A Tactical Framework for Cyberspace Situational Awareness

Lt Col David C. Bares
Student, AFIT GCO 11M

Overview

- US Air Force Culture Change
- Situational Awareness (SA) Defined
- SA in the Air & Space Operations Center
  - Master Caution Panel (MCP)
  - Command & Control Resource Monitoring System (C2RMS)
- Implications of being an Major Weapons System
- Scalable, Distributed SA Tool
- Notional Resource Mappings & Parameters
- Conclusion

USAF Culture Change

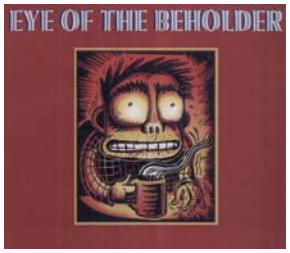
"Cyberspace operations reinforce and enable everything we do – from administrative functions to combat operations – and we must treat our computers and networks similarly to our aircraft, satellites, and missiles."
– General Norton A. Schwartz, Chief of Staff, USAF

1. Software programs & cyberspace resources should be treated as weapons systems.
2. As Airmen we are cyberspace operators
3. We need situational awareness in cyberspace just like any other traditional weapons system

"We also need common operating pictures, just like the ones demanded by commanders in every other domain."
– General Kevin P. Chilton, Commander, USSTRATCOM

Situational Awareness (SA)

- Situational Awareness = "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."[1]
- SA = the operator's mental model of the current state of their environment.[2]
- "true situation awareness exists only in the mind of the human operator".[2]
- SA is in the 'eye of the beholder'.



1. 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.
2. 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.

Levels of SA

- Level-1 *Perception* ≈ Tactical
- Level-2 *Comprehension* ≈ Operational
- Level-3 *Projection* ≈ Strategic

1. 
2. Low airspeed
   Low altitude
   High angle of attack
3. Dangerous stall condition, recover!

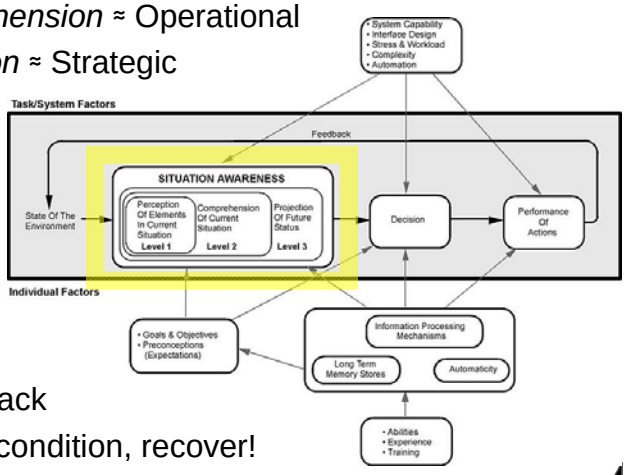
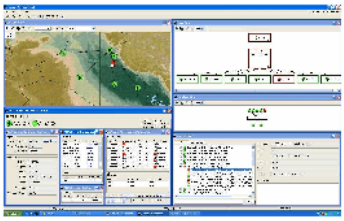


Image used with permission of author: Mica Endsley, Ph.D., President, SA Technologies. Adapted from the following source: 3. Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems".

SA in the AOC

- The AN/USQ-163 "Falconer" weapon system, Air & Space Operations Center (AOC), provides command & control over conventional airpower.*
- SA to AOC operators, commanders, and administrators facilitated by Master Caution Panel (MCP) / Command & Control Resource Management System (C2RMS).[4 & 5]

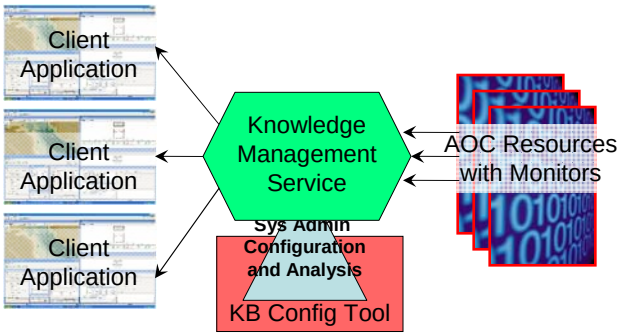


* http://www.centaf.af.mil/units/caoc/index.asp

4. B. Jos and T. Culbertson, "Leveraging Net-Centric Monitoring Techniques with Information Fusion to Increase US Air Force Information Dominance"
5. C. McFarland and B. Jos, "Leveraging the Command and Control Resource Management System to Enhance Collaboration with the Air Operations Center".

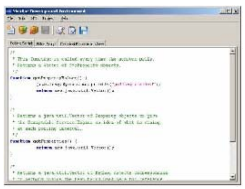
MCP / C2RMS

- Monitors reside on AOC resources reporting to KMS
- Knowledge Management Service (KMS) consolidates resource status and reports
    1. Each resource and its status
    2. How configured tasks are affected by resource status
- Client Applications display resource/task details as tailored by Knowledge Base (KB) Configuration Tool



C2RMS Pros & Cons

+ Provides SA to operators, administrators, commanders
+ Leverages military and industry standards…
    + Java 2 Enterprise Edition (J2EE) specification
    + Java Messaging System (JMS) specification
    + Java Database Connectivity (JDBC) compliant
    + Information Secure Support Environment (ISSE) Star Guard
    + Simple Network Management Protocol (SNMP)
+ Flexible and expandable, incrementally added…
    + Airborne networks
    + Mapping and Digital Terrain Elevation Data (DTED)
    + Monitor Development Kit (MDK)
    + Joint Weather Impact System (JWIS)
+ Relates systems to operational tasks
- Dependent upon system administrator / a-priori analysis



Implications of being a MWS

19,000 software applications in 2006

Targeting 2000 applications by FY2012

vs.

46 aircraft major weapons systems (MWS)

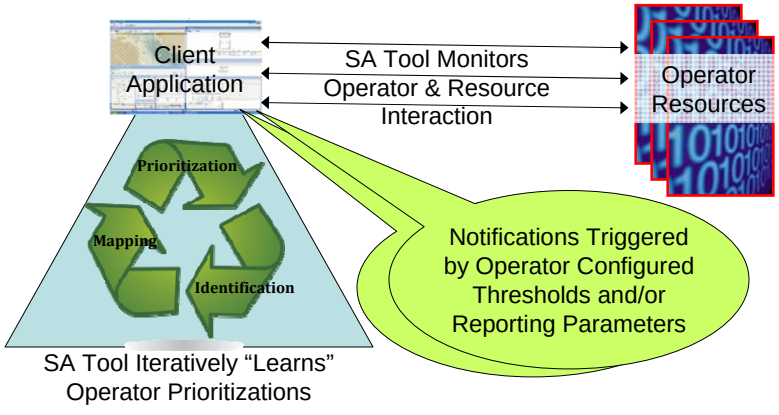
<150 “traditional” MWSs including space, unmanned aerial systems, and “weapons”

* http://www.af.mil/information/factsheets/index.asp

Distributed SA Tool

- Agent monitors resource & SA metadata
- Operator driven iterative “learning” …

  Identification → Mapping → Prioritization
- Operator tailors data collection & reporting parameters.



Notional Mappings

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

Fidelity Parameters

Objective Criteria

- Recency of Use
- Frequency of Use
- Latency
- Data Volume

Subjective Criteria

- Priority of Service
- Privilege Level
- Temporal Relevance
- Confidentiality
- Integrity
- Availability
- Polling Frequency
- Alert Threshold

Conclusion

- Airmen are dependent upon cyberspace
- Airmen need cyberspace situational awareness tools
- The MCP/C2RMS suite is a great start
- Large number of systems/resources
  + **Larger** number of operators/views of SA
  = Scalable, distributed learning model
- Develop tactical SA tools first
- *Then* aggregate upward and develop higher level SA

Significant References

1. 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.
2. 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.
3. Mica R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems”, Human Factors, 37(1) (March 1995), 32-64.
4. 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.
5. 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.
6. Mica R. Endsley, “Theoretical Underpinnings of Situation Awareness: A Critical Review”, *Situation Awareness Analysis and Measurement*, (© 2000 Mahwah, NJ: Lawrence Erlbaum Associates), 3-32, http://zonecours.hec.ca/documents/A2007-1-1399574.TheoricalUnderpinningsofSituationAwareness_ACriticalReview.pdf .
7. Air Force Doctrine Document 3−12, *Cyberspace Operations (DRAFT)*, xx Mar 2010.
8. Air Force Operational Tactics, Techniques, and Procedures 3−3.AOC, *Operational Employment - Air and Space Operations Center*, 1 November 2007.
9. 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, 24-25.
10. Marc Grégoire and Luc Beaudoin, “Visualisation for Network Situational Awareness in Computer Network Defence”, http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-IST-043///MP-IST-043-20.pdf
11. 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.

Questions? (points to ponder)

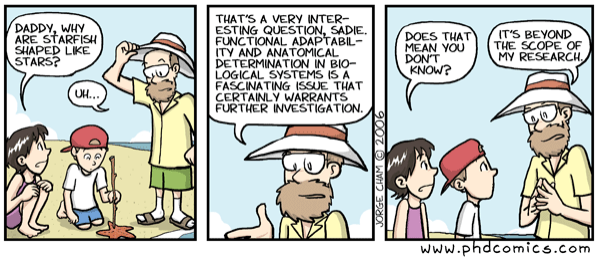
What is mission assurance?

What constitutes FMC-PMC-NMC in cyberspace?

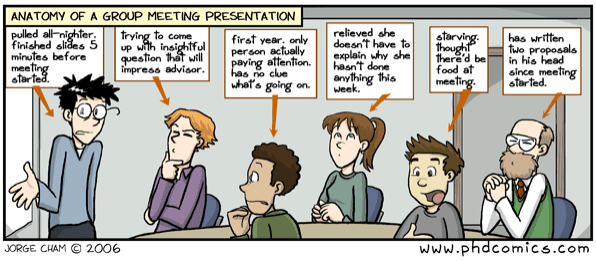
Are-there / what-are acceptable thresholds of confidentiality, integrity, and availability below100%?

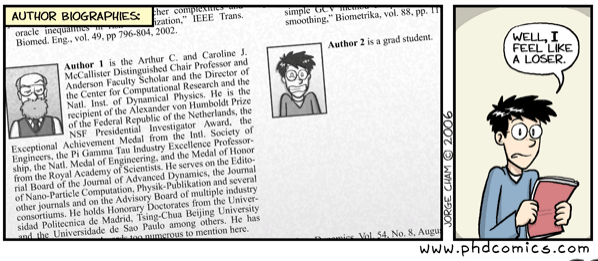
How do you design tools that satisfy my SA needs?

How do we migrate to a common mental model regarding cyberspace/cyber SA?



Thank you





…NOT true, but a little funny (for those who can relate).