns about institutional firewalls or network configuration management. When they want to update their software version, they go to the vendor's site, download and install the latest and greatest capabilities. They don't worry about a Preferred Products List or certification on their home

networks. Those who are not familiar with the technology do not have the patience or understanding to troubleshoot even the smallest of problems. If the technology doesn't work the first time they try it, then it doesn't work and they are moving on to the next option. Their memories will be long on this topic. Any introduction of a new system will have one opportunity to succeed. Initial failure will leave a bad taste in the warfighter's mouth and they will be unwilling to allow their time and energies to be diverted for a second try.

If we are to overcome these challenges, we need to institute training in collaboration tools and processes at all levels and schoolhouses. Basic training might include how to use instant messaging (IM). As noted above, for many recruits, this exposure is likely to be redundant, but it will serve to level the playing field to some common ground. Training in what tools are sanctioned on the network and available is needed for all. As a military member progresses through his career, we might expect to introduce the person to more robust forms of collaboration. Classes in use of imagery and maps might include modules on how to share such material in a collaborative session. While the specific tools will almost certainly change over time, the underlying processes will remain fundamentally unchanged. Training in these processes will be instrumental in overcoming the familiarization challenges.

2.2. Generations

The impact of having Digital Natives on the force was mentioned briefly above. These personnel, born since about 1982, exhibit a comfort level with technology that is unparalleled by the Digital Immigrants [3]. A digital native is likely to refer to their "new camera," whereas an immigrant would refer to their "new digital camera." Their comfort level with the tools will lead them to demand more and better technology to support their work. And it doesn't stop there.

A digital native is extremely comfortable in a collaborative environment. Rather than growing up with bound books of knowledge on the shelves called encyclopedias, they grew up with Wikipedia, a dynamic, evolving body of knowledge to which they have been encouraged to contribute. When the first televised debate aired in 1960, the newscaster controlled the questions to candidates Kennedy and Nixon. In 2007, digital natives blogged on their Facebook profile that their YouTube submissions had been accepted by CNN in the presidential primary

debates. They place bets regarding who will say what on predictive market Web sites like Hubdub.

They expect meetings to be conversations. They expect that their input will be sought after and valued. These expectations will have a profound impact on their participation in collaboration sessions. In 2000, when I would discuss the power of this new technology, I noted that anyone in the meeting could draw on the whiteboard. Many senior officers expressed concern that anyone in the meeting would be permitted such power. They worried that the more junior members of their staffs would say or do inappropriate things. Such fears are understandable if one has grown up in a strict hierarchical structure. Experience has shown that these concerns are generally unfounded. The military members are typically professionals who are looking to get their job done. After all, every Sailor knows the Chief of Naval Operations' email address. Few use it to jump the chain of command. For many years, nearly anyone has had access to the radio net and continue to exercise proper radio discipline.

Nonetheless, senior and junior members of staffs and organizations will have to come to terms with the collaborative cultural environment that the collaborative technical environment brings. Policy, of course, is the obvious answer along with training. Just as we have instituted policy to ensure that Web and e-mail use are in keeping with DoD core values [4], so we can expect that collaborative sessions will be subject to those some values.

However, acceptance of the Brave New World is the avenue likely to bring to the most benefit. We have power and wisdom in our military that, unfortunately, goes untapped. Allowing junior members to contribute may just be what we need to move forward as a smaller, more agile and adaptive force.

2.3. Language

Language impacts interoperability on a number of levels. Certainly in a coalition environment, we often see that those members who are native English speakers (when English is the language of the coalition, as it in Afghanistan and Iraq) dominate the staffs. Of course, this is also true of other languages when a command staff routinely speaks another language. Since the United States no longer fights or wins alone (if, indeed, we ever did), the reality of coalition planning and the requisite language translation should be built into the collaboration tools [5]. Even our Canadian brethren often are native

French speakers who have difficulty understanding our Texans. Most translation engines, including those developed by or for military use, expose their services so that they may be consumed by nearly any technology. However, to date, only a few collaborative tools have embedded language translation services.

Another, more interesting challenge has emerged in the use of IM slang in online collaboration tools. Those digital natives familiar with the tool have brought their language with them as they joined the military. Examples include the more familiar fyi (for your information) to the fairly pedestrian brb (be right back) and ttyl (talk to you later), to the difficult afaik (as far as I know). See Table 1 for more examples. IM slang can be elaborate and subsequently confusing for the uninitiated [6].

In a face-to-face meeting, a person with good public speaking skills can dominate a meeting. In an online collaborative session, a fast typist who knows her slang can dominate. This language and skill barrier may prevent senior military members from fully embracing online collaboration. The VTC is often their preferred collaboration tool. The interface requires no technical expertise by the user, they can maintain control through their physical presence as well as avoid the onslaught of confusing acronyms.

Table 1. Some common IM shorthand.

Acronym	Meaning
AFAIK	As far as I know
CYE	Check your e-mail
FWIW	For what it's worth
GR8	Great
H/O	Hold on
HTH	Hope this helps
NRN	No reply necessary
SP?	Spelling?
TIA	Thanks in advance
W8	Wait

Once again, training will be critical. We should train and establish a useful set of IM acronyms from the civilian world, as well as embrace those already being used in the military collaboration circles (i.e., lc for load and clear). We have practiced radio discipline for years, and need only to take those lessons and apply them to the newer technology to realize success.

2.4 Culture

Most proponents of online collaboration agree that cultural barriers are the most daunting [7]. In the military context, we combine a hierarchical structure with an inculcation of secrecy and need-to-know. Some individuals believe that knowledge is power and they don't wish to share it. Others simply wish to shield seniors and subordinates from unnecessary or confusing information.

These structures exist for good reason and have been proven effective for hundreds of years. However, as the current Vice Chairman of the Joint Chiefs of Staff, General James Cartwright has noted, the chain of information is not the same as the chain of command [8]. Commands flow from the commanders to their forces. Information must flow up, down, around and through an organization. This horizontal flow of information is a fundamental change and is therefore scary. Rather famously, General Cartwright established an event log at Strategic Command while in command. The log became rather like a blog, with General Cartwright asking questions and expecting answers from all quarters. The system is not universally popular. Blog responses are still occasionally subject to the same staffing process that a more formal message might endure [8].

While some areas of the military are embracing this new method of communication and increased collaboration, many would prefer to remain in their enclaves. These commands and communities may permit internal collaboration, but often stop short of permitting others visibility into their planning processes. They fear that if higher headquarters were to become too involved, that micro-management would result. This fear may be amplified in a multi-national environment with differing doctrines and differing philosophies of warfare are in use.

This risk is not unfounded. The increased visibility provided by collaborative tools can bring increased oversight and may lead to micromanagement of the battlespace [9]. Commanders must remember that their subordinate commanders can be trusted and that their attention is best focused on issues at their level. This challenge is truly unique to the information age and must be addressed by command and control training.

3. Process and policy issues

Large organizations require formal processes and the DoD is no exception. We have processes at all

levels. Some of these are expressed in instructions, others in policy documents, and still others are embedded in our service and command cultures. Most, if not all, of these processes assume that organizations will act as independent entities without a great deal of collaboration interoperability among them. The DoD values the independence of the warfighting commander as the most sacred of cows. In particular, the Navy vests a great deal of authority and responsibility in their commanders. All commands, services and agencies permit commands latitude in the implementation of regulation and process. This latitude is incredibly important in a dynamic and adapting landscape that is a battlefield. However, such dispersal of responsibility can impede true interoperability.

3.1. Trust

Server federation will be required if we are to achieve collaboration interoperability across the DoD. But a simple issue of trust may get in the way.

A few years ago, the Army and the Navy both implemented the same IM software for their respective portals. The same vendor provided the same client software and identical server software. Technically, federation of these servers was a rather simple task and would allow a level of Joint IM interoperability. And yet, the policy issues to permit the interoperability took well over a year to resolve. The services had implemented different standards for account establishment. The trust model simply failed. Because of process differences, the Army might trust Alice, but that didn't mean that the Navy would trust her as well.

We also face a trust issue when we must collaborate with members of industry, academia, state and local law enforcement. Just as we do not fight with our coalition partners, we also do not fight without our industry and academic partners.

In the realm of humanitarian assistance and disaster relief (HA/DR), we must coordinate with other governments and non-governmental organizations (NGOs) [10]. Some of these organizations do not wish to be seen as working too closely with the military. Many NGOs work to alleviate suffering without regard for politics and therefore must avoid being too closely affiliated with any particular government. It is quite literally a matter of life and death for some of these personnel. Doctors Without Borders/Médecins Sans Frontières (MSF), for example, is adamantly independent.

At home, we can expect the Department of Homeland Security to take the lead in any HA/DR event. But while not in the lead, the DoD often brings the most people and equipment during any response. By the sheer magnitude of the DoD's participation, we may expect DoD tools and processes to dominate, at least initially. It will likely be the DoD's communication gear and collaborative tools that will be the primary means of communication in the resultant ad-hoc networks.

This trust issue has obvious ties to the technical issues of identity management. Those issues are well-known and will not be addressed here.

3.2 Security

Traditionally, we have always permitted commands to be more secure than policy dictated. The ports and protocols listing provides recommendations only. However, many collaborative tools require specific ports to be open on firewalls to successfully collaborate. Since nearly any base, post, station or command can choose to be more secure by shutting down ports, the collaboration interoperability can be fragile. Many tools have reacted to this possible restriction by bundling their data and protocols, and using ports 80 and 443. These ports are used by the Web and are never blocked, even by the most zealous of firewall administrators. This solution works for the short term, but does set us up for new challenges in the future as we try to implement Quality of Service on these services. Bundling services makes them indistinguishable as voice and video streams that might merit higher QOS. Additionally, we're not able to screen the data in bundled services, making any potential cross-domain filter nearly impossible to implement.

While security is truly important, we must always balance that need with the operational need. Establishing a required-to-be-permitted section of the ports and protocol listing would enable collaboration across the enterprise. Obviously, this action would require a shift in policy as well, with the dictator of security settings and hence responsible for the risk to the network. Fortunately, the Joint Task Force - Global Network Operations is well-positioned to evaluate the risks involved and require compliance with such mandates.

3.3 Data

Data interoperability is a complex problem and potentially highly technical challenge. The impacts of

data on collaboration interoperability primarily involve discovery issues. In order to successfully collaborate, we must discover the people with whom or places where the collaboration is occurring. Very often, we are working in countries that do not share our alphabet. When we discuss place or people names, we must ensure that we are sharing a common vocabulary. For example, two provinces in Afghanistan are named Paktia and Paktika. They are physically close to each other as well. Similarly, Uruzgon province can be spelled "Oruzgon" or "Uruzgun." These alternate spellings create confusion not only in discussions about them, but when sorting through a lengthy list of potential meeting times or Web site URLs.

3.4 Tactics, Techniques and Procedures (TTPs)

Traditionally, tactics, techniques and procedures (TTPs) are implemented at a unit or command level. These instructions are a way of codifying best practices and lessons learned without the lengthy process of changing doctrine. Also, they tend to be of minimal importance of whether something is done in one manner or other, just that everyone does it in the same manner. For example, it's unimportant whether an email address is `firstname.lastname@` or `lastname.firstname@`. That an organization would choose to do it one way for everyone provides ease of use. Doing it the other way would have minimal impact.

With collaboration tools now being provided to the enterprise through NCES, some of TTPs should be brought to the enterprise level.

During military operations, only rarely do people actually care about the name of the person with whom they are speaking. Position is more important and enduring in battle than personality. We have instituted this for years with radios. An Army commander, for example, might be called "Danger 6." When anyone in the 1st Infantry Division hears that call sign on the net, they can be assured that they're talking to the Division Commander of the Big Red One. Nearly everyone in the Army knows this. If the commander was lost in battle, his second would pick up the call sign along with the command. Similarly, the Navy will call the Commanding Officer of a ship by the ship's name ("ENTERPRISE, arriving").

Radio calls have always been bound by the physical length of Radio Frequency (RF) waves. While they can support collaboration, radios do not

extend collaboration beyond the battlefield. Joint interoperability of collaboration will bring a broader variety of warfighters into the collaborative environment. This extended reach will require joint procedures and conventions.

Currently, collaboration participants are often allowed to identify themselves without any guidance as to how they should do so. Alternative, the system may provide a display name that is equivalent to their log-in identification. Often, this causes the list of members to be sorted quite unhelpfully by the participant's first name. Codifying a radio-like identification at the enterprise level helps us answer the most basic question - who am I talking to?

Table 2. A few potential names for a sailor.

John Paul Jones
Jones, John
CAPT Jones
Captain J. P. Jones, USN
Jones (Captain, United States Navy)
CO, <i>Bonhomme Richard</i>
BONHOMME RICHARD
BHR
N00, BHR
BONHOMME RICHARD, CO, CAPT J. Jones, USA

In August 2007, the Collaboration Interoperability Working Group (CIWG), a group chartered by the Military Communications Executive Board, addressed this very issue of naming conventions for participants. This recommendation should be published as a TTP by the Joint Staff and, if possible, codified into the collaboration tools currently in use.

The recommendation was to include, as a minimum, the following information in the display name:

- Country of service trigraph
- Organization
- Duty position/title
- Type: rank/pay grade/contractor
- Last name
- First initial

The preferred display name of our Sailor in Table 2 would then be "BONHOMME RICHARD, CO, CAPT J. Jones, USA" [11].

Of course, we must also consider that most people belong to many organizations. Captain Jones belongs not only to his ship, but to a particular strike force, perhaps to a particular Joint Task Force, his Navy and his country. In a multi-national meeting, he might be representing the United States or he might

be representing all maritime forces. Clearly, one display name will not suffice to allow him to represent all of his roles.

TTPs should also be developed that address room naming conventions. When collaboration occurs on separate servers and the tools are not interoperable, we don't need enterprise TTPs. The "J6 Morning Brief" on the Pacific Command's (PACOM) server is by default the PACOM J6 Morning Brief. On an enterprise server, the same meeting could be anyone of the nine combatant commanders or the myriad of Joint Task Force (JTF) J6 morning briefs. Already, we're seeing meetings on the enterprise collaboration servers that are named "Chaplain" or "CSM Meeting" (presumably a Command Sergeant Major's meeting, but which one we surely don't know).

Other useful enterprise TTPs may involve meeting facilitation standards, such as who takes the notes and who gets to draw with which color on the whiteboard. Some of the TTPs might be able to be embedded in the collaboration tool, others may require training or peer pressure to be well-implemented.

Nearly every Combatant Command has recognized that collaboration TTPs must be established for recurring processes.

4. Technical issues

While the focus of this paper is on the people and process challenges of collaboration interoperability, two technical challenges stand out. The first challenge is one of standards and the second is that of cross-domain. Neither will be easy, but both are necessary.

4.1. Collaboration standards

The DoD's earliest attempts at resolving collaboration interoperability were standards-based approaches. In the late 1990s, the Defense Collaboration Tool Suite (DCTS) was designed to provide robust collaboration using industry-based standards. The only problem, and it was a major one, was that the industry standards were immature or not implemented by more than one vendor. As a result, only minimally interoperability existed, despite the best efforts of vendors and the government working together.

Today, the standards picture has not improved substantially. The Extensible Messaging and Presence Protocol (XMPP) provides interoperability for IM and presence. Mandated by the DoD Information

Technology (IT) Standards Registry (DISR) for use on DoD networks, XMPP has provided us with the first glimpses of what collaboration interoperability will look like [12].

Everyone is welcome to choose their own XMPP client, just as we choose our own telephones and telephony providers. We are able to find and chat with others, without consideration of the XMPP client that they are using. We do, however, still have to meet the challenges of trust and security that are required before we are able to federate our XMPP servers. Those challenges have been addressed above.

Given the robust collaboration environments now in use in the DoD, it may be difficult to imagine how a warfighter might join a meeting using a tool of choice. Full interoperability of robust collaboration may be a few years away. However, voice and video standards are mature. Interoperability in these areas are likely to come next.

4.2. Cross-domain

As briefly stated above, the United States does not conduct military operations alone. Even in our earliest days, we were partnered with French naval and ground forces in the siege on Yorktown. Today, we are part of a 37-nation force in Afghanistan and partner with other nations in Iraq as well as else where in the world. HA/DR missions bring even more diverse friends and partners, in addition to our traditional and formal allies. For example, in the 2004 tsunami response, the DoD was required to coordinate air space and other support with the Indonesian military. For over 10 years preceding this event, DoD had not conducted any operations or exercises with the Indonesians.

Today, staff officers in both Baghdad and Kabul regularly have over five computers on their desks to coordinate with the various coalition partners. In addition to NIPRnet (an unclassified DoD network connected to the Internet) and SIPRnet (a classified DoD network), the typical warfighter may need CENTRIX (Combined Enterprise Regional Information Exchange System), a NATO-classified system and other local or regional networks. The feature most requested by the warfighter is the ability to talk to whomever they need to talk to, using a single system.

The security challenges poised by cross-domain are clear, but not insurmountable. What is needed is an effort at the enterprise level to deploy the proper guards. Cross-domain guards are currently available that can pass certain types of collaboration traffic.

Currently, they must be individually certified and maintained by the requesting commands. An enterprise solution will achieve synergies as we continue to move this important solution forward.

5. Conclusion

As we begin to achieve interoperability of our collaboration tools, we must address the people and process challenges in addition to the technical challenges. Training and policy will play a critical role in improving our ability to collaborate and create additional value through our collaborations.

While some of these issues seem new, traditional common sense will always keep us in good stead. Change is hard for everyone, so we must help personnel move through the change. We shouldn't hesitate to question our assumptions – why can't the junior personnel contribute? – as we base our decisions on solid experience and proven performance.

Because collaboration is a human endeavor, the interoperability challenges will always start and end with the people involved. The processes and the technology must support them as we continually improve how we fight.

6. Reference

- [1] Watson, C., *Collaboration Through Technology*, Military Information Technology, Dec 2004, retrieved from <http://www.military-information-technology.com/article.cfm?DocID=354>, April 2008.
- [2] Alberts, D., Garstka, J. and Stein, F., *Network Centric Warfare*, 1999, Command and Control Research Program, p. 79.
- [3] Prensky, M., *Digital Natives, Digital Immigrants*, from *On the Horizon*, NCB University Press, Vol. 9 No. 5, October 2001, p. 1-2.
- [4] Department of Defense 5500.7R, Section 2-301, *Use of Federal Government Resources*, p. 27.
- [5] FY06 C7F Top Ten Information Technology Requirements, Naval Message from Commander, Seventh Fleet, 2005.
- [6] *The List of Chat Acronyms & Text Message Shorthand*, retrieved April 2008, <http://www.netlingo.com/emailsh.cfm>
- [7] Tapscott, D. and Williams, A., *Wikinomics: How Mass Collaboration Changes Everything*, Penguin Group, 2006, p. 253.
- [8] Cartwright, J., *Collaboration at USSTRATCOM*, Speech at National Defense Industrial Association Conference, Washington, DC, 2007, Text retrieved April 2008, http://www.stratcom.mil/Spch&test/Copy%20of%20CC_NDIA_6Mar07.html
- [9] *Joint Operations Concept*, Department of Defense, 2003, p. 35.
- [10] *Department of Defense, Information Sharing Strategy*, Department of Defense, 2007, p. 4.

- [11] *Collaboration Interoperability Working Group Enterprise TTP Brief Out*, Collaboration Interoperability Working Group, 2007, p. 4.
- [12] *DoD IT Standards Registry*, retrieved April 2008, <https://disronline.disa.mil>.

Author's Biosketch

Diane Boettcher attended Marquette University in Milwaukee, Wisconsin. Graduating from NROTC, she was winged a Naval Flight Officer the following year. She flew in the EP-3 Aries reconnaissance aircraft. She was then assigned to Pacific Command. While in Hawaii, she became a SCUBA diving instructor, creating a web site for her business in 1993.

Next, in Rota, Spain, Ms. Boettcher established the base's presence on the Internet. Following this assignment, she was the Security Officer for a telecommunications station in Washington DC, where she took additional webmaster duties.

In 2000, Ms. Boettcher became the Web/Marketing Manager at a healthcare IT consulting firm in Maryland. In 2001, she supported Commander, Task Force Navy Marine Corps Intranet as a Knowledge Management Engineer. Later, Ms. Boettcher became the Internet Technologies Advisor with Naval Network Warfare Command.

In 2004, she joined SRA and supported the Defense Information Systems Agency (DISA) Chief Technical Officer and Collaboration Management Office.

She was mobilized into the Navy in December of 2006 and served at U.S. Joint Forces Command in Virginia and Afghanistan.

Upon her return from mobilization, she became the Director of Knowledge Management at SRA's Advanced Programs and Business Technology Operations group.

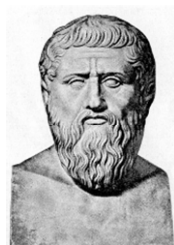


The Many Faces of Collaboration Interoperability

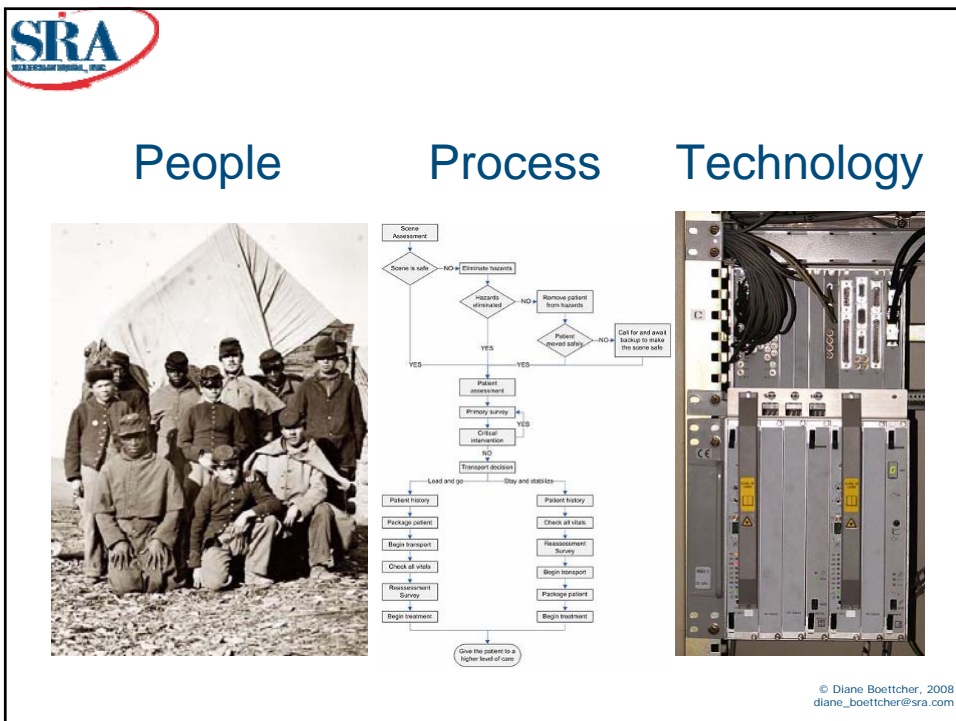
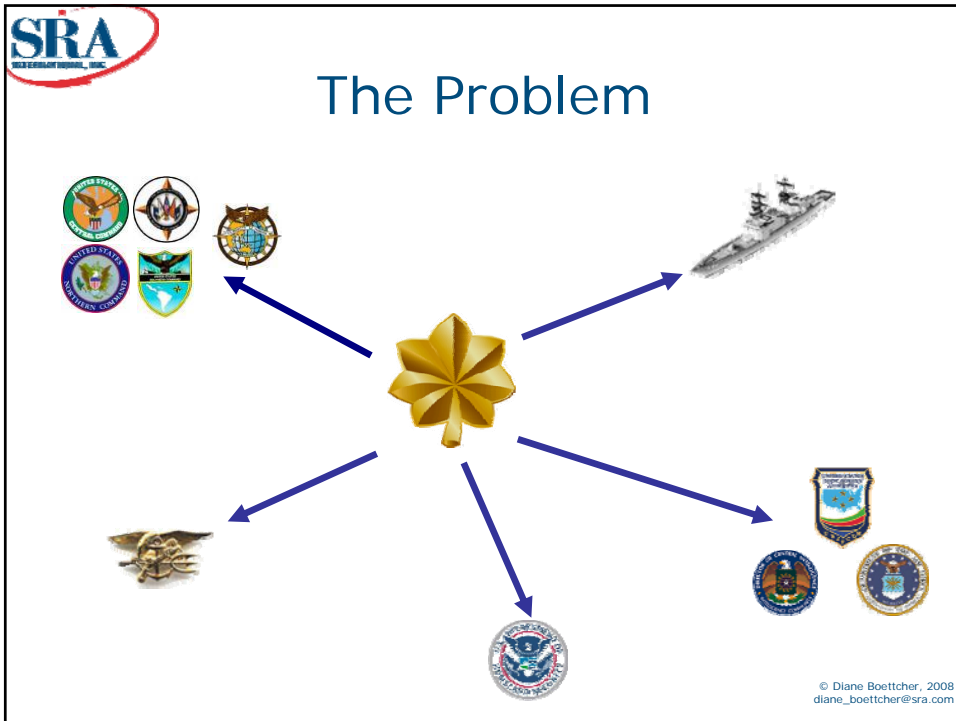
© Diane Boettcher, 2008
diane_boettcher@sra.com



Who am I?



© Diane Boettcher, 2008
diane_boettcher@sra.com





People




© Diane Boettcher, 2008
diane_boettcher@sra.com






Familiarization and training

© Diane Boettcher, 2008
diane_boettcher@sra.com





The improvement must outweigh
the pain of transition.

© Diane Boettcher, 2008
diane_boettcher@sra.com

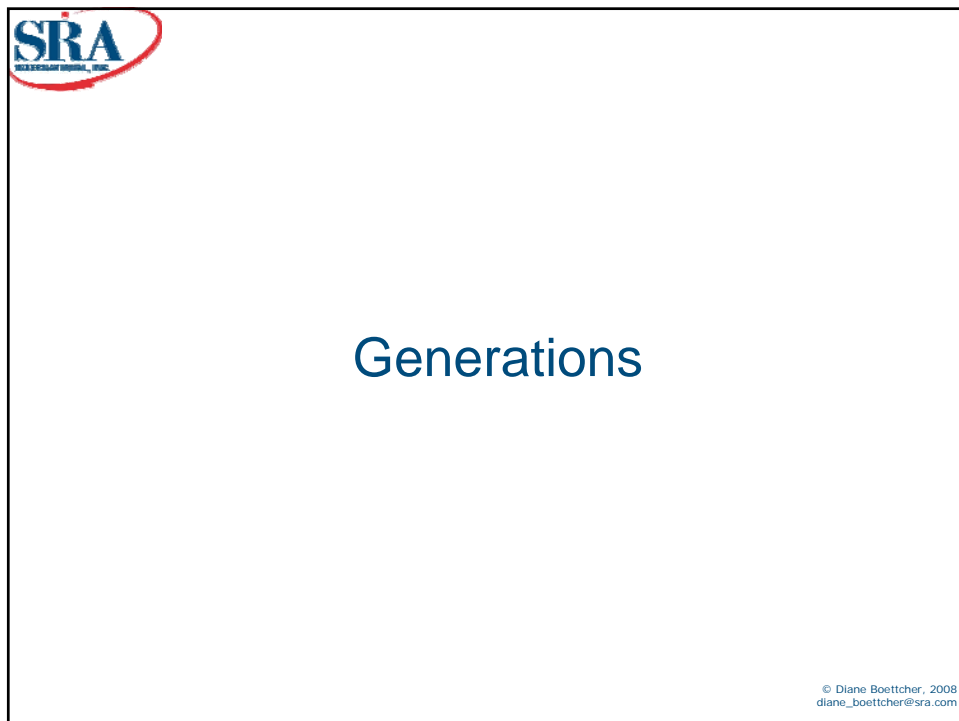


SRA
SPECIAL RESEARCH ASSOCIATES, INC.

When faced with
problems....


...people will revert to
what they know.

© Diane Boettcher, 2008
diane_boettcher@sra.com









Language

© Diane Boettcher, 2008
diane_boettcher@sra.com



Acronym	Meaning
AFAIK	As far as I know
CYE	Check your e-mail
FWIW	For what it's worth
GR8	Great
H/O	Hold on
HTH	Hope this helps
NRN	No reply necessary
SP?	Spelling?
TIA	Thanks in advance
W8	Wait

© Diane Boettcher, 2008
diane_boettcher@sra.com



Culture

© Diane Boettcher, 2008
diane_boettcher@sra.com



The chain of information
is not
the chain of command.

The customer is not
the commander;
it's everyone who
uses [information].

- Gen Cartwright
Vice Chairman
Joint Chiefs of Staff



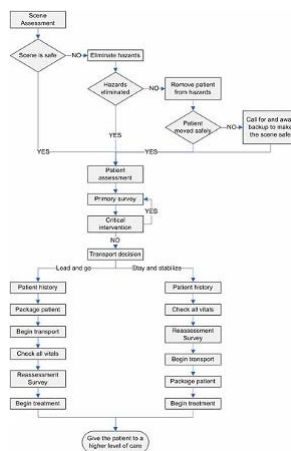
© Diane Boettcher, 2008
diane_boettcher@sra.com



That tank has a commander.



Process



© Diane Boettcher, 2008
diane_boettcher@sra.com



Trust

© Diane Boettcher, 2008
diane_boettcher@sra.com



© Diane Boettcher, 2008
diane_boettcher@sra.com



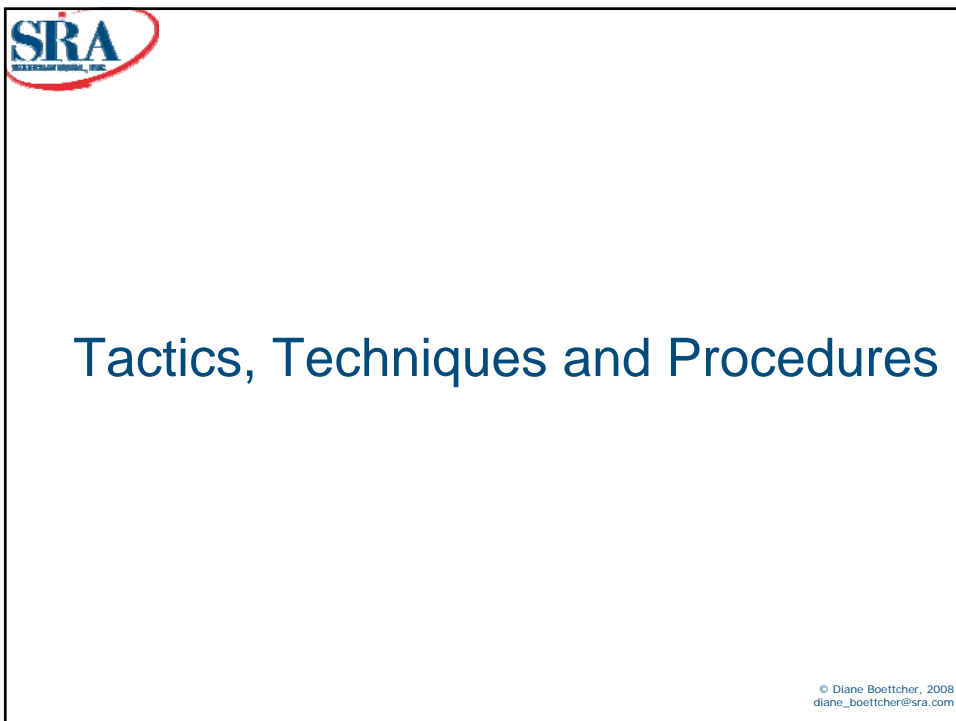
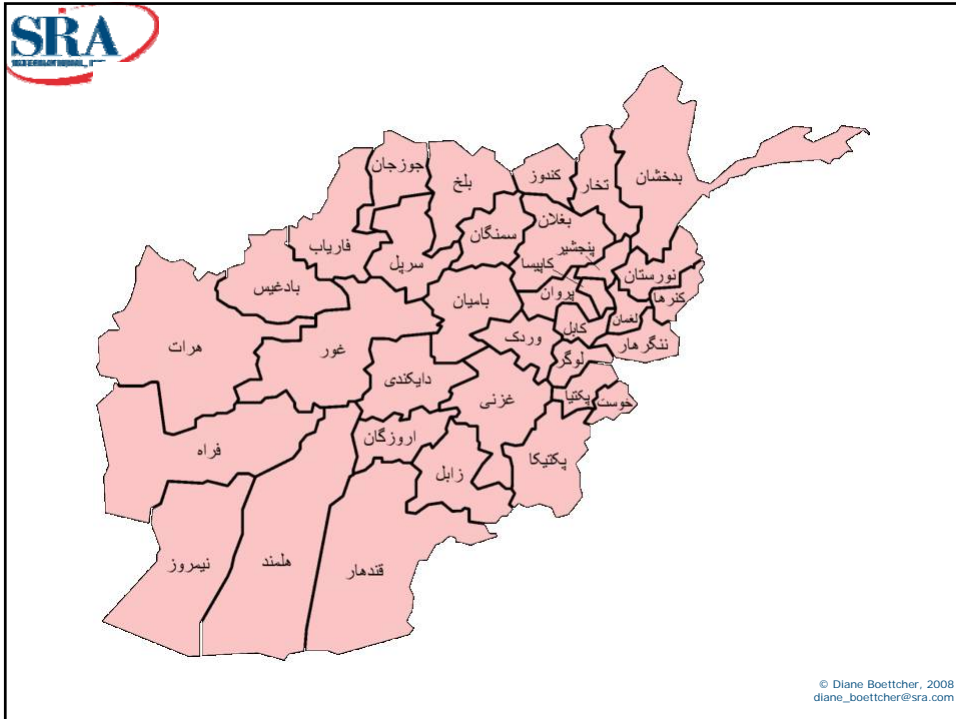


© Diane Boettcher, 2008
diane_boettcher@sra.com



Data

© Diane Boettcher, 2008
diane_boettcher@sra.com





John Paul Jones
Jones, John
CAPT Jones
Captain J. P. Jones, USN
Jones (Captain, United States Navy)
CO, Bonhomme Richard
BONHOMME RICHARD
BHR
N00, BHR
BONHOMME RICHARD, CO, CAPT J. Jones, USA



© Diane Boettcher, 2008
diane_boettcher@sra.com



BONHOMME RICHARD, CO, CAPT J. Jones, USA



US Navy, Senior SWO, CAPT J. Jones, USA



CJTF-HOA, J37, CAPT J. Jones, USA




CFMCC, J35, CAPT J. Jones, USA

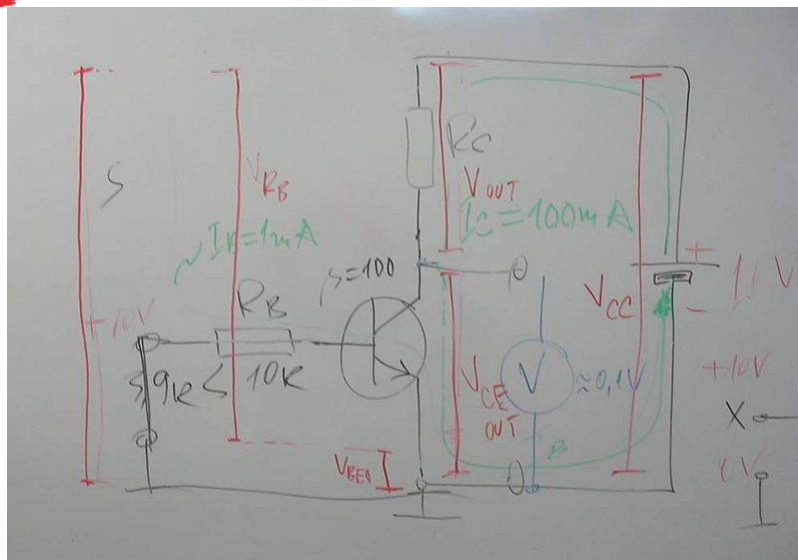


© Diane Boettcher, 2008
diane_boettcher@sra.com



		
RSOS	04Feb08	15:00
OCS General	05Feb08	00:00
3ID G6 TEST	13Dec08	00:00
DIMHRS	23Jan08	00:00
AFCYBER Staff Mtg	19Dec07	00:00
Chaplain	23Apr08	00:00
RATSS Demonstration	27Dec07	00:00
JTF-GNO Test 30 Dec 07	21Dec07	00:00
ESTA TEST	30Dec07	15:20
Web Site Registration	03Jan08	00:00
Global Medic	04Jan08	00:00
NETCOM A-GNOSC and MEDCOM meeting	04Jan08	00:00
GE21 Test Meeting	10Jan08	12:00
broader	10Jan08	00:00
	03Jan08	14:00

© Diane Boettcher, 2008
diane_boettcher@sra.com



© Diane Boettcher, 2008
diane_boettcher@sra.com

Technology

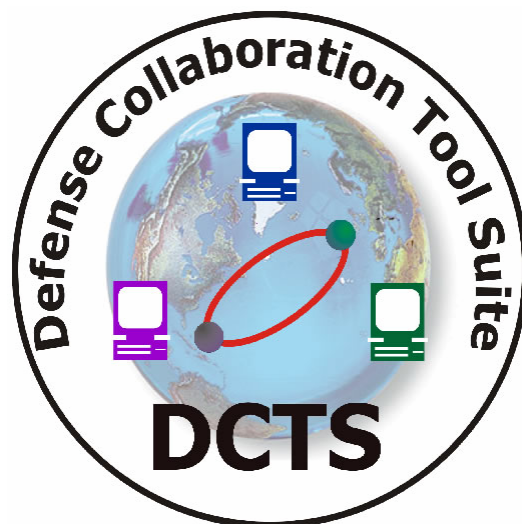


© Diane Boettcher, 2008
diane_boettcher@sra.com



Collaboration Standards

© Diane Boettcher, 2008
diane_boettcher@sra.com

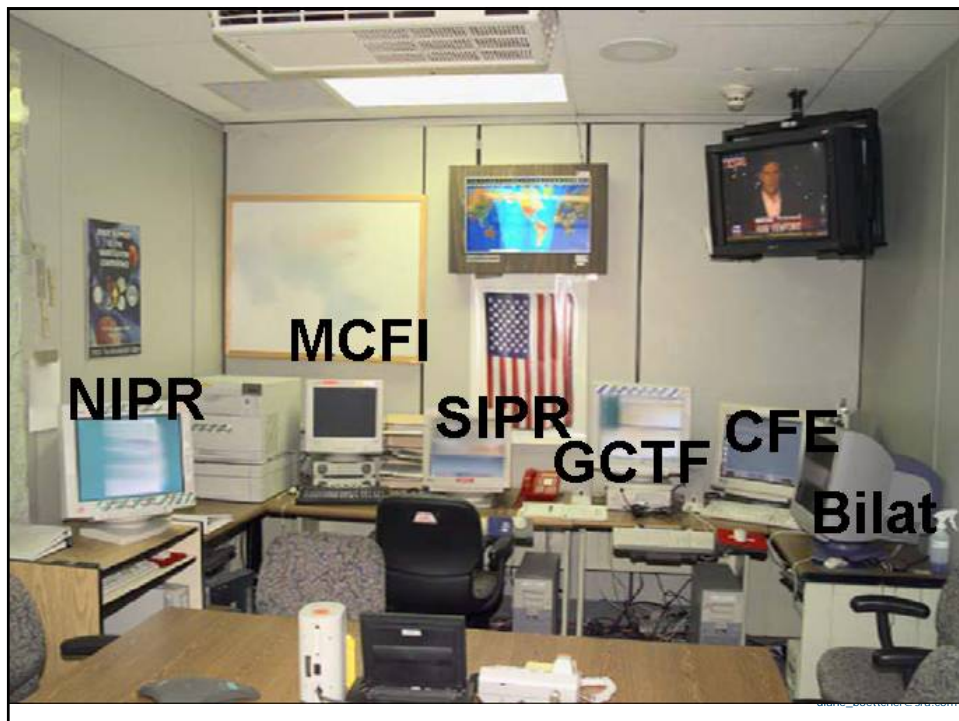


© Diane Boettcher, 2008
diane_boettcher@sra.com



Cross-Domain

© Diane Boettcher, 2008
diane_boettcher@sra.com





Conclusion

© Diane Boettcher, 2008
diane_boettcher@sra.com



Reach me at:
diane_boettcher@sra.com
703-803-1911

© Diane Boettcher, 2008
diane_boettcher@sra.com