15th ICCRTS

"The Evolution of C2"

A Tactical Framework for Cyberspace Situational Awareness (Paper #196)

Topic 8: C2 Assessment Metrics and Tools

Authors: Lieutenant Colonel David C. Bares (Master's Student, 3rd term),
Major Eric D. Trias (Ph.D.), & Doctor Robert Mills (Ph.D.)

Point of Contact: Lt Col David C. Bares
Air Force Institute of Technology
AFIT/ENG
2950 Hobson Way, Bldg 641
Wright Patterson AFB, OH 45433
703-973-7726
David.Bares@afit.edu

Abstract:

We are increasingly dependent on computers, networks, and cyberspace resources to accomplish military missions. Manifested via email, the web, databases, applications, command and control messages, and myriad other forms, the health and status of cyberspace affects everyone. Information technology is a strategic asset driving the Air Force towards a culture change such that we are all "operators" in cyberspace. As operators, each of us must maintain an appropriate level of situational awareness (SA) in cyberspace. In an airplane, the crew maintains SA through visual and instrument scan, radio, intercom and audible queues, and by operator interaction with mission systems. Unfortunately, cyberspace situational awareness tools are not as mature or clearly defined as those of an aircraft and its crew or other traditional weapons systems. Insight into confidentiality, integrity, and availability of information as well as what constitutes fully mission capable, partially mission capable, or non-mission capable for cyberspace highlight the need for improved situational awareness in cyberspace. This paper will explore situational awareness in the context of cyberspace, evaluate one existing implementation of a cyberspace situational awareness tool, and present an alternative scalable concept model for identifying and linking cyberspace resources to mission impacts at the tactical level.

A Tactical Framework for Cyberspace Situational Awareness

Lieutenant Colonel David C. Bares, USAF

Student, Air Force Institute of Technology, Graduate Cyber Operations Program

Doctor Robert F. Mills, Ph.D.

Associate Professor, Air Force Institute of Technology, Electrical & Computer Engineering

Major Eric D. Trias, Ph.D., USAF

Assistant Professor, Air Force Institute of Technology, Electrical & Computer Engineering

Cyberspace operations reinforce and enable everything we do – from administrative functions to combat operations – and we must treat our computers and networks similarly to our aircraft, satellites, and missiles.[1]

– General Norton A. Schwartz, Chief of Staff, USAF

Everyday we are increasingly dependent on computers, networks, and cyberspace resources to accomplish our mission. As issued by General Chilton, "I challenge anyone to claim that he or she is not dependent on cyber networks every day."[2] Manifested via email, the web, databases, applications, command and control messages, and myriad other forms, the health and status of cyberspace affects us all. Treating the Global Information Grid (GIG) as an uncontested utility with complete reliance on the "comm guy" to design, defend, and monitor cyberspace are head-in-the-sand attitudes that must change. Information technology (IT) is a strategic asset driving the Air Force towards a long overdue culture change such that we are all operators in cyberspace.[3, 4] To that end, we must all maintain an appropriate level of situational awareness (SA) in cyberspace. In an airplane, the crew maintains SA through visual and instrument scan, listening to radios, intercom and audible queues, and by operator interaction with mission systems. Unfortunately, in cyberspace situational awareness tools are not so clearly defined nor so well developed. What are the airspeed, altitude, and attitude safety-of-flight equivalents in

cyberspace? Are they the coveted confidentiality, integrity, and availability of information or something else and how do you measure them? Furthermore, what constitutes fully mission capable (FMC), partially mission capable (PMC), or non-mission capable (NMC) for cyberspace? Specifically when accomplishing one's mission, what are the mission impacts of a compromised database or severed communications to/from a given location? While these questions may not have immediate tangible answers, they are just a few that highlight the need for improved situational awareness in cyberspace. Thus, this paper will explore situational awareness in the context of cyberspace, evaluate one existing implementation of a cyberspace situational awareness tool, and present a scalable method for operators to link cyberspace resources to mission impacts at the tactical level with eventual aggregation at higher levels.

Situational Awareness Defined

Situational awareness (SA) is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[5] Taken from Dr. Mica Endsley's widely recognized model for situational awareness, this definition and her model imply three levels of SA. Level-1 SA, perception, is contingent upon identifying and assimilating appropriate data queues from the environment. Level-2 SA, comprehension, depends on comparison of the observed data relative to baseline conditions or goals. Level-3 SA, projection, focuses on predicting future scenarios to achieve proactive instead of reactive decision making.[6 & 7] In an airplane, airspeed, altitude, and attitude are just a few of the many data elements operators monitor for Level-1 SA. Given these data elements, extension to Level-2 SA implies the operator understanding the danger of a low airspeed, low altitude, and high angle of attack condition. Level-3 SA then manifest as the operator's prompt recognition of the dangerous scenario, applying power, and leveling the aircraft's nose to avert stalling and crashing the plane. Applied to cyberspace, Level-1 SA involves monitoring basic resource status parameters such as utilization or availability. Level-2 SA implies understanding parameter deviations from established baselines or goals thus facilitating a sort of FMC, PMC, NMC, assessment of the monitored resources. Finally, Level-3 SA provides the sought-after timely and accurate

projection of mission impacts that result from the current status of cyber resources. Unfortunately, we are playing a catch-up game in terms of situational awareness *of* cyberspace relative to the situational awareness *facilitated by* cyberspace.

For years developers have recognized the importance of situational awareness and incorporated SA tools into traditional weapon system designs.[8] Within the SA process, operators synthesize data from the environment, system interfaces, other crewmembers, experience, and elsewhere into an integrated picture from which decision and action takes place.[9] In many cases, as a consequence of cyberspace and the 'information age', operators are flooded with information.[10] On other occasions, especially regarding our SA of cyberspace, the case may be a lack of relevant information. Citing General Chilton's statement on this matter, "we have some unknown number of computers on the GIG that have unknown configurations, are in unknown locations, and are being operated by unknown users."[11] In either case, developing situational awareness and keeping it up to date in a rapidly changing environment is a significant portion of an operator's job.[12] Just as an aircrew's degraded situational awareness may adversely impact their mission, degraded SA among cyberspace operators may degrade our mission effectiveness. Therefore, as more facets of cyberspace are treated as weapons systems, and as the paradigm shifts from Airmen as cyberspace users to operators, situational awareness tools and common operating pictures rivaling those available to front line operators in air, land, sea, and space are imperative as well.[13]

Situational Awareness in the Air and Space Operations Center

As the nerve center for air operations, the Joint Forces Air Component Commander (JFACC) and his or her staff need situational awareness regarding the Air and Space Operations Center (AOC) and its systems. Just as the E-4B National Airborne Operations Center aircraft is a major weapons system (MWS) for command and control, the AN/USQ-163 Falconer, commonly known as the Combined Air and Space Operations Center (CAOC), is also a MWS providing command and control over airpower.[14 & 15] As a MWS, the CAOC has Air Force tactics, techniques, and procedures describing its systems, processes, and personnel.[16] Its operators receive formal qualification training and participate in

training exercises such as BLUE FLAG and RED FLAG.[17] Likewise, CAOC and AOC operators need tailored SA tools just like any other MWS operator. Master Caution Panel (MCP) and Command and Control Resource Management System (C2RMS), satisfy this need and exemplify the first of many steps towards developing comprehensive situational awareness tools throughout cyberspace.

Figure 1 An AOC (top) and C2RMS[18] (bottom)

MCP was first introduced in the fall of 1998 adopting its title from the aviation Master Caution Panel that provides aircraft system status information at a glance.[18] Advanced Technology Master Caution Panel, as it was formally called, supported the Joint Force Air Component Commander with AOC information technologies systems management and provided situational awareness by tying enterprise network components to the operational tasks they support.[19] Its purpose was to monitor the IT system resources of the AOC and *alert system administrators* to possible problems impacting operations.[20] Comprised of automated monitors, a server, clients, and a configuration tool, monitors reside on any computer and feed the server with raw data from monitored resources.[21] The MCP Knowledge Management Service (KMS) resident on the server consolidates resource monitor input and sends messages to the clients providing two essential pieces of information: 1) identification of which resource is in what status and 2) how the task list is affected by resource status.[22 & 23] Clients access tailored views displaying resource details and task status based on settings from a Knowledge Base (KB) Configuration Tool which system administrators and team chiefs use to configure the system. [24 & 25] The key distinguishing feature of MCP is its *ability to relate systems to the operational tasks that depend on those systems*.[26] MCP later evolved into C2RMS with an expanded feature set including: application

across multi-level security; Simple Network Management Protocol-based monitors for insight into airborne network systems; a Monitor Development Kit (MDK) that provides monitor development in the field; integration of mapping software and Digital Terrain Elevation Data components; and finally, the Joint Weather Impact System (JWIS) monitor.[27]

Lessons from MCP/C2RMS

The MCP/C2RMS suite is a cyberspace SA success story with multiple lessons applicable towards development of situational awareness tools outside of the AOC. First, the suite has already evolved beyond MCP's original, limited target audience focus of monitoring resources and alerting *system administrators*. Recall that a degraded system is no longer just the "comm guy's" concern. As part of the cyberspace culture change, operators, commanders, and administrators all need insight into the status of systems and resources.[28 & 29] C2RMS widened its focus and provides operators, administrators, and commanders at each level, to include the JFACC, real-time insight into the status of tasks and resources.[30] Similarly, any new cyberspace SA tools should provide appropriate insight to those using as well as overseeing resources. Second, MCP/C2RMS successfully leverages industry and military standards and technology. It is a tiered system utilizing the Java 2 Enterprise Edition and Java Messaging System specifications coupled with a Java Database Connectivity compliant database.[31] C2RMS can also interface with other systems or remote nodes using extensible markup language files and, if needed, establish secure connections through an Information Support Secure Environment Star Guard. [32 & 33] Other SA awareness tools should also incorporate these and other standards like Web 2.0 to shorten the development cycle, integrate with existing commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) programs, and maximize flexibility and interoperability.[34 & 35]

Another lesson emerges from the MCP/C2RMS linkage of resources and tasks. As previously mentioned, C2RMS relates systems to the operational tasks that depend on those systems.[36] This resource to task and mission-impact relationship depends upon a priori analysis of the AOC with significant administrator involvement. Within C2RMS, "system administrators use the KB Configuration Tool to identify what resources must be monitored, identify how these resources relate to tasks to be completed,

create and configure alerts for monitored resources and deploy monitors to systems running the Monitor Service."[37] When a resource is degraded or fails, notifications are sent to those affected with courses of action (COAs) elaborating the nature of the problem, proposed solution, estimate time to reconciliation, and possible workarounds.[38] Status notifications provide Level-1 SA insight to operators but the COAs that begin to provide higher level SA are simply communication messages relaying the human initiator's analysis. As an alternative to this administrator centric, a priori configuration and analysis methodology of C2RMS, future operators might someday individually tailor cyberspace SA tools and leverage automation for analysis of AOC task-to-mission relationships.

Finally, the MCP/C2RMS suite has demonstrated growth potential. Original monitors were assigned to *AOC-specific* resources. However, monitors could be developed for other resources emulating what was done for JWIS using the C2RMS monitor development kit. The Core Automated Maintenance System (CAMS) provides mission capable status for aircraft in the fighter/bomber community with a system known as G081 providing similar functionality to tanker and airlift units.[39] Already identified for future work, "C2RMS monitors could fuse data from maintenance systems to provide status to the decision makers."[40] Extrapolated further, monitors could be developed for almost any resource to include maintenance, logistics, munitions, scheduling, or personnel databases and email or web servers to name few. However, even when incrementally addressed one resource or application at a time, this is a daunting challenge.

Beyond the Air and Space Operations Center

While the CAOC may be unique among computer-based systems with its formal recognition as a weapons system, it is not exclusive in its status as a mission enabler. Software applications are instrumental in a variety of everyday tasks such as changing pay information, adding family to personnel records, ordering aircraft parts or fuel, storing maintenance records, manifesting a flight, or transmitting targeting coordinates for a missile strike.[41] In 2006 the Air Force had more than 19,000 such applications residing in thousands of systems across the service.[42] Fortunately, modernization efforts focused on sharing and exchanging data centrally from secure and trusted sources should migrate the service to less

than 2,000 applications by fiscal year 2012.[43] In comparison, the Air Force has 46 different aircraft major weapon's systems ranging from the A-10 Thunderbolt II to the WC-135 Constant Phoenix.[44] Tripling this number conservatively accounts for its unmanned aerial systems, space systems, and multiplatform "weapons" like the Joint Direct Attack Munition and Sniper Advanced Targeting Pod while still being orders of magnitude less than the desired number of software applications.[45] Thus, despite the projected 90% reduction in software applications, treatment of the remaining applications as weapons systems with commensurate situational awareness tools is an enormous undertaking. This is further complicated by the complex nature of situational awareness in general and implied characteristics of meaningful SA tools.

Situational awareness is largely dependent upon the eyes of the beholder. Each person perceives their environment differently, comprehends those perceptions differently, and draws upon different experiences when contemplating future actions. As emphasized by Dr. Endsley, "the key here is the understanding that true situation awareness only exists in the mind of the human operator."[46] Further, basic data collection varies based on assigned task. As previously noted, aircrews require airspeed, attitude, and altitude among other data points for aircraft situational awareness. Meanwhile, back in their squadron, commanders, mission planners, and schedulers need insight into varying applications, databases, and communication links that facilitate their respective functions. Alternatively, medical forces utilize a largely different suite of resources thereby needing different data points for situational awareness. As a result, far from one size fits all or even centrally managed SA solutions, a more realistic scenario for cyberspace SA involves individuals tailoring data collection and presentation to their own needs *then* leveraging commonality, where it exists, in the roll-up aggregation from tactical to operational to strategic levels.

Incremental Development of Tactical SA Tools

In pursuit of comprehensive situational awareness tools that provide Level-3 insight across large spans of cyberspace, smaller scoped, incremental steps, as taken by MCP/C2RMS, present a prudent approach. Level-1 SA is a prerequisite for Level-2 SA which is a perquisite for Level-3 SA.[47] In light of the present lack of SA regarding much of cyberspace, implementation of the Level-1 SA "low hanging

fruit" reaps significant forward progress. Quantifying the operator's or commander's sphere of concern, thus answering simple questions of how many, where, and who, is a logical starting point. Next, mapping the results to identifiable resources facilitates prioritization of resources or assignment of other measures of significance. Finally, resource monitoring in the context of operator assigned parameters yields meaningful insight for resource to task and mission impact situational awareness. In many ways this was the formula for success for MCP/C2RMS. The CAOC is a scoped weapons system with established dependencies. Systems, tactics, and experience-based knowledge evolved such that MCP/C2RMS provides tactically oriented SA to the operators of a very significant, operationally oriented weapons system. In a similar fashion, near term cyberspace situational awareness efforts should be tactically oriented, focused first on specific needs, and then incrementally expanded to address larger numbers of programs or systems and their associated operators.

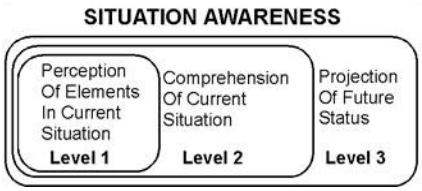

Figure 2 Levels of SA[47]

Keep in mind, tactically oriented cyberspace situational awareness tools do not exclude utility at higher headquarters echelons. Red-Yellow-Green "stoplight" charts are a popular tool used at all levels to depict operational status of the network. Information derived from these charts typically contributes to Level-1 SA with little benefit towards achieving the ultimate goal of Level-2 and Level-3 SA.[48] However, tactically oriented, Level-1 SA tools like these are essential to operators, units, wings, and even the Integrated Network Operations and Security Center.[49] Starting with a tactical focus simplifies implementation and satisfies the Level-1, then 2, then 3 prerequisite of the SA process. Incremental growth from the bottom up also leverages commonalities that may become evident as part of the aggregation process. Even with SA dependent upon the eyes of the beholder, many tasks and functions of a bomber squadron will closely match those of a fighter, tanker, or airlift squadron. Similarly, tasks and functions of Air Combat Command wings will share commonality with Air Mobility Command wings. Thus, when resource to task and mission mappings are aggregated common threads will emerge providing logical focus areas for higher-level situational analysis utilities.

Learning through Iterative Identification, Mapping and Prioritization

The central feature of the inferred bottom up, tactically oriented, situational awareness framework is an iterative identification, mapping, and prioritization of resources and their parameters by the operator. This iteration begins with a learning period of identifying information resources and monitoring basic characteristics. Doing so not only quantifies number and location or linkage of resources, it helps establish the Level-1 SA foundation required for the higher level SA goals such as mission impact assessment.

Figure 3 Iterative Identification, Mapping, Prioritization Process

In the context of cyberspace, data is information in numerical form that can be digitally transmitted or processed.[50] Further, data that provides information about other data, known as metadata, often facilitates data transmission or processing.[51] As a result, basic metadata already present within cyberspace to facilitate network communication divulges much about the data itself. As an example, application level network protocols identify data objects as email messages, webpages, web-based transactions, remote terminal commands, or even telephone calls.[52] Further transport and network layer protocol headers provide insight into the source and destination of the data.[53] Thus, having no *a priori* knowledge of an IT architecture and without interrogating the data (which may often be precluded by encryption), an automated system can construct a mapping of data flows by reading and storing appropriate metadata fields.[54] Further, to simplify the many-to-many correlation of operators and resources to a one-to-many problem, data flow tables could be generated at the user/operator level and aggregated upward. Over time, an operator's flow table will include every resource they utilize in the performance of their duties.

The next step involves human interaction to refine this basic discovery of data flows into a meaningful, manageable list of resources linked to operational tasks and capabilities.[55] Resources such as email will be readily identifiable with Post Office Protocol 3, Internet Message Access Protocol, and Simple Mail Transport Protocol messages communicated to/from local Internet Protocol (IP) addresses

and the singular or small number of IP addresses of the mail server(s).[56] In contrast resolving Hypertext Transport Protocol web pages and web-based transactions is more involved. Even though web traffic will concentrate around a quantifiable set of destination addresses, further data mining or human intervention is needed to map websites to mission related resources. Fortunately, once the initial task of identifying IP address (136.149.54.22) and hostname (ask.afpc.randolph.af.mil) with resources (the Air Force Personnel Center) is accomplished, maintenance of the mapping is much easier.[57] Web server addresses are reasonably static, and when they do change, updates are easily retrieved from the Domain Name System.[58] Alternatively, the evolving distributed SA tool could reference one or more central lookup tables containing previously resolved destination to resource to task mappings. Akin to first identifying airspeed, attitude, and altitude as data points for aircraft SA, the resulting resource list provides a baseline set of data points from which to build Level-1 cyberspace SA. Further, since the list is generated based on operator activity, it is inherently constrained to their sphere of concern.

At this point in the iterative process, one can make a binary assessment of the overall relationship between resources and missions; a given system resource either was or was not utilized. Trend analysis and optional additional parameters add fidelity to this otherwise binary relationship. Basic trend analysis tracks resource use over time which yields utilization as one example parameter for cyberspace SA. In its simplest form, frequently used resources imply greater importance than infrequently used resources. Though this may not always hold true, it's a baseline assumption for later adjustment by the operator when prioritizing resources and/or parameters. Also, in addition to frequency of use, recency of use, peak and low usage periods, intervals between use, and other time-based measures are easily extracted from resource utilization analysis. Of greater importance is the potential for Level-2 SA implied from the comparison and understanding of actual utilization values relative to expected goals. For example, extraordinarily high or low actual use may motivate the operator to reconsider priority of that resource relative to others.

Ultimately, operator intervention is required to prioritize resources and parameters. Consider a simplified scenario with utilization being the only parameter observed over a set of ten resources found in

an aircraft operations unit. Following the assumption that greater utilization implies higher priority, automated analysis can produce a ranked ordering of resources based on the operator's actions. Logically, different operators with varying functions will use different resources and therefore witness different initial prioritizations from the analysis. Operator interaction then either confirms the automated analysis or adjusts the rank ordering based on desired feedback and their experience regarding the relationship between resources, tasks, and mission. Expanding the scenario to include other parameters, the operator adjusts each parameter accordingly tailoring the system to their needs. For example, voice and instant messaging communications may be of utmost importance to a commander while a mission planning application or scheduling database warrant top priority from personnel providing those functions as depicted below. It follows that operators would prefer more frequent status polls or, better yet,

Notional Resource/Application Priorities for Different Operators/Functions

Command & Control	**Mission Planning**	**Aircraft & Aircrew Scheduling**
1. VOIP Telephone	1. Application (PFPS)	1. Web App (PEX)
2. Internet Chat	2. Email	2. Database (ARMS)
3. Web App (TBMCS)	3. Web App (TBMCS)	3. Web App (TBMCS)
4. Email	4. Internet Chat	4. Email
5. Web App (PEX)	5. VOIP Telephone	5. Database (CAMS)
6. Database (CAMS)	6. Web App (PEX)	6. VOIP Telephone
7. Database (ARMS)	7. Database (CAMS)	7. Application (PFPS)
8. Database (LogMod)	8. Database (ARMS)	8. Internet Chat
9. Resource (WWW)	9. Database (LogMod)	9. Resource (WWW)
10. Application (PFPS)	10. Resource (WWW)	10. Database (LogMod)

System/Resource	**Function(s)/Contribution to Mission**
ARMS – Aviation Resource Management System	Aircrew currencies, qualifications, flying hours, training
CAMS – Core Automated Maintenance System	Aircraft maintenance status
Email	Command & control, Coordination, Morale
Internet Chat	Command & control, Time-sensitive coordination
LogMod – Logistics Monitor	Deployment processing (equipment, personnel, aircraft)
PEX – Patriot Excalibur	Unit level aircraft and aircrew scheduling
PFPS – Portable Flight Planning System	Collaborative mission planning (routing, weapons, etc.)
TBMCS – Theater Battle Management Core System	Wing and higher echelon coordination
VOIP – Voice Over Internet Protocol	Telephone command & control and coordination
WWW – World Wide Web	General reference information, Morale

Figure 4 Notional Resource/Application Priorities for Different Operators/Functions

threshold based alerts for higher priority resources with less concern regarding lower priority resources. Alternatively, a particular resource may be infrequently used but critically important when needed requiring operator judgment on how it and its reporting criteria should be prioritized relative to other

resources. With operator inputs incorporated, the iterative processes of identifying, mapping, and prioritizing resources and parameters then repeats. Using this iterative process, the automated tool "learns" directly from the operator in place of the operator or a third party manually performing an a priori analysis to configure and maintain the resource-to-task and-mission relations. This offers the greatest scalability to accommodate the vast combinations of software applications, cyber resources, and associated operators.

Further Fidelity from Additional Parameters

As previously mentioned, interrogating additional parameters of cyberspace resources, with trend analysis of those parameters, provides supplementary input for Level-1 and hopefully higher levels of SA. For example, round trip time analysis, which also may be gleaned from metadata already included in IP network data streams, offers insight into resource latency.[59] As an alternative to metadata inherent in networking protocols, other metadata, either embedded within the data or explicitly added for situational awareness, could also enhance SA. Here in lies the challenge, determining the what, where, when, why, and how of supplementing raw data with metadata in order to improve situational awareness. If implemented haphazardly, rather than having little to no data from which to infer situational awareness, data overload looms as the polar opposite threat to cyberspace situational awareness. Suffice it to say the right data is useful while the wrong data adds noise; for now assume the right data is added and available for analysis.

Without delving into metadata selection and implementation details, there are numerous characteristics that may be tracked and presented to the operator for insight regarding resources and increased fidelity to mission impact valuations. Priority of service, for example, may be a significant factor under low bandwidth or high congestion conditions. General privilege levels are also useful for prioritization or inclusion/exclusion decisions. Similarly, security classification and chain of command are instantiations of privilege levels with similar discriminating utility. The age of information relating its half-life or other temporal relevance has bearing on latency thresholds and could factor into priority of service assessments. Assuming agreement on how they are measured, confidentiality, integrity, and

availability parameters would surely be useful discriminators. The point is that cyberspace situational awareness tools could present a very simple (based on utilization or some other single parameter) or complex assortment of resource to task and mission relationships to be critiqued and adjusted by the operator.

From Iteration to Display

Iterative adjustments to resource parameters and priorities, basic data collection and reporting settings, and task to mission priority relationships result in operator tailored changes to the feedback provided by SA tools. In a sense, the operator could have a situational awareness multifunction display (MFD) that they can configure to suit their needs. Like an aircraft MFD, available data fields depend on system wide instrumentation, display options are variable but finite, and even though different aircraft or aircrew members may share the same avionics, the "best" display for situational awareness often changes based on the mission or task at hand. In the AOC, the MCP/C2RMS suite provides the cyberspace MFD. On the horizon, an SA tool that iteratively derives the identification, mapping, and prioritization of resources and associated parameters from everyday Airmen as operators could provide a similar tactically oriented MFD to units, wings, and elsewhere. Many of its implementation details, to include use of military and industry standards, COTS and GOTS technology, and agent based data mining could and should mirror MCP/C2RMS. The key difference between the two being the central KMS knowledge base configured and maintained by systems administrators in MPC/C2RMS verses distributed resource to task and mission valuations adjusted by the operator.

Conclusion

Today, Airmen are more dependent on cyberspace, the Global Information Grid, and thousands of software applications to accomplish our daily tasks and missions than ever before. Implied from this, each of us is an operator in cyberspace who must adopt a weapons system mindset towards the systems and resources we depend on.[60] Like other traditional weapons systems, we need tactical cyberspace situational awareness tools that facilitate common operating pictures just like every other domain.[61] The MCP/C2RMS suite is a mature example of this needed capability providing SA to operators of the

Falconer weapons system. It represents a huge step forward with many lessons applicable towards development of other SA capabilities outside of the AOC. However, given the large number of systems used by even larger number of operators, each with their own view of situational awareness, a distributed learning model provides a scalable foundation for tactically oriented SA tools. From such tools, operators, administrators, and commanders in units, wings, and headquarters can develop basic Level-1 SA and then address higher levels of situational awareness as tools mature.

---

1. General Norton A. Schwartz, Chief of Staff of the Air Force, "Cyberspace Operations Culture Change", email 27 May 2009.

2. General Kevin P. Chilton, "Cyberspace Leadership", *Air & Space Power Journal* (Fall 2009), 1 September 2009, http://www.airpower.au.af.mil/airchronicles/apj/apj09/fal09/chilton.html (accessed 29 Sep 2009).

3. Jeffrey E. Stanley, Robert F. Mills, Richard A. Raines, and Rusty O. Baldwin, "Correlating Network Services With Operational Mission Impact", Military Communications Conference, 2005, 17-20 October 2005, 162-168.

4. General Norton A. Schwartz, "Cyberspace Operations Culture Change".

5. Mica R. Endsley, "Design and Evaluation for Situation Awareness Enhancement", Proceedings of the Human Factors Society 32nd Annual Meeting, (Santa Monica, CA, 1998), 97-101.

6. Mica R. Endsley, "Designing for Situation Awareness in Complex Systems", Proceedings of the Second international workshop on symbriosis of humans, artifacts, and environment, (Kyoto Japan, 2001) 1-13.

7. Major Lee E. Chase, "Integration of Cyberspace Situational Awareness Into System Design and Development" (Graduate Research Paper, AFIT/ISE/ENV/09-J02, Air Force Institute of Technology, Wright-Patterson AFB, OH, 18 Jun 2009), 11-20.

8. Mica R. Endsley, "Designing for Situation Awareness in Complex Systems", 1-13.

9. Ibid.

10. Ibid.

11. General Kevin P. Chilton, "Cyberspace Leadership".

12. Mica R. Endsley, "Designing for Situation Awareness in Complex Systems", 1-13.

13. General Kevin P. Chilton, "Cyberspace Leadership".

14. United States Air Force Fact Sheet, "E-4B", http://www.af.mil/information/factsheets/factsheet.asp ?fsID=99, (accessed 24 November 2009).

15. United States Air Forces Central website, http://www.centaf.af.mil/units/caoc/index.asp, (accessed 24 November 2009).

16. Air Force Operational Tactics, Techniques, and Procedures 2-3.2, *Air and Space Operations Center*, 13 December 2004.

17. Jodi L. Jordan, "Orchestrating excellence: 505th Operations Squadron trains behind the scenes", *Air Force Print News*, 2 Feb 2009, http://www.505ccw.acc.af.mil/news/story_print.asp?id=123134674 (accessed 29 November 2009).

18. Basil Jos and Tracy Culbertson, "Leveraging Net-Centric Monitoring Techniques with Information Fusion to Increase US Air Force Information Dominance", Military Communications Conference, 2006, 23-25 October 2006, 1-6.

19. Ibid.

20. Ibid.

21. Ibid.

22. Ibid.

23. Craig McFarland and Basil Jos, "Leveraging the Command and Control Resource Management System to Enhance Collaboration with the Air Operations Center", Collaborative Technologies and Systems, 2008, 19-23 May 2008, 174-180.

24. Basil Jos and Tracy Culbertson, "Leveraging Net-Centric Monitoring Techniques with Information Fusion to Increase US Air Force Information Dominance", 1-6.

25. Craig McFarland and Basil Jos, "Leveraging the Command and Control Resource Management System to Enhance Collaboration with the Air Operations Center", 174-180.

26. Basil Jos and Tracy Culbertson, "Leveraging Net-Centric Monitoring Techniques with Information Fusion to Increase US Air Force Information Dominance", 1-6.

27. Ibid.

28. General Norton A. Schwartz, "Cyberspace Operations Culture Change".

29. General Kevin P. Chilton, "Cyberspace Leadership".

30. Craig McFarland and Basil Jos, "Leveraging the Command and Control Resource Management System to Enhance Collaboration with the Air Operations Center", 174-180.

31. Ibid.

32. Ibid.

33. Basil Jos and Tracy Culbertson, “Leveraging Net-Centric Monitoring Techniques with Information Fusion to Increase US Air Force Information Dominance”, 1-6.

34. Tim O’Reilly, “What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software”, http://oreilly.com/lpt/a/6228 (accessed 3 December 2009).

35. San Murugesan, “Understanding Web 2.0”, *Information Technology Professional* 9, no. 4, July-August 2007, 34-41.

36. Basil Jos and Tracy Culbertson, “Leveraging Net-Centric Monitoring Techniques with Information Fusion to Increase US Air Force Information Dominance”, 1-6.

37. Craig McFarland and Basil Jos, “Leveraging the Command and Control Resource Management System to Enhance Collaboration with the Air Operations Center”, 174-180.

38. Ibid.

39. Basil Jos and Tracy Culbertson, “Leveraging Net-Centric Monitoring Techniques with Information Fusion to Increase US Air Force Information Dominance”, 1-6.

40. Ibid.

41. Staff Sergeant C. Todd Lopez, “IT modernization: Leveraging the power of information”, *Air Force Print News*, 22 May 2006, http://www.af.mil/news/story_print.asp?id=123020655 (accessed 16 November 2009).

42. Ibid.

43. Ibid.

44. United States Air Force Fact Sheet Index, http://www.af.mil/information/factsheets/index.asp, (accessed 3 December 2009).

45. United States Air Force Fact Sheet Index, http://www.af.mil/information/factsheets/index.asp, (accessed 3 December 2009).

46. Mica R. Endsley, “Designing for Situation Awareness in Complex Systems”, 1-13.

47. Mica R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems”, Human Factors, 37(1) (March 1995), 32-64.

48. Major Lee E. Chase, “Integration of Cyberspace Situational Awareness Into System Design and Development”, 24-25.

49. Air Intelligence Agency Public Affairs, “Air Force stands up first network warfare wing”, *Air Force Print News*, 5 July 2006, http://www.af.mil/news/story_print.asp?id=123022799 (accessed 4 December 2009).

50. Merriam-Webster online, “data”, http://www.merriam-webster.com/dictionary/data (accessed 17 November 2009).

51. Merriam-Webster online, "metadata", http://www.merriam-webster.com/dictionary/metadata (accessed 17 November 2009).

52. James F. Kurose and Keith W. Ross, *Computer Networking: A Top Down Approach,* 5th ed., (Addison-Wesley, Boston, MA, © 2010 Pearson Education, Incorporated), 97, 133, 198, 204, 213, 246.

53. Ibid.

54. Jeffrey E. Stanley, Robert F. Mills, Richard A. Raines, and Rusty O. Baldwin, "Correlating Network Services With Operational Mission Impact".

55. Ibid.

56. Kurose and Ross, *Computer Networking: A Top Down Approach,* 97, 133, 198, 204, 213, 246.

57. Author's analysis of network traffic to/from http://ask.afpc.randolph.af.mil/ on 17 November 2009 using the Wireshark network protocol analyzer (http://www.wireshark.org/about.html).

58. Kurose and Ross, *Computer Networking: A Top Down Approach,* 97, 133, 198, 204, 213, 246.

59. Kurose and Ross, *Computer Networking: A Top Down Approach,* 97, 133, 198, 204, 213, 246.

60. General Norton A. Schwartz, "Cyberspace Operations Culture Change".

61. General Kevin P. Chilton, "Cyberspace Leadership".

Lieutenant Colonel David C. Bares is a Graduate Cyber Operations student at the Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio. Lt Col Bares initially served as a Computer Developmental Engineer at Los Angeles Air Force Base for the Defense Dissemination Program, National Imagery and Mapping Agency, and Space and Missile Systems Center Developmental Planning Office. He then went through Joint Undergraduate Navigator Training at Naval Air Station Pensacola eventually becoming a B-52H Instructor Radar Navigator stationed at Minot Air Force Base. He flew combat missions over Afghanistan and Iraq in 2002 and 2003 respectively and was later deployed to Afghanistan as the Bomber Liaison Officer in 2005. Prior to attending AFIT, Lt Col Bares served as an Instructor/Evaluator Mission Commander/Deputy Team Chief with the Defense Threat Reduction Agency performing Open Skies aerial missions in the OC-135B, C-130, Saab 100, AN-30B, and AN-26 over Russia, Europe, and North America.

Doctor Robert F. Mills (Ph.D.) is an Associate Professor of Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. He teaches graduate courses and directs research in support of AFIT's cyber operations and warfare program. His research interests include

network management and security, communications systems, cyber warfare, and systems engineering. He is a member of Tau Beta Pi and Eta Kappa Nu, and is a Senior Member of the IEEE. He retired from active duty as a Lieutenant Colonel after serving 21 years in the United States Air Force.

Major Eric D. Trias (Ph.D.) is an Assistant Professor of Computer Science in the Department of Electrical and Computer Engineering at AFIT, Wright-Patterson AFB, Ohio. He enlisted in 1988 and was nominated for the Air Force Twelve Outstanding Airmen of the Year award in 1994. In 1998 he received his commission through the Airman's Education and Commissioning Program and Officer Training School. As a communications officer, he has served operationally at Osan Airbase and Camp Humphreys Army Installation, Republic of Korea, and at the Distributed Mission Operations Center, Kirtland Air Force Base, New Mexico. He is a graduate of Squadron Officer School and Air Command and Staff College. Major Trias' current research interests include knowledge discovery and data mining, information systems security, digital forensics, and various cyberspace-related topics.