15th ICCRTS
"The Evolution of C2"

Can't We All Just get along?

Topic 4: Collective Endeavors

Name of Author(s)

CDR Joe Stillwaggon, USN

CDR Dave Biddinger, USN (retired)

Point of Contact: Dave Biddinger
E-mail Address: dbidd2@hotmail.com

ABSTRACT

More than any time in history, the command and control of networked, quickly forming coalitions (that also dissipate in a planned manner) is dependent on the rapid and bandwidth-considerate dissemination of accurate information to the right players. While today's wikis and blogs and somewhat nascent portal and information sharing applications have helped, more advances are required if collaboration is to create true shared awareness and joint decision making. An understanding of security "nuances" and organizational cultural issues (both in forms of nationality and group dynamics) is essential to carry out the disparate disaster relief and counter-insurgency missions of today. We just might need to move beyond the Napoleon inspired J2, J3, J6 structure and even the current classification strata frameworks to get the mission essential data to the decision maker (who could be the General or the Strategic Corporal) in a timely and safe (commensurate with risk) manner. There are unintended consequences of any decision to make data "sharable" and they must be addressed in conscious, proactive, deliberate manner when approving procedures or designing information system architectures.

Coalition Considerations

More than any time in history, the command and control of networked, quickly forming coalitions (that also dissipate in a planned manner) is dependent on the rapid and bandwidth-considerate dissemination of accurate information to the right players. It is easy to state that "one of us is smarter than all of us" (we can cite many ICCRTS resources on the pros and cons of "groupthink"), but not simply to harness the collective wisdom when the would-be collaborators are in different time zones speaking different languages. Ironically, the ease at which ad hoc communications networks can be established sometimes leads to virtual stovepipes of vital information. Mechanisms that perform well in the dissemination of (assumedly accurate) information are not necessarily the best means to collaborate on REACHING a decision (or validating conclusions).

In most instances, the greatest barrier to information sharing is still POLICY. Project Managers have found that even in NATO there are only a few technological impediments to sharing information. In a few cases there are legal barriers (for example, one country has a law that prevents the police or Interior ministry from sharing information that might be used in a military operation.), but those examples are very few. In most cases, the nations are willing to share, but will not agree to a blanket sharing policy. They would like to reserve the right to share information on a case by case basis. And that is only with the 23 (out of 28) NATO nations that have an interest in Maritime Situational Awareness (MSA). Imagine trying to discover the policies for all the nations that have an interest in MSA but are not NATO, for example, Singapore, Finland, Sweden, Indonesia, Japan, China. I think it would take at least two to three years just to obtain and database the information exchange policies of each country. Then you have to factor in information exchange with NGO's (for humanitarian situations) and even private corporations, and you can quickly see that a matrix of information exchange agreements would be incredibly complex. It would be the first step to identifying those policies that are impeding information exchange, but could be modified or cancelled more easily than others.

Popular Tools and Collective Endeavors

While today's wikis and blogs and somewhat nascent portal and information sharing applications have helped, more advances are required if collaboration is to create true shared awareness and joint decision making. An understanding of security "nuances" and organizational cultural issues (both in forms of nationality and group dynamics) is essential to carry out the disparate disaster relief and counter-insurgency missions of today.

The young people joining our (humanitarian or military) coalitions today were weaned on information sharing and will continue to rebel against policies (and even long-held "truths") that they think restricts information sharing un-necessarily. They also expect that the tools they use "at work" will not lag three generations behind what they have at home (or more likely, on their person at all times).

Organizational cultural issues- "not invented here "(NIH) syndrome, resistance to change, clinging to "rice bowls"- typically present a greater challenge to attaining Information Supremacy than do technology challenges. Many experts point to the fact that no one body "owns" the Internet as one of the reasons for its growth and success. Bodies convene, agree on standards, and let the end user develop the solutions and the "rules of engagement". While this self-policing is not appropriate for every area of the C2 of coalition systems, we just might need to move beyond the Napoleon inspired J2, J3, J6 structure and even the current classification strata frameworks to get the mission essential data to the decision maker (who could be the General or the Strategic Corporal) in a timely and safe (commensurate with risk) manner.

Operations Security in Test and Evaluation

There are unintended consequences of any decision to make data "sharable" and they must be addressed in conscious, proactive, deliberate manner when approving procedures or designing information system architectures.

One of the purposes of a sound Test and Evaluation program is to expose any weaknesses or vulnerabilities before the system "goes live". However, the discovery, analysis, correction, and dissemination of these weaknesses should be handled in a proactive manner as part of an Operations Security (OPSEC) process. OPSEC is performed throughout the Test and Evaluation of a new system/process/product for a variety of reasons. This section will focus on regulations and on methods to prevent unauthorized disclosure to a potential (economic or political/military) adversary.

Development of OPSEC during the testing and evaluation of any new system involves a six step process. These steps are: identify Critical Information; derive Associated Indicators; analyze the intelligence threat; identify vulnerabilities; assess risk to Critical Information; and develop and apply OPSEC measures. Critical Indicators are the "crown jewels" of the program, such that the release of information would provide the adversary vitally needed information to defeat or neutralize the system undergoing test and evaluation. An example might be the algorithm that a radar system uses to shift frequencies, or shifts from searching to tracking. In the area of

kinetic weapons systems, many OPSEC methods are well understood, having been honed over the years. In the information age, as we test systems to be used by joint and coalition forces, OPSEC can become more cost prohibitive because of the availability of the information and the difficulty in securing the information during the test and evaluation phase.

Today's "net-centric" systems under development may in fact be self-contained and arrive at the Test and Evaluation facility with an understanding of how the system will protect the information it contains. However, the facility must also take care to protect the data gleaned from the Test and Evaluation process- that is, the data about the performance of the system/capability during the Test and Evaluation. By their nature, Test and Evaluation reports must be shared for the systems to correct identified deficiencies, and certainly the lure of collaborative tools such as blogs and wikis as a way to engage system stakeholders appeals to those reviewing the data for improvements and those looking for cost-effective methods to arrive at a solution to a problem revealed during testing and evaluation.

While information security/information assurance techniques have evolved since the mainframe/dumb terminal days, some issues persist, such as the ability of information systems to more easily aggregate unclassified data so that classified data or conclusions become readily apparent. Just as "Identity Theft" is affecting thousands of computer users, information security becomes a critical wall to those adversaries attempting to gain insight into testing and evaluation reports and plans. Examples abound throughout history of military and national forces ability to "surprise" adversaries with new systems. In some cases, the adversary had no knowledge of the development, testing and evaluation of the system. In others, while knowledge of the system existed, the testing and evaluation OPSEC resulted in employment of systems without adversarial countermeasures.

Tenets of Secure Interoperability

Even if we have moved forward from a culture of "data ownership" to "data stewardship" in theory, there is still the matter of making it all work in practice. The mantra of "**Secure the data, not the network** has been in place for a while, but most nonfictional (sorry, *NCIS* or *24*) data centers still show the symptoms of the failure to do this; multiple screens on every operator desk. Data tagging and binding standards must become more robust and prevalent.

Another area that warrants more experimentation is the temporal aspect of data (data is perishable, and the protection accorded that information must be able to degrade predictably after time). This concept is already established in the physical world; safes are rated by the amount of time it will take to "crack" them.

This is a nontrivial exercise in the world of military and international C2; actuarial tables that account for the VALUE (not just the predicted longevity, as is the case of insurance companies and annuity issuers) of human life thankfully do not exist.

Case in Point- How application of principles above as well as those found in the *NATO Code of Best Practices for C2 Assessment* could have been applied to recent humanitarian efforts in Haiti.

Each of the high-level topics above can be translated into a NATO C2 Assessment Measure of Merit. These measures are then in turn applied to the Haiti experience, and the results analyzed (and presented in June 2010). At the core of "assessing" a situation prior to making a command decision is the principle of risk reduction. According to the *NATO Code of Best Practices for C2 Assessment*, any assessment MUST result in less risk/uncertainty to the decision-maker (as compared to the levels prior to the assessment).

Every theme discussed in this paper can be (and will be) re-written in the parlance of risk, uncertainty, and sensitivity (applying the NATO C2 definition as in "response to stimuli", NOT political sensitivity nor relative importance).

Wrap Up and Suggestions for more Research

Author's Note: It remains my intent to present the "lessons learned" from the response to the recent Haiti disaster in more detail during my presentation in June 2010. If I can do so in a non-polarizing fashion, I might even (verbally) compare it to the response to recent Southern California quake response (might be topical, considering the ICCRTS venue). I'll likely avoid the terms "FEMA" and "Katrina", though my silent partner, the Liberal Arts major, might create a haiku using those terms.

The ISO 20000 (Information Technology Service Management) standard has been in place for several years. Adherence to the practices contained in this standard might help confront some of the issues presented in this paper (and hopefully some more of the "real life" issues brought out during the session!).

Several recent *C2 Journal* articles highlight the need for a "C2 level of maturity" assessment among the lines of levels of maturity for organizations themselves or for the processes of an organization (i.e., CMMi). This area of study could benefit from attention by ICCRTS stakeholders.

Recent improvements in the area of *Maritime Situational Awareness* and *Maritime Domain Awareness* also illustrate the themes discussed in this paper.

References:

http://www.rta.nato.int/Activity_Meta.asp?ACT=SAS-026, accessed 2 APR 2010

http://www.usaid.gov/helphaiti/, accessed 1 APR 2010

http://www.army.mil/-news/2010/01/13/32876-military-assesses-haiti-disaster-readies-for-response/, accessed 27 MAR 2010

http://www.timesonline.co.uk/tol/life_and_style/food_and_drink/real_food/article7081929.ece, accessed 1 APR 2010

http://www.baltimoresun.com/news/nation-world/bal-te.haitiborder03apr03,0,4400497.story, accessed 3 APR 2010

A Global Force for Good- Humanitarian Relief in Haiti, Shipmate Magazine, MAR-APR 2010 edition