

Risk Management and Information Sharing in Tomorrow's Networked Coalition

Submitted to:
11th ICCRTS

Authors:
Dave Biddinger, CISSP, SPARTA
Peter Shanley, Sapient
Michael Stubbings, Qinetiq

Single Point of Contact:
Dave Biddinger, CISSP
7110 Samuel Morris Drive Columbia, MD 21045
Ph: 443-430-8007
E: dave.biddinger@sparta.com

Date Submitted:
April 17, 2006

Abstract

In networked, coalition operations, information security policies must enable data sharing while simultaneously protecting the information in a manner that satisfies the national information provider.

Most security practitioners recognize that the current Risk Management approach (codified in the information systems certification and accreditation framework) does not address all of the challenges as the focus of interconnected “families of systems” transitions from a “need to know” model to a “need to share” {securely} model.

This paper will stimulate thought about and invite audience participation in reviewing changes we need to make to coalition policy, governance, systems engineering, and information management to ensure that we maximize the effectiveness of our “effects based operations”.

Table of Contents

Abstract.....	i
1.0 Executive Summary	3
2.1 Dependence on the Subjective Inputs of Humans	5
2.2 Risk Process to Support Command and Control.....	5
3.0 Coalition Information Sharing	7
3.1 Discussion Cases.....	7
3.1.1 University Challenge Ground Rules	8
3.1.2 Impact to Human System Integration	9
3.1.3 The Robots are Coming	9
4.0 Preparing for the Needed Changes to the Certification and Accreditation frameworks	11
4.1 IACAP is coming- prepare the humans	11
5.0 Integrating the Results of a successful Risk Management process to improve Domain Awareness	12
5.1 Does a Risk Common Operating Picture make sense?.....	12
5.2 Feeding your RM Program (or is it Programme?)- why a common risk language (lexicon) is necessary	12
5.3 Cross Domain Solutions	12
5.4 Metrics for Maritime Domain Awareness	13
6.0 Recommended Roadmap for Success.....	14
6.1 Alternatives to the Current Classification Schema	15
6.2 Incorporating eMASS into your Defense Environment.....	15
6.2.1 First Things First – How is your requirements management system?.....	16
6.3 CWID 2007	16
6.4 The Strategic Corporal Chimes in.....	17
6.5 ISO 27001 and Interoperability- Drivers for Certification and Accreditation framework improvement.....	17
6.6 Areas for Future Research	17
7.0 References.....	19

1.0 Executive Summary

The genesis of our team's concept for a paper occurred during the DoD CCRP event in June 2005. Our original topic was "Beyond DIACAP: A Certification and Accreditation framework for 2020". As our discussion ensued, we found ourselves delving into more of the underlying Risk Identification and Management and we adjusted our scope.

Despite advances in technology and simulation, the current state of Risk Management (RM) practice is still more art than science, dependent upon the subjective inputs of humans, and relative to a single instance. Our coalition partners realize that RM methods are not adequate for tomorrow's operating environment. RM needs to be accomplished continually, in an adaptive, context-aware manner. In today's environment of the "Strategic Corporal" and the "three block war", we fail to give the personnel on the "pointy" (tactical) end the tools and freedom to exercise their best judgment when it comes to sharing information.

The U.S. Government has acknowledged the severe limitations of its DoD information technology system accreditation process (DITSCAP) and is already embarking on a replacement, the DIACAP. Even this approach may be perceived as too paper-intensive and ill suited for the challenges of today's Service Oriented Architectures employed to enable Information Sharing in a secure manner if all coalition members cannot participate. The U.S. Government has embarked on a "Revitalizing C&A" effort with wide participation from both government and industry.

By employing a lively format and a wide range of scenarios, the conference session will further the discussion of changes we need to make to coalition policy, governance, systems engineering, and information management processes to ensure that we maximize the effectiveness of our "effects based operations". Our metrics will include the contribution to Maritime {this is the U.K. after all} Domain Awareness as well as the impact on the end users {Human System Integration}.

The outcome of this interactive, workshop-light session will be a RECOMMENDED Roadmap for Success that we hope will address:

What non-technical (cognitive, procedural) changes need to be considered?

What risks do poorly designed information systems pose to mission success?

How do we reconcile the needs of all stakeholders while continuing to recognize that in a coalition environment "a risk accepted by one is a risk shared by all"?

As international standards such as ISO 27001 gain more widespread acceptance, will they help solve these problems?

What risk management decision criteria should be applied prior to “collapsing” networks and their corresponding Cross-Domain Solution (CDS) elements?

The valid argument that “the risk does not exist unless the threat and vulnerability together are associated with a defined, probable costed, business impact that the risk acceptor cares about enough to avoid.

2.0 Brief History of Risk Management Practices

Risk Management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components in the organization's information system. (Principles of Information Security, 2nd Edition, Dr. Whitman and Mr. Mattord)

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} - \text{Security}$$

Alternately, the UK government information security policy documents characterize risk as being a combination of threat, vulnerability and (unwanted) business impact. All three components are needed for a risk actually to exist - including the impact. 'Residual risk' would be the risk left after you've taken any counter-measures. Residual risk is a significant concept in UK thinking and is written into the HMG Information Security Standards.

Regardless of your definition for Risk Management, it is performed to:

- protect national assets
- protect privacy
- counter threats
- improve business processes
- meet regulations
- ensure a repeatable process

Risk Management spans from international interests to personal privacy. As the world moves toward a higher reliance on digital communications, the need for RM will increase.

Despite advances in technology and simulation, the current state of RM practice is still more art than science, dependent upon the subjective inputs of humans, and relative to a single instance. RM continues to be based on the long history of counter-terrorism and the protection against espionage. The RM approach was based on a nation against nation geo-political world. In this former world, our adversaries developed capabilities slowly and often times in a predicted way. The main threat was from other nations discovering our secrets. Today's threats

are exponentially more dynamic, effective and numerous. RM practices need to adjust to the current state and quickly adapt to future needs.

2.1 Dependence on the Subjective Inputs of Humans

It is interesting that we expect people to consider a wide range of risks: risks to themselves, risks to colleagues, risks to civilians, risks to the operation, risks to the good name of their unit and their country. Decision makers do not assess and take these risks in isolation. Military and political command structures and policies constrain and support decision-makers at all levels of command and control. The risks and consequences of risk decisions are nevertheless real and potentially far-reaching. The interesting point is, however, that while we allow and often encourage risk decisions with significant military or political consequences to be taken far down the command chain, information security risk decisions do not appear to be similarly delegated. Instead, risk decisions can be - and often are - built into network architectures; they can be centrally implemented through public key infrastructures; they can be reviewed centrally by system accreditors.

This is not necessarily a bad thing. In a highly networked battlespace it is certainly arguable that “a risk accepted by one is a risk shared by all” – a principle of much wider significance now that coalition operations have such a significant place in our military endeavors. Given that principle, battlespace information security risk management might best be undertaken by those in a position to make optimum decisions on behalf of all, e.g. accreditors. Like many principles, this one has a complement: “a risk avoided for all is a risk the opportunities of which are denied to all”.

On the one hand we have collective risk. On the other hand we have individual opportunity. Those opportunities are likely to be fleeting, local, unpredictable, possibly misleading, and almost certainly inadequately defined. But they might well be significant, and might constitute a pivot point between success and failure. The collective risks are likely to be more clearly defined in scope and significance; more pervasive; more predictable. It is not surprising that we concentrate more on collective risk than on individual opportunity.

2.2 Risk Process to Support Command and Control

There are many people in information security who know where they are going. They are building ‘security’ into the network; introducing centralized control through techniques such as public key encryption and increasingly sophisticated authentication approaches; and encouraging central ownership and management of information. In such an interconnected age, such an approach is not surprising especially when it has been noted that ‘a risk accepted by one is a risk shared by all’: someone somewhere has to make decisions on behalf of ‘all’.

In questioning whether this path remains the optimum one for command and control systems, we are genuinely leaving the question open. To challenge

something does not necessarily mean that it is wrong; it means that the subject is important enough to be worth measuring against developing command and control needs and against new ways of expressing those needs. So – are we heading in the right direction? Have we identified the right destination?

It is probably wise to consider the destination itself before we consider the direction which will take us there. Where is it? What does it look like? How will we know when we have got there? It would be straightforward to come up with bland, high-level statements about the optimum balance between operational flexibility and the protection of critical national and coalition information assets. Being bland is not necessarily the same thing as being wrong or inappropriate. Bland can still be right. But the interpretation of such statements and their application to real situations inevitably display elements of subjectivity and caution, heavily informed by one's own personal experience. Perhaps more importantly, they also rely heavily on established policies, definitions, mental models and cultures. For example, the definitions and procedures associated with the classification system are so deeply ingrained into our thinking that we rarely question or examine them.

This paper does not present a comprehensive list of recognition criteria for a proposed command and control security 'destination'. The criteria suggested below are meant to start a conversation between people who come from the security profession and people whose job it is to make information systems, and much more importantly, the information they carry, work efficiently and constructively in the field. We therefore suggest that a good information security regime would:

- Be in accordance with a broad range of internationally-accepted information security management regimes including those used in the commercial domain;
- Be based upon an information asset valuation system which recognizes the aspects of information which really matter to command and control system users;
- This could mean more than just conventional classifications of documents or diagrams held on 'the network'. It could mean noting how perishable information is and when it expires. It could mean registering the type of data (whatever 'type' means). It could mean recognizing that the reliability and provenance of data might be as important, if not more important, than whether it is disclosed or not.
- Allow a very rapid set-up and tear-down of information system networks, sub-networks and connections without extensive (i.e. operationally expensive) constraints from security approvals regimes;

- Be able to use local telecommunications resources (e.g. in the manner of the UK Defence Logistics Organisation's Field Service Pack);
- Allow rapid decision-making for disclosure or information sharing with non-coalition individuals or organizations (e.g. local authorities or the Red Cross) – and equally rapid implementation of decisions – based upon notions of risk and risk management which acknowledge not only the dangers of policy breaches, but also that not connecting, or not disclosing might sometimes be unacceptable;
- Be technology-independent – we do not want a regime which has to be rethought every time new types of hardware or software become available.

Clearly today's and tomorrow's coalition operation commanders stand to benefit from the good information security regime (framework) discussed above.

3.0 Coalition Information Sharing

The most dangerous phrase in the language is, "We've always done it this way."

Grace Hopper

Our coalition partners realize that RM methods are not adequate for today's nor tomorrow's operating environment. RM needs to be accomplished continually, in an adaptive, context-aware manner. Information needs to be delivered appropriately throughout the coalition both on-demand and as discovered. The RM practices need to span multiple networks and allow for the flow of information throughout the operational forces. RM will need to handle the Global Information Grid (GIG) information flows and interoperate coalition systems .

Risk Management needs to be decentralized down to the key decision makers who hold the context of the situation. Need to know and dissemination is now controlled centrally and is not effective for the holistic coalition.

3.1 Discussion Cases

The need for balance is certainly recognized: the dictum 'classify the data not the network' is an example of this. Have we achieved the optimum balance between these two imperatives? Do we largely maintain that balance? If not, when, where and how do we get the balance wrong? Can we produce evidence, narratives, to back up our perceptions? If we have got it right, can we produce evidence for that? Are we even sure about how we would recognize our success or our failure in achieving this balance?

This section of the paper does not present answers to these questions. It does, however, suggest a set of topics which should be studied and discussed, and not just by information security professionals. That last point is critical: information security regimes, cryptographic key management processes, classification schemas and the like are not there for the accreditor, the security manager, or the security policy-making organizations of our respective countries. They are there to achieve political and military advantage, to enable our organizations to comply with international laws and treaties, and to enable us to trust each other. The subject is therefore far too important to be discussed only by security professionals. Those who have something to win and something to lose must also be part of this – which is why this paper is being presented at a Command and Control conference, and not at an information security conference.

Our intent is to utilize a portion of our conference presentation time as a mini-“workshop” (under University Challenge’ ground rules) to discuss our scenarios (or if we can reach a quick consensus, a scenario of the audience’s choosing) in a manner such that we can show that improvements to the coalition RM processes and information sharing agreements can yield tangible results in the areas of Maritime Domain Awareness (MDA) and Human System Integration (HSI).

3.1.1 University Challenge Ground Rules

There is a UK game show called ‘University Challenge’ where teams from different universities compete to show how much general (but generally obscure) knowledge they have managed to acquire during their studies. The first questions each form a ‘starter for 10’ – they get things rolling. Here are some ‘starters for 10’ – this isn’t a complete list, but it will do for now.

We have a classification system dating from the Second World War, if not before. Is it fit for today’s purposes?

What candidate criteria could we suggest for assessing the fitness of our classification regime?

Our classification regime is very static – it makes little or no allowance for rapid down-grading or up-grading, or for the useful life of the assets classified. Do we need a temporal attribute in our marking regime?

How do we communicate risk? Can it be reduced to numbers in some risk assessment algorithm, or does it have a subjective, narrative or contextual quality which needs to be recognized and structured?

In a widely networked battlespace, with an expanding range of military and non-military coalition stakeholders, what significance do the terms ‘asset owner’ and ‘data owner’ actually have?

Should we consider information security risks in relation to the functions of our data and other classified assets? Is Command and Control data a separate category from other types of data? If so, does the difference matter?

Who assesses information security risk? Who should assess it?

How do we know when the risks change? What do we do if the risks do change? – and like investments, risks can go down as well as up.

Who can decide to take a risk? Under what circumstances? How do we decide whether a risk is worth taking or not?

But there is something we should consider first. What is our experience? Is there any evidence that opportunities have been lost because we observed the information security rules strictly? Are there examples where flexibility in applying security rules has come at a price? – or might have done if someone had not stepped in and corrected matters? What has operational military – especially Command and Control – experience got to say that information security practitioners and policy makers should heed? This conference would seem like a good place to ask the question.

If everything is in fact working well, to the advantage of our military operations, then the ‘starters for 10’ need not be asked. But if not, then now is a good time to ask questions. There is no security question too iconoclastic to ask: our information security principles and practices may be robust enough to resist all challenges, but if we do not challenge them we will never know how robust they are.

3.1.2 Impact to Human System Integration

At previous CCRTS and ICCRTS events, Human System Integration (HSI) has been discussed in the context of reduced ship manning, improved communications systems, wearable computers, and more readable COPs. For our RM purposes, we have examined how to minimize the inherent errors in RM process inputs due to human bias, while creating an output that is both understandable and “actionable” so that coalition decisions can be made and acted upon in the dynamic environment.

3.1.3 The Robots are Coming

Partially due to the success of Unattended Aerial Vehicles (UAVs) in current operations, we anticipate that the use of robots in coalition operations of the future.

For our workshop, we have created a scenario where “swarms” of nano-sensors are feeding data (known to contain errors, both false positive and false negative, at 10% rate; of course our artificial intelligence system cannot quite determine which 10% are erroneous) to our BLUE FORCE maritime robots.

The UK ARMY robot will accept all inputs as true and has a huge tolerance for risk. He also shuts down every day at 1600 until refilled by 2 liters of tea.

The SUBMARINE robot, knowing that he is smarter than all of the rest, always requires that three independent inputs concur before he updates his COP.

The AIR FORCE PILOT robot, which joined the maritime component of this coalition due to a lost wager on the 11th hole, is wired to believe that landing his aircraft on a ship that moves carries a very high risk.

The purple JOINT COALITION robot cares only about completing the mission, and will broadcast all information he receives regardless of handling caveats or origin.

The BUREAUCRAT robot will make no decisions at all, and will often slow down the decision making algorithms of the other robots by demanding that CPU cycles be wasted on mundane tasks.

The RED FORCE maritime robots are actually old BLUE FORCE robots that were acquired on eBay. They have a rigid, hard-wired “need to know” algorithm and communicate on three channels: JEWEL, CROWN JEWEL, and PROPAGANDA. If a RED FORCE robot sends data through a channel incorrectly, he self destructs.



4.0 Preparing for the Needed Changes to the Certification and Accreditation frameworks

As expressed under the DITSCAP, the system-security status is heavily focused on documents. The primary documentation is the System Security Authorization Agreement (SSAA), in which each author independently decides how to describe requirements and solutions, what requirements and solutions apply, how to implement solutions, how to test, and how to assess risk. A lack of standardization in execution and terminology means that security documentation cannot easily be compared or analyzed across multiple system environments. Because the DITSCAP C&A cycle is three years, there can be no assurance that security information is current. And the DITSCAP process may be more expensive than is warranted by system-security requirements. This type of isolated, platform-centric C&A process is no longer viable in an environment in which systems are evolving from discrete networked entities to nodes in the network. "These collections of entities will ultimately become dynamically reconfigurable packs, swarms, or other organizations of highly specialized components that work together like the cells of our bodies. As such, they will be able to be far more discriminating and precise in the effects they cause.

Glenda Turner, DISA

4.1 IACAP is coming- prepare the humans

All coalition members share in the risk of coalition information sharing.

The transition from current certification regimes or frameworks to other "Information Assurance Certification and Accreditation Programs" has been analyzed in other ICCRTS papers as well as in defense publications.

For our purposes, we will assume that the rollout of the coalition "IACAP" is met with unanimous approval by coalition members and embraced by the developers of command and control information systems as a framework that has kept pace with the Service Oriented Architectures such that individual GiG services can be "certified" to a certain level.

Our focus will be on the risks associated with the aggregation of GiG-like services into ad hoc, dynamic "systems" with fluid boundaries. Key tenets of this (interim?) solution include:

- Dynamic process
- IA posture reviewed not less than annually
- Enterprise C&A decision structure
- Establishes objectives, context & decision structure
- IACAP Scorecard -- conveys compliance with assigned IA Controls and the IS C&A decision status
- Implements baseline (enterprise) level IA Controls based on the IS Mission Assurance Category (MAC) and Confidentiality Level (CL)

In looking to the (near?) future of 2015-2020, one can envision a “Quality of Protection” or “Quality of Assurance” metric analogous to the “Quality of Service” paradigm used by the telecommunications industry today.

While the U.S. plays a major role, it is important to recognize that international standards such as ISO 27001 (which grew largely out of BS 7799) will continue to grow in influence.

5.0 Integrating the Results of a successful Risk Management process to improve Domain Awareness

5.1 Does a Risk Common Operating Picture make sense?

Even the best COPs today, often designed by Human System Integration (HSI) experts, prove the entropy theories and yield a significant amount of “screen clutter” if not refreshed. Most operators understand the theory of refreshing based upon a change in time (as track uncertainty deteriorates) and space (as the distance between ship sensors and target emitters increases), but what about risk?

Is there a repeatable, well understood way to overlay or integrate the “risk attributes” of our sensor data?

How do we know if our “bogies” are bogus?

5.2 Feeding your RM Program (or is it Programme?)- why a common risk language (lexicon) is necessary

Even between service branches of a single nation connote certain terms (if no one at this conference has yet to make reference to the old but relevant jokes about how our services interpret the terms “tank” or “secure”, I’ll be surprised) differently. In terms of information system vulnerabilities, a common lexicon is required to ensure the enactment of appropriate countermeasures with a minimal disruption to ongoing operations. How shall we cut back on the “self-inflicted denial of service attacks” due to over-responding to changes to the INFOCON level?

5.3 Cross Domain Solutions

As long as coalitions need to categorize or classify nuggets of information into “bins” that require different levels of protection, we will have information that resides in “domains” and strict rules about when and how the information can cross domain boundaries.

This field of work is often termed “Cross Domain Solutions”; a Google © search will yield the following information:

Risk Management and Information Sharing

Within military and intelligence domains, classification level and need-to-know directives define the sensitivity of information. All information at a particular sensitivity level constitutes a security domain. Unauthorized information leaks from one security domain to another are of paramount concern, as violations may result in significant damage or loss of life. Conversely, effective conduct of operations often requires sharing of information, even across security domains. Cross-domain solutions ensure information availability while guaranteeing information security. Traditionally, information security has been achieved by physical separation. For each critical security domain, a front-to-back system is developed. All components of the system — clients, networks, servers — operate at system high, that is, the highest sensitivity of any information existing on the system. Sharing of information across security domains has been accomplished using guards, regraders, data replication and data diodes. Even though physical separation can be an excellent strategy for information security, as it minimizes opportunity for leaks, it does not scale well as the number of security domains expands. Maintaining multiple workstations, networks and servers becomes costly and eventually intractable, and the availability of data is often delayed as it passes through associated cross-domain processes. Galois, in partnership with the Navy and security agencies and in accordance with the DoD NetCentric vision, is working on critical cross-domain components which minimize required infrastructure and support a compose-able framework where data sources and applications are easily and securely reconfigured for new security domains. The architecture also accommodates the use of COTS tools wherever possible, leveraging the investment and capabilities available in the commercial marketplace. The cross-domain components are being developed following the Multiple Independent Levels of Security/Safety (MILS) approach and leveraging Galois' high assurance software development methods.

Évariste Galois (pronounced GAL-wah) possessed a remarkable genius for mathematics. Among his many contributions, Galois founded abstract algebra and group theory, which are fundamental to computer science, physics, coding theory and cryptography. Galois' contributions are even more remarkable in light of the fact that many were captured as hastily scribbled notes on the eve of his untimely death in a duel. Today, a "Galois connection" is a way of solving challenging mathematical problems by translating them into different mathematical domains, making the original problem amenable to a number of new solution techniques.

The keys appear to be that data must be labeled properly in a manner that resists unauthorized changes and that "old dogs" must trust the math algorithms to secure their data. Again, the temporal element (the fact that some data is "perishable", and could and should be "downgraded" within minutes of hours of its initial use) is an important factor in assessing the actual risk of sharing.

5.4 Metrics for Maritime Domain Awareness

Inputs to maritime operational pictures arrive from a myriad of sensors (some human, most not) in a variety of formats and at differing levels of data classification. We assert that in order to improve overall coalition Maritime Domain Awareness (MDA), we need to change the RM doctrine behind the data sharing processes and systems. For this scenario, we will develop a set of MDA metrics.

During the 9th ICCRTS, Galdorisi (et al) posited that there were four NCW capability options:

- Sub-Baseline: Organic self defence (with no shared situational awareness).
- Baseline (Low): Limited shared situational awareness between platforms sufficient to enable coordinated action.
- Intermediate: Shared situational awareness sufficient to enable co-ordinated action at the unit level. Reachback capability available
- High: Shared situational awareness sufficient to enable weapons targeting based solely on inorganic contact information.

In almost all cases of MDA, there is a need for better Joint Track Management. During our workshop, we will discuss the risks of sharing tracks with coalition partners (and the even greater risks of accepting the tracks as truth without some correlation efforts). We will use the robots paradigm of Section 3.1.3 to simulate different flavors of Track sharers.

6.0 Recommended Roadmap for Success

It is often easier to ask for forgiveness than to ask for permission.

Grace Hopper

Perhaps we can re-wicker the quote above to fit a time and place where informed RM decisions rule the day, and connectivity is dynamically granted (or denied) in real time.

If that is the sort of place we want to be, how should we get there? It is not yet possible to set out a detailed roadmap, nor to establish how long the journey will take. But some necessary preparations for that journey seem to be emerging:

There is a need to re-examine and if necessary re-express the information security properties of confidentiality, integrity, availability and non-repudiation in terms which are thoroughly in accord with operational military experience.

The classification system we have all grown up with should then be re-assessed in the light of these re-articulated properties.

Notions of risk, and in particular the articulation of risk, should be re-examined to see whether they map onto operational military experience, and how information security risk management maps onto broader models of military risk management and decision-making. This means in particular examining how we reconcile local and national or coalition imperatives.

Two types of listening are necessary for these activities to produce useful results. One is to the experience of information security management in other arenas. That does not mean importing wholesale the risk management practices of civilian business life – though it does mean willingness to see if there is something there which is useful to us. The other type of listening is to operational experience with current information security procedures and concepts. That means listening to people such as those attending this conference. It means noting where the rules work and where they do not. Perhaps they always work when applied properly – or perhaps not. The point is this: information security is there to make things work better for those who have much to win and much to lose; it is far too important a debate to be restricted to information security professionals.

6.1 Alternatives to the Current Classification Schema

Almost no one (except the “information wants to be free” zealots) disputes the need for a classification schema. We have all witnessed the over-classification of material that stifles information exchange and adds complexity and expense to storage and transmission. We have also experienced the political backlash when the information (or redacted subsets of it) is declassified decades later.

One useful analogy we uncovered involved whether we are introducing more complexity into local decision-making than military commanders actually want.

We used the analogy of the classifications being a set of handrails - he wondered whether we're considering taking them away and replacing them with some sort of guidance when what people really want is handrails. They're there, fixed and you can hang onto them. It does leave open the question of whether we've got the right handrails of course, but he suggested that people are comfortable with a fixed set of rules that they can either obey or conveniently ignore. I think he's saying that the rules don't actually have to be the right ones - the existence of handrails is more important than whether they are in precisely the right place. He's got a point, but even so I think it's worth asking whether better handrails would help.

The Strategic Corporal's friend

The current set of fixed classifications/ protective markings that governed who was allowed to see what information worked well throughout World War Two and during the Cold War. As coalitions gear up for Net Centric Operations/Warfare, perhaps an “upgrade” to the current system is warranted.

6.2 Incorporating eMASS into your Defense Environment

Future eMASS spirals may include logic that digests itemized scorecard information into a set of numerical expressions—an IA “score.” The score value will ostensibly denote the current level of system compliance within a predetermined range—from non-compliance to full compliance—on a dynamic scale. The manner in which this score will be used is still being defined within

the eMASS program; however, it is expected that the score may serve as a form of IA “token” that will be exchanged without human interface and analyzed at the system level as a pre-requisite for initiating a communication session between two GIG hosts. Presuming a simple line of communication between two hosts, eMASS will mediate the session request and compare the two IA scorecard values. Based on the values directly or in conjunction with some set of predetermined security conditions, eMASS may permit or deny the session and consequently permit a host-to-host connection or force a communication termination.

- Glenda Turner, DISA

6.2.1 First Things First – How is your requirements management system?

Of course we all know that information systems requirements are well known in advance and rarely change. Ha! Just as your system development requirements management system must be flexible, coalition processes (TTPs) that govern the sharing of information must have a temporal element and be adaptive to the dynamic environment.

Once a robust IA requirements management system is in place, changes to the operational requirements or the environment or even the insertion of a new coalition partner or component can be assessed to determine if the overall risk has increased. If the risk has increased, the “IA score” change will be reflected in the “tokens” such that information sharing decisions will continue to be made based upon solid data.

6.3 CWID 2007

Often information system procurement contracts are structured such that information cannot be shared legally between procurement agents who would otherwise benefit from synergy. While there are obvious differences between the Services (the Air Force does not typically design and procure ships), there are areas where consolidation makes sense (all Armed Forces require some type of logistics system). In the U.S., PPBS procurement system does not lend itself to interoperability. The coalition agencies suffer from similar stove-piped budget structures that often stifle information sharing, resulting in parallel but uncoordinated efforts to solve the same problems. Collaboration between coalition entities involves a level of trust that is not easily maintained war fighting allies are often economic competitors. Even if one nation develops a system with the intent of sharing its capability, there is no effective coalition mechanism to facilitate sharing its cost. The coalition management must recognize the barriers and move forward together to achieve the goals. The Coalition Wide Area Network (CWAN) development (demonstrated in JWID 1999 and used through JWID 2005) is a step in the right direction.

Another management challenge is to overcome individual and institutional resistance to change. This is often related to the “not invented here” syndrome

that permeates much of the coalition culture. This is the phenomenon where nations will not accept the practice or process or product that had its roots in a different country. Without a sharing of best practices across the coalition, effort is wasted in duplication and inefficiency.

Clearly the most obvious (and frustrating) barriers to coalition interoperability are antiquated regulations enforced in the name of “security “. Beyond the ridiculous system of “passing clearances” individually in message format when a shared database is an obvious solution, the need for security in designing interoperable systems is paramount to successful coalition collaboration and necessary for management acceptance. The paradox is that security can be viewed as both everyone's and no one's responsibility.

One venue to test the theories posed in this paper would be to apply them in an actual system or set of scenarios that could be demonstrated in CWID 2007.

6.4 The Strategic Corporal Chimes in

If you have read this far, you must be curious as to how we have helped the poor Strategic Corporal, who is now 2 $\frac{3}{4}$ blocks into his 3 block war and still unaware if the information that he has disclosed to the local cleric has helped our hurt his mission. As an example, part of the future vision of MAGTF C2 is that every Marine will become a user, producer, and consumer of Command and Control. With the emergence of new Operational Concepts and Functional Concepts that look to the future of Command and Control, the Marine Corps will need to have a guiding principle for the adoption of new tactics, techniques, and procedures that will reduce the proliferation of stove-piped systems across the air, ground, command, and support elements of the Marine Corps. In order for all Marines to be able to execute command and control RM will need to adjust to allow for the input of the these decisions in order to process the effects and continually update the holistic risk operating picture.

6.5 ISO 27001 and Interoperability- Drivers for Certification and Accreditation framework improvement

Examples here might include ways the ISO27001 (formerly BS7799) standard is applied in commerce, industry and government (noting that it is already in use in UK and US defense circles). This is not to say that there is a direct read-across from, say, banking into command and control. Banks do not open walk-in branch offices in battle areas. But they have a very clear attitude towards risk, accepting the cost of risks realized where that is less than the cost of control. It would be sensible at least to keep looking with an open mind for lessons from security management in other domains.

6.6 Areas for Future Research

Risk Management and Information Sharing

The governmental research arms of many coalition partners are happy to broadcast their command and control and other shortcomings to the world in the form of “research” needs. We will solicit input from our workshop participants but provide one recommendation to get things started.

- The addition of formal RM training to our field grade officers and senior enlisted as part of “Joint Professional Military Education” curricula.

7.0 References

The following sources were consulted at various times throughout the paper.

Jenifer M. Wierum, Defense Information Assurance Certification and Accreditation Process (DIACAP) and the Global Information Grid (GIG) Information Assurance (IA) Architecture, 10th International Command and Control Research and Technology Symposium: The Future of C2

Dr. Whitman and Mr. Mattord, Principles of Information Security, 2nd Edition,

Glenda Turner, Patrick Holley, Julie E. Mehan, and Michael Colon, Net-Centric Assured Information Sharing—Moving Security to the Edge through Dynamic Certification & Accreditation

Giorgio Venturi, Jimmy Troost, An agile, user-centric approach to combat system concept design, 10th International Command and Control Research and Technology Symposium: The Future of C2

CBRNE conference, Ottawa (22 September 04), Dealing with the RN side of terrorist acts: A view from the sideline

Garry Loeper, INTEGRATED CBRNE MANAGEMENT SYSTEM (MS) REQUIREMENTS

Dave Biddinger, Overcoming Barriers to Information Superiority in Coalition Operations, 2000 International Command and Control Research and Technology Symposium

Dave Biddinger, ISO 17799- Friend of the Auditor?, 2002 ISACA CACS Oceania presentation

Bost, Bob (NAVSEA) and Galdorisi, George (SPAWAR SSC SD), Transforming Coalition Naval Operations by Utilizing Human Systems Integration to Reduce Warship Manning: Lessons Learned from the USN DDG-51 Class Warship Reduced Manning Study, 9th International Command and Control Research and Technology Symposium, Copenhagen, Denmark, September 2004.

Jarret B. Rush , The GIG Information Assurance Architecture – NetCentric Enabler or Mission Impediment?, 2006 CCRTS, The State of the Art and the State of the Practice

<http://www.galois.com/aboutgalois.php>, accessed 1600 14 APR 06