17th ICCRTS
"Operational C2 Agility"

Humans and Their Impact on Cyber Agility

Topic #1: Concepts, Theory, and Policy

By: Dr. Paul W. Phister, Jr.

AF Research Laboratory, Information Directorate
AFRL/RIZ
Chief, Special Programs Division
525 Brooks Road, Suite C-6, Rome, NY 13441-4514
paul.phister@rl.af.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Humans and Their Impact on Cyber Agility	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **AF Research Laboratory, Information Directorate,AFRL/RIZ,525 Brooks Road, Suite C-6,Rome,NY,13441-4514**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 17th International Command & Control Research & Technology Symposium (ICCRTS) held 19-21 June, 2012 in Fairfax, VA.

14. ABSTRACT

Autonomous operations are the best way to operate in cyberspace. Six variables are appropriate with respect to cyber agility, namely: robustness, resilience, responsiveness, flexibility innovation, and adaptability. This paper explores the role of humans and their impact on cyber agility. It is envisioned that there are four basic ways a human can interact with the ?loops? associated with cyber C2 systems, namely: Human-BEFORE-, Human-ON-, Human-IN-, and Human-AFTER-the-Loop. These interactions can have significant impacts regarding mission success and these interactions will play a major role when considering the complex nature of the human during the six phases of conflict. Net-enabled approaches have the potential to be more agile in the cyber domain simply because it?s more machine-to-machine oriented. The role of humans within cyberspace definitely is related to the particular mission. It is postulated that: a) Human-BEFORE-the-Loop will perform better in discovery and prediction; b) Human-ON-the- Loop is best when periodic injection of decisions are required; c) Human-IN-the-Loop is best when time is not a critical factor for mission success; and, d) Human-AFTER-the-Loop is best during the assessment phase of operations. It is postulated that, again, Human-IN-the-Loop would display the least cyber agility as compared to the other three.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**43**	

Abstract

Autonomous operations are the best way to operate in cyberspace. Six variables are appropriate with respect to cyber agility, namely: robustness, resilience, responsiveness, flexibility, innovation, and adaptability. This paper explores the role of humans and their impact on cyber agility. It is envisioned that there are four basic ways a human can interact with the "loops" associated with cyber C2 systems, namely: Human-BEFORE-, Human-ON-, Human-IN-, and Human-AFTER-the-Loop. These interactions can have significant impacts regarding mission success and these interactions will play a major role when considering the complex nature of the human during the six phases of conflict. Net-enabled approaches have the potential to be more agile in the cyber domain simply because it's more machine-to-machine oriented. The role of humans within cyberspace definitely is related to the particular mission. It is postulated that: a) Human-BEFORE-the-Loop will perform better in discovery and prediction; b) Human-ON-the-Loop is best when periodic injection of decisions are required; c) Human-IN-the-Loop is best when time is not a critical factor for mission success; and, d) Human-AFTER-the-Loop is best during the assessment phase of operations. It is postulated that, again, Human-IN-the-Loop would display the least cyber agility as compared to the other three.

Introduction

Command and Control (C2) is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.[1] A command and control system is the facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the missions assigned.[2] Recently, within the C2 Joint Capability Area, the DoD has delineated C2 into Tier 1 and Tier 2 as follows (Pontius 2011, Slide 4)[3]:

a. Tier 1:

> C2: The ability to exercise authority and direction by a properly designated commander or decision maker over assigned and attached forces and resources in the accomplishment of the mission.

b. Tier 2:

> 1. Organize: The ability to align or synchronize interdependent and disparate entities, including their associated processes and capabilities to achieve unity of effort
>
> 2. Understand: The ability to individually and collectively comprehend the implications of the character, nature, or subtleties of information about the environment and situation to aid decision-making
>
> 3. Planning: The ability to establish a framework to employ resources to achieve a desired outcome or effect
>
> 4. Decide: The ability to select a course of action informed and influenced by the understanding of the environment or a given situation
>
> 5. Direct: The ability to employ resources to achieve an objective
>
> 6. Monitor: The ability to adequately observe and assess events/effects of a decision.

This process of C2 has worked within the air and space domains for decades; however, it is the position of the authors that this process does not work very well within the cyber domain when humans put themselves directly into the decision loop.

[1] Joint Pub on C2
[2] Joint Pub on C2

Within the net-centric warfare literature, there are six definitions applicable for this paper. They are:

a. Robustness: maintain effectiveness across a range of tasks, situations and conditions

b. Resilience: ability to recover or adjust to misfortune, damage or destabilizing perturbations

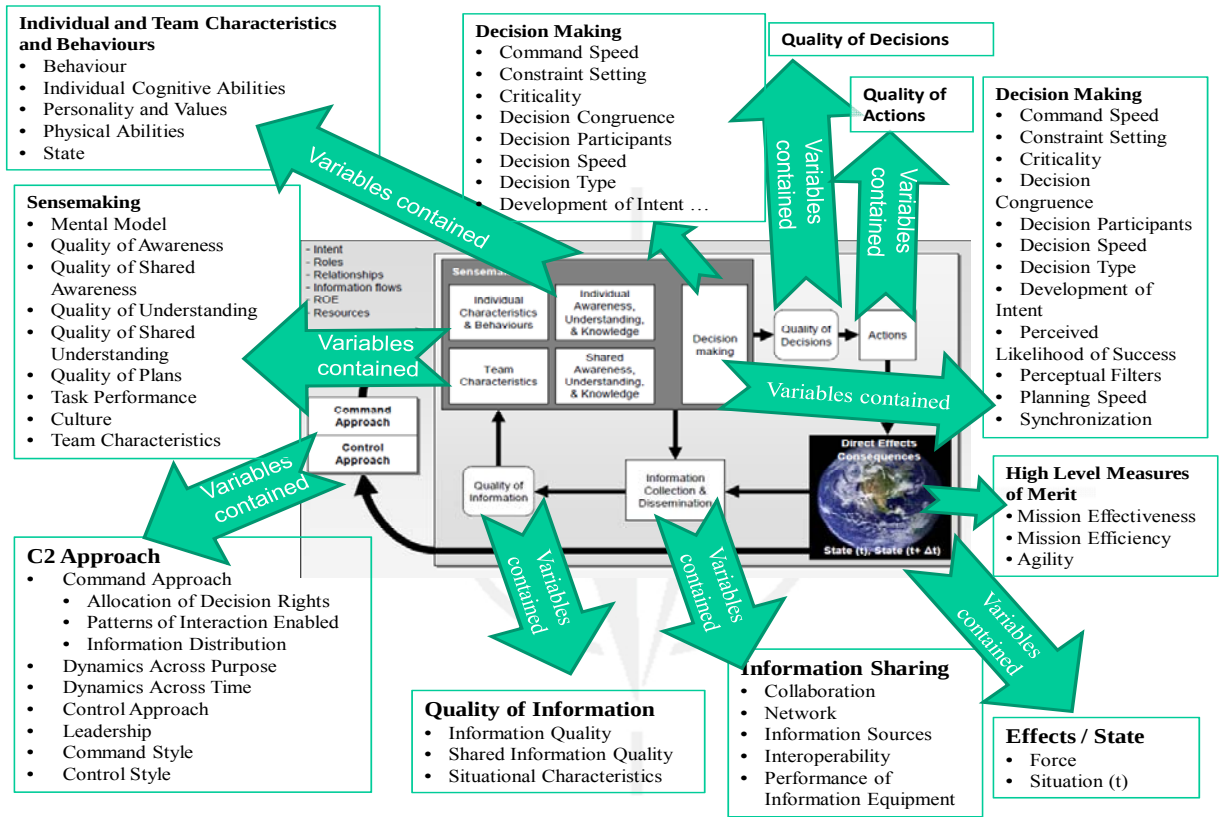
c. Responsiveness: ability to react to change in environment in timely manner

d. Flexibility: ability to employ multiple ways to succeed and ability to move between them

e. Innovation: ability to do new things and ability to do old things in new ways

f. Adaption: ability to change work processes and ability to change the organization

Additionally, as part of NATO's international C2 working groups (SAS-065 and SAS-085), there have been significant clarifications regarding the variables contained within the C2 Conceptual Reference Model[4] as shown in Figure 1. These variables were modified to better incorporate "C2 Agility" concepts.



[4] The C2 Conceptual Reference Model was originally developed as part of the NATO sponsored SAS-050 working group. All information is public releasable.

Figure 1: Value View of C2 Conceptual Reference Model and Underlying Variables[5]

C2 APPROACH SPACE

The C2 Approach Space is defined by three C2 dimensions. It describes possible approaches to accomplishing the functions associated with C2. It is described by means of the following three major axes (or dimensions of Command and Control) (Alberts & Hayes, 2010, p. 66):

- Allocation of Decision Rights (ADR),
- Patterns of Interaction (PI),
- Distribution of Information (DI).

The end goal is to approach what is termed an "edge" organization.

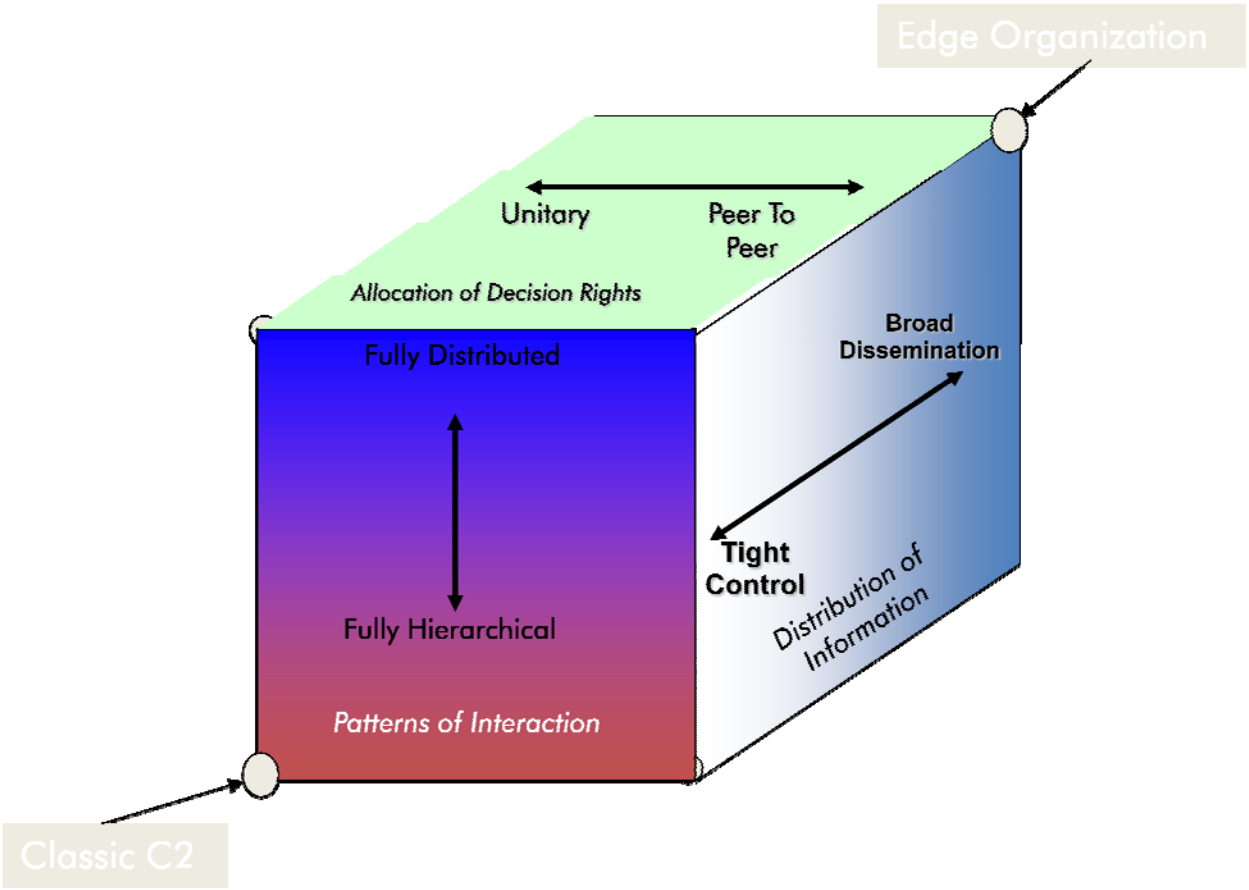


Figure 2: 3-Dimensional Approaches to Command and Control

ALLOCATION OF DECISION RIGHTS

"Decision rights belong to the individuals or organizations accepted (whether by law, regulation, practice, role, merit, or force of personality) as authoritative sources on the choices related to a particular topic under some specific set of circumstances or conditions. The allocation of

[5] Taken from SAS-065 non-published sections," Feb 2010. All information is public releasable.

decision rights is their distribution within the international community, a society, an enterprise, or an organization" such as "a military, a coalition, an interagency effort, or an international effort including military elements. There can be different distributions of those rights across functions, echelons, time, or circumstances." (Alberts & Hayes, 2010, p. 48).

PATTERNS OF INTERACTION

For Information Age networks, *Patterns of Interaction* is a C2 Key Dimension defined by means of three key elements:

- Reach (the number and variety of participants),
- Richness (the quality of the contents), and
- Quality of interactions enabled.

Understanding Patterns of Interaction requires focusing on more than just connectivity needs. It requires analysing:

- Level of interoperability achieved (more than technical interoperability, including also semantic interoperability and "cooperability" or willingness to interact and desire to communicate clearly).
- Range of media across which these interactions occur (e.g. voice, email, video conferencing and whiteboards)
- Collaborations (working together toward a common purpose)
- Digital connectivity

Information Age Patterns of Interaction are social networks enabled by whatever mechanisms are available (e.g. courier, telephone, videoconference, LAN, WAN, WWW) which mainly depend on cooperability, i.e., the willingness to work together and collaborate when appropriate (Alberts & Hayes, 2010, p. 48). When considering human responsiveness, Patterns of Interaction becomes the dominate C2 dimension.

DISTRIBUTION OF INFORMATION

The distribution of information across participating entities refers to the extent to which the information needed to accomplish required tasks is available to each participant. (Alberts & Hayes, 2010, p. 49)

Before we explore this concept in depth, some examples of "loops" are in order.

What is a "Loop?"

Generically a "loop" is defined as something that is folded over and joined at the too ends. It is a closed circuit. Within C2, the major loop is called the MAPE (Monitor-Assess-Plan-Execute) which is used to create an Air Tasking Order (ATO) to conduct air operations. Naturally, this is not a single "loop", but repetitive smaller loops (i.e. loops within loops) to accomplish the overall MAPE process. Some examples of "loops" are:

a. Complex Endeavor "Loop"

Conducting operations within the Cyber Domain is complex; especially when one considers the compressed timelines and the global players (military, civil, etc). The work that was accomplished under a NATO sponsored "C2 Agility" working group (SAS-065) was published under the CCRP Publication umbrella (Alberts and Hayes 2007, p123). Figure 3 summarizes the space that has become known as the "Endeavor Space." This is a multi-dimensional, multi-loop space that consists of a set of possible approaches that can be applied, known as the "Approach Space.[6]" Figure 3 illustrates the Complex Endeavor" Loop" (actually loops-within-loops) that is used within the "Endeavor Space" of operations.

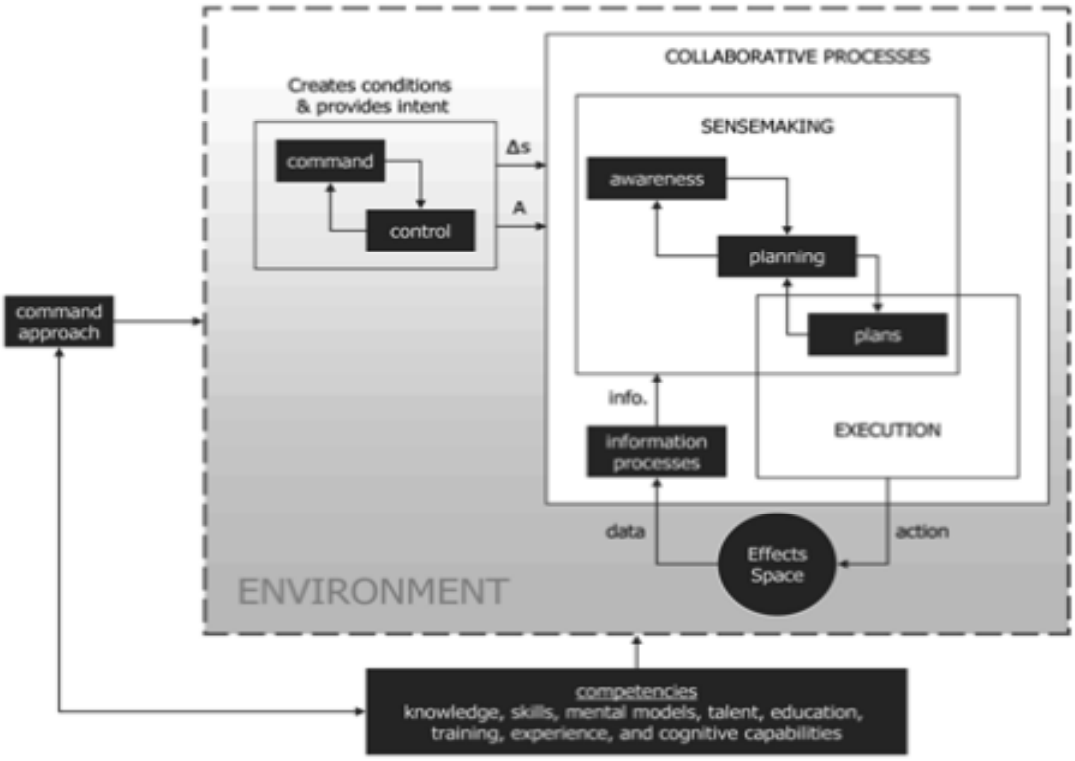


Figure 3: Complex Endeavor "Loop"

b. F2T2EA4 "Loop"

The F2T2EA4 (Find-Fix-Track-Target-Engage-Assess-Anything-Anytime-Anywhere) loop can also be termed the "sensor-to-shooter" loop that can find anything, anywhere and at anytime as shown in Figure 4. The concept of "sensor-to-shooter" is used within the Air Force as a targeting process within the ATO timeline. A key factor in this process is the timeline involved to be able

[6] Work currently being conducted by SAS-085.

to: a) obtain data/information; b) develop a shared awareness; c) develop a shared understanding; d) time to make a decision; and e) execution time. A generic timeline is presented in Appendix A.

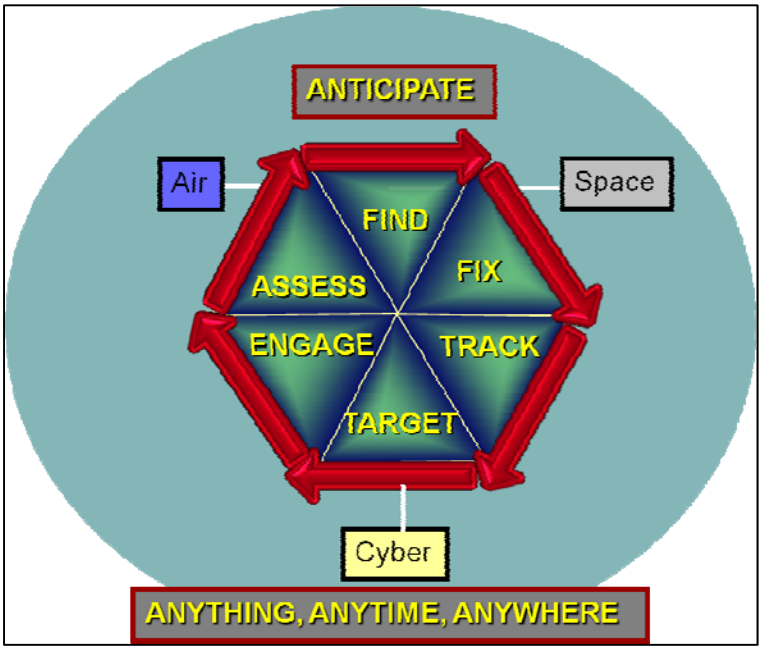


Figure 4: F2T2EA4 "Loop"

c. OODA "Loop"

A well known "loop" is the "Observe-Orient-Decide-Act" loop first developed by Boyd in the 1970s and is shown in Figure 5. Boyd developed the concept to explain how to direct one's energies to defeat an adversary and survive. Boyd emphasized that "the loop" is actually a set of interacting loops that are to be kept in continuous operation during combat. He also indicated that the phase of the battle has an important bearing on the ideal allocation of one's energies. Boyd hypothesized that all intelligent organisms and organizations undergo a continuous cycle of interaction with their environment. Boyd breaks this cycle down to four interrelated and overlapping processes through which one cycles continuously:[7]

- Observation: the collection of data by means of the senses
- Orientation: the analysis and synthesis of data to form one's current mental perspective
- Decision: the determination of a course of action based on one's current mental perspective
- Action: the physical playing-out of decisions

Boyd's diagram shows that all decisions are based on observations of the evolving situation tempered with implicit filtering of the problem being addressed. These observations are the raw information on which decisions and actions are based. The observed information must be processed to orient it for further making a decision.

[7] Information taken from en.wikioedia.org/wiki/OODA_loop.

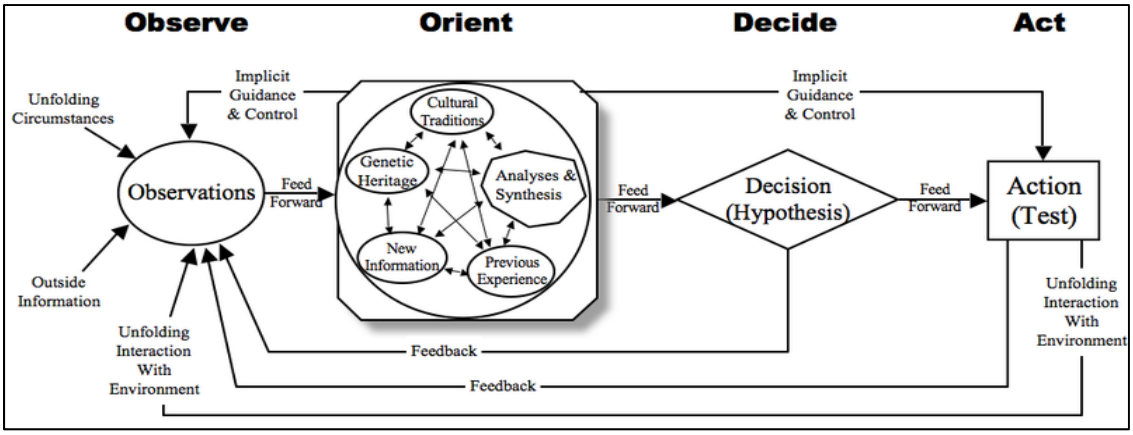


Figure 5: Observe-Orient-Decide-Act "Loop"

d. Prevent-Detect-Survive-Recover "Loop"

Within the cyber domain, there is a "protect-detect-survive-recover" loop as shown in Figure 6. Given a particular threat, the C2 system needs to:

1. "Prevent" the incursion of the threat into the C2 system (can be of various means, such as viruses, worms, etc.).

2. "Detect" all incursions into the C2 system early enough so that protective measures can be taken to minimize threat effects (D5[8] in reverse).

3. "Survive" the D5 effects incurred by an outside/inside threat in a timely manner.

4. "Recover" from a successful incursion by an outside/inside threat in a timely manner. The goal would be to be 100% back into mission in the shortest time possible.

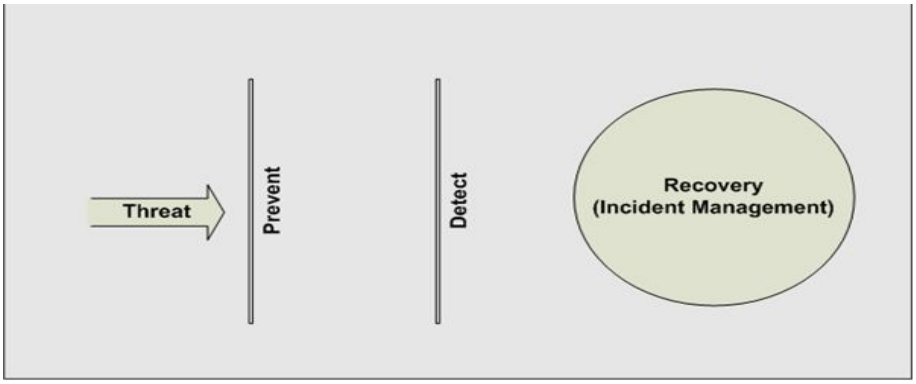


Figure 6: Protect-Detect-Survive-Recover "Loop"

[8] D5 stands for Deceive, Deter, Deny, Destroy and Degrade.

Human Interaction and "The Loop"

Figure 8 provides a graphical representation of the four basic ways a human can interact with a C2 system. It is important to note that interactions will play a major role when considering the complex nature of the human. These interactions are: human-to-human, human-to-machine, machine-to-human, and machine-to-machine.

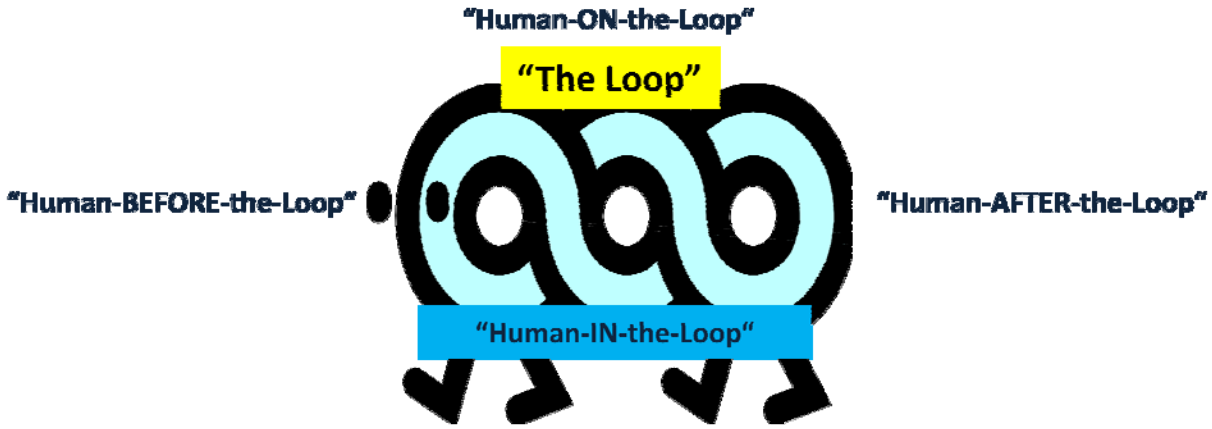


Figure 8: Human Relationship within "The Loop"

Fundamentally, it is envisioned that there are four basic ways a human can interact with a cyber C2 system in the performance of a particular mission. They are:

a. Human-BEFORE-the-Loop:

The area of "security agility" plays a role during this interaction phase. Considering coalition operations, "classify by default" vice share by default" needs to be the norm to improve "security agility."

1) Emphasis: "predictive" nature of potential courses-of-action.
2) Enabler: Flexibility and Innovation.
3) Applicable C2 Approach: Delegation of Decision Rights, Distribution of Information.
4) Timescales[9]: Days to Months

When considering INFOCON[10] as an example, the Human-BEFORE-the-loop would be responsible for developing necessary sets of COA depending on the conditions and what needs to be accomplished (or prediction) to protect computer architectures. Key aspect is that these developments do not have to be accomplished in real-time, but does need to exhibit "security agility" allowing flexibility in developing necessary COA. The primary role here is in

[9] Appendix A provides a generic timescale indicating what is taken place from data to execution.
[10] INFOCON stands for Information Condition that is applied to networks to deal with world-wide conditions imposed on US and friendly computer architectures.

"prediction" of possible events so that a comprehensive list of COA can be developed and deployed.

b. Human-ON-the-Loop:

Considering the concept of "dial-a-autonomy level", the human's role is essentially "on-the-loop". The human waits until a decision point is reached, makes the decision, then the system continues autonomously until the next decision point is reached.

1) Emphasis: focusing more on the "cognitive" nature of planning and monitoring.
2) Enabler: Adaption, Innovation and Robustness.
3) Applicable C2 Approach: Delegation of Decision Rights, Patterns of Interaction.
4) Timescales: Minutes to Hours

In the INFOCON example, the Human-ON-the-Loop would be responsible for implementing the appropriate COA and interjecting at particular decision points. Other than these decision points, the system is totally autonomous in executing the INFOCON instructions. Key aspect here is that the Human-ON-the-Loop needs to exhibit adaption and robustness since nothing goes as planned. The Human-ON-the-Loop may be required to interject and change particular COAs depending on changes in the architectural environment.

c. Human-IN-the-Loop: focusing on the actual "execution" of events as they happen.

1) Emphasis: Real-time Monitoring and Execution of courses-of-action
2) Enabler: Adaptability, Flexibility, Responsiveness and Robustness
3) Applicable C2 Approach: Patterns of Interaction and Distribution of Information
4) Timescales: Milliseconds to Seconds

Regarding INFOCON, the Human-IN-the-Loop would be responsible for real-time management of the changes as outlined in the INFOCON. It is postulated that for other than routine operations, this option is the least desirable since the Human can't exhibit flexibility, responsiveness and robustness fast enough to keep up with the changes nor be able to change the architecture fast enough to minimize damage to the world-wide computer architecture.

d. Human-AFTER the Loop:

1) Emphasis: Assessment as to mission effectiveness
2) Enabler: Adaptability, Flexibility, Innovation and Responsiveness
3) Applicable C2 Approach: Patterns of Interaction and Distribution of Information
4) Timescales: Minutes to Hours

For the Human-AFTER-the-Loop with respect to INFOCON, the responsibility would be real-time assessment and lessons learned on how well the entire INFOCON process was executed. It is postulated that for other than routine operations, this option would not be able to contribute as well in the real-time aspect of damage assessment. As with the Human-IN-the-Loop, the Human can't exhibit flexibility, responsiveness and robustness fast enough to keep up with the changes nor be able to influence the on-going changes to the architecture fast enough to minimize damage to the world-wide computer architecture.

Measures of Cyber Agility

The concept of agility does not apply to a stable situation; therefore, agility can be defined as the capability to successfully effect, cope with and/or exploit changes in circumstances[11]. Net-enabled approaches have the potential to be more agile in the cyber domain simply because it's more machine-to-machine oriented. Additionally, it is postulated that cyber security and agility are directly related.

The set of relevant missions and circumstances forms an Endeavor space[12]. An agility map is a projection of performance onto the Endeavor space[13]. Since endeavor spaces can have large number of dimensions, SAS-085 group has proposed two candidates for agility metrics:

a) Percent Endeavor Space Covered: the percentage of Endeavor Space where a particular approach or an Entity employing multiple approaches can successfully operate. One can envision this as the percent of Endeavor Space Covered indicating a successful approach regarding cyber agility. The areas that can be measured are: responsiveness, robustness, flexibility, adaptability and resilience.

b) Benchmarked Agility: involves a comparison between projected and expected performance.

Within an edge approach, some examples of cyber agility are:

1. Human-BEFORE-the-Loop: Predictive, discovery,[14] and information agility.

2. Human-ON-the-Loop: Cognitive, Synchronized, and organizational agility.

3. Human-IN-the-Loop: Execution, Synchronized, and organizational agility.

4. Human-AFTER-the-Loop: Assessment agility.

[11] SAS-085, work-in-progress.
[12] SAS-085, work-in-progress.
[13] SAS-085 is working on defining an endeavor space as a multi-dimensional space consisting of regions that correspond to different endeavor characteristics and conditions.
[14] This is the ability to discover information and/or applications anywhere.

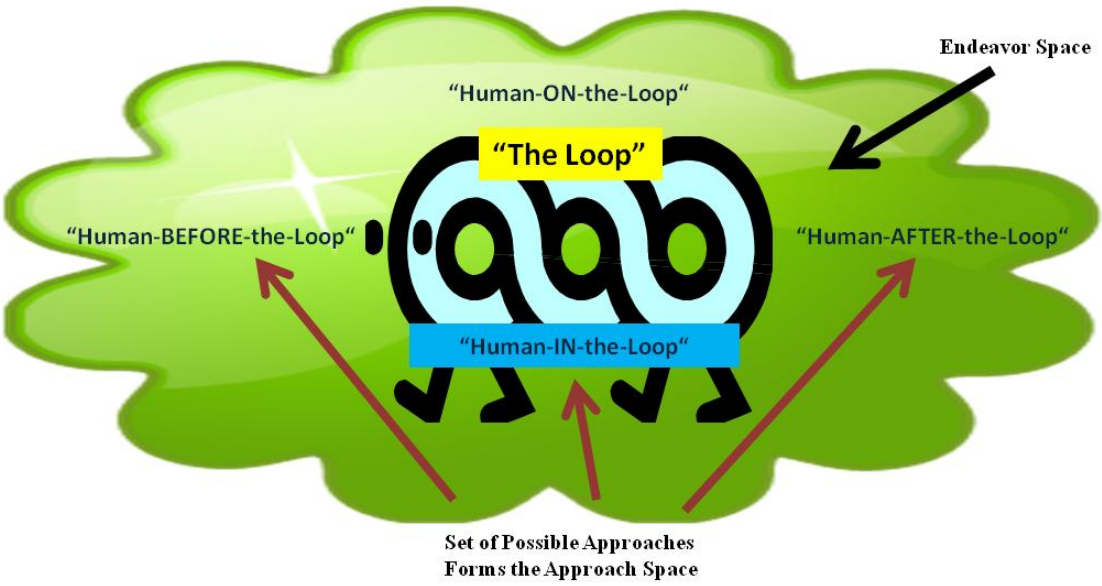


Figure 9: Approach Space within Endeavor Space

Metrics Relating to Cyber Agility

As discussed, there are six net-centric metrics that can be employed to measure cyber agility. Relating these six to the endeavor space, you have:

a) Robustness
1. Percent Endeavor Space Covered: Range of no robustness to maximum robustness.
2. Benchmarked Agility: Amount of robustness typically displayed in operational scenarios.

b) Resilience
1. Percent Endeavor Space Covered: Range of no resilience to maximum resilience.
2. Benchmarked Agility: Amount of resilience typically displayed in operational scenarios.

c) Responsiveness
1. Percent Endeavor Space Covered: Range of no responsiveness to maximum responsiveness.
2. Benchmarked Agility: Amount of responsiveness typically displayed in operational scenarios.

d) Flexibility
1. Percent Endeavor Space Covered: Range of no flexibility to maximum flexibility.
2. Benchmarked Agility: Amount of flexibility typically displayed in operational scenarios.

e) Innovation
1. Percent Endeavor Space Covered: Range of not showing innovation to maximum utilization of innovation.
2. Benchmarked Agility: Typical amount of innovation displayed in operational scenarios.

f) Adaption
1. Percent Endeavor Space Covered: Range of no adaption to maximum adaption.
2. Benchmarked Agility: Amount of adaption typically displayed in operational scenarios. Can be viewed as inherent adaption for given scenarios.

Mathematical Representations of Cyber Agility

There are numerous methods of performing analysis to determine "mission effectiveness" within complex endeavors. Performing analysis regarding cyber agility as a function of human interactions is primarily qualitative (e.g., using a four-part evaluation: totally-unacceptable, unacceptable, acceptable, totally acceptable), using "subjective logic" (See Appendix D for a short overview) is a possibility. The mathematical representation can be shown as:

MOE (cyber agility) = f(belief) + f(disbelief) + f(uncertainty)

This would entail using disbelief uncertainty algebra for cyber agility analysis. (Denny, 2010: Paper 113) Denny's paper describes a methodology that can translate a particular cyber effect into a Measure of Effectiveness (MOE). The scale could be a continuous range from 0 to 1 for each of the variables [belief (b), disbelief (d) and uncertainty (u)]. The resultant nth order effect measure:

0 = Detrimental to Operations,

.25 = Unacceptable,

.50 = Acceptable,

.75 = Very Acceptable,

1 = Significantly Acceptable to Operations

A way of graphically displaying the results could be by spider graph. Figure 11 illustrates an example for comparing two different Courses-of-Action (COA) options for each of the Human interactions (BEFORE, AFTER, ON, IN) discussed. Each analysis would take into account a weight factor for each of the six metrics (wt-1 to wt-7 normalized to total one) and their values would factor in the "subject logic" as discussed. The resultant effectiveness would indicate "success" for a particular set of COA. Risk mitigation is never easy within an operational environment. Figure 11 illustrates low vs. high risk on mission effectiveness (MOE). Clearly,

green is better; however, it comes with a high risk which would be different for each of the four interaction options. The goal would be to show the resultant effectiveness so that the Commander could make a more informed decision.

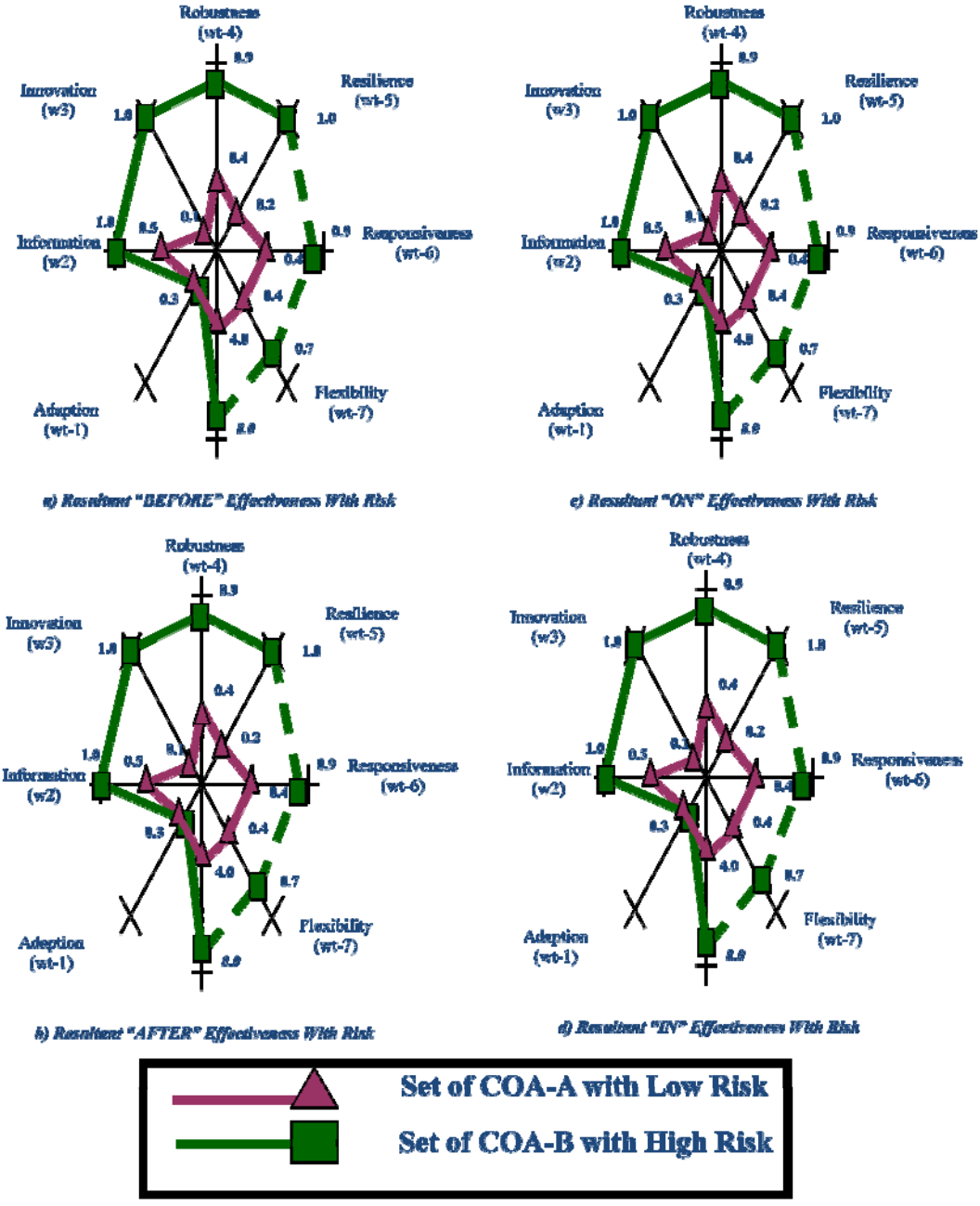


Figure 11: Spider Graph Representations of Effectiveness with Risk[15]

[15] Data does not represent actual values. They are included for illustrated purposes only.

Risk Mitigation Effects Cyber Agility

Within the development of any COA, there is an inherent risk that the Commander must take. Figure 12 illustrates effectiveness vs. impact on mission for particular events when taking into account the variables shown in Figure 11[16]. This figure is the classic "watermelon" chart. Consider these two examples:

1) Human-IN-the-Loop during a high intensity cyber engagement (high probability) could have catastrophic effects since the human does not have the capacity to think and execute in milli-seconds. This would affect responsiveness (C7), flexibility (C2), and adaption (C3).

2. Human-IN-the-Loop during a low intensity cyber engagement (high probability) could have minimal consequences provided the human has minutes to hours to think and execute particular COAs. This would affect innovation (C1), robustness (C4), and information (C6).

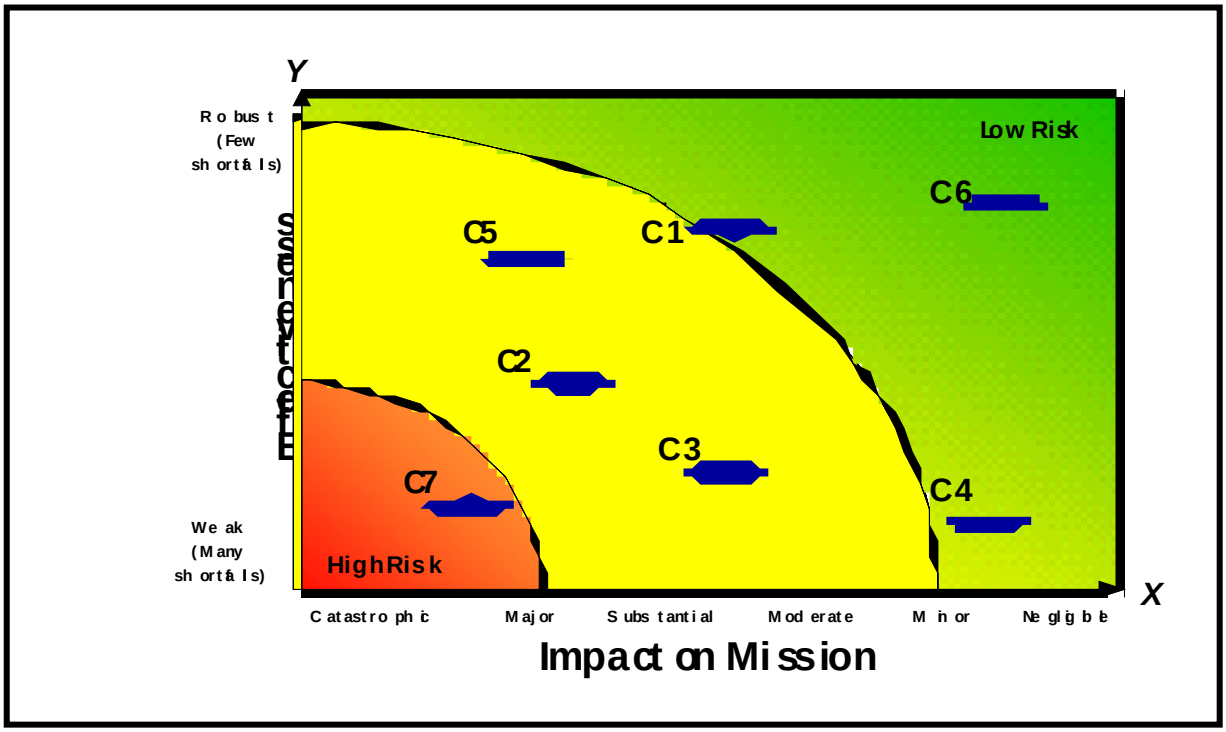


Figure 12: Risk Mitigation and Impact on Mission[17]

Figures 11 and 12 are just samples of the types of analytical representations that can be formed to illustrate "mission effectiveness" used to evaluate potential COA. The key is to include all

[16] C1=Innovation, C2=Flexibility, C3=Adaption, C4=Robustness, C5=Resilience, C6=Information, and C7=Responsiveness
[17] Data does not represent actual values. They are included for illustrated purposes only.

aspects of human interactions during the planning and assessment phases of operations. This is a more robust incorporation of effects-based operations to provide a more comprehensive analysis of potential effects given a set of COA.

Taking human interactions into account it seems clear that a combination of the four options would provide optimum mission effectiveness within the cyber domain. Naturally, it goes without saying that the optimum combination depends on the mission being performed. For example, if the operation is a highly complex cyber engagement that is being conducted in a short period of time, having a Human-IN-the-Loop vice Human-ON-the-Loop may not be the optimum choice.

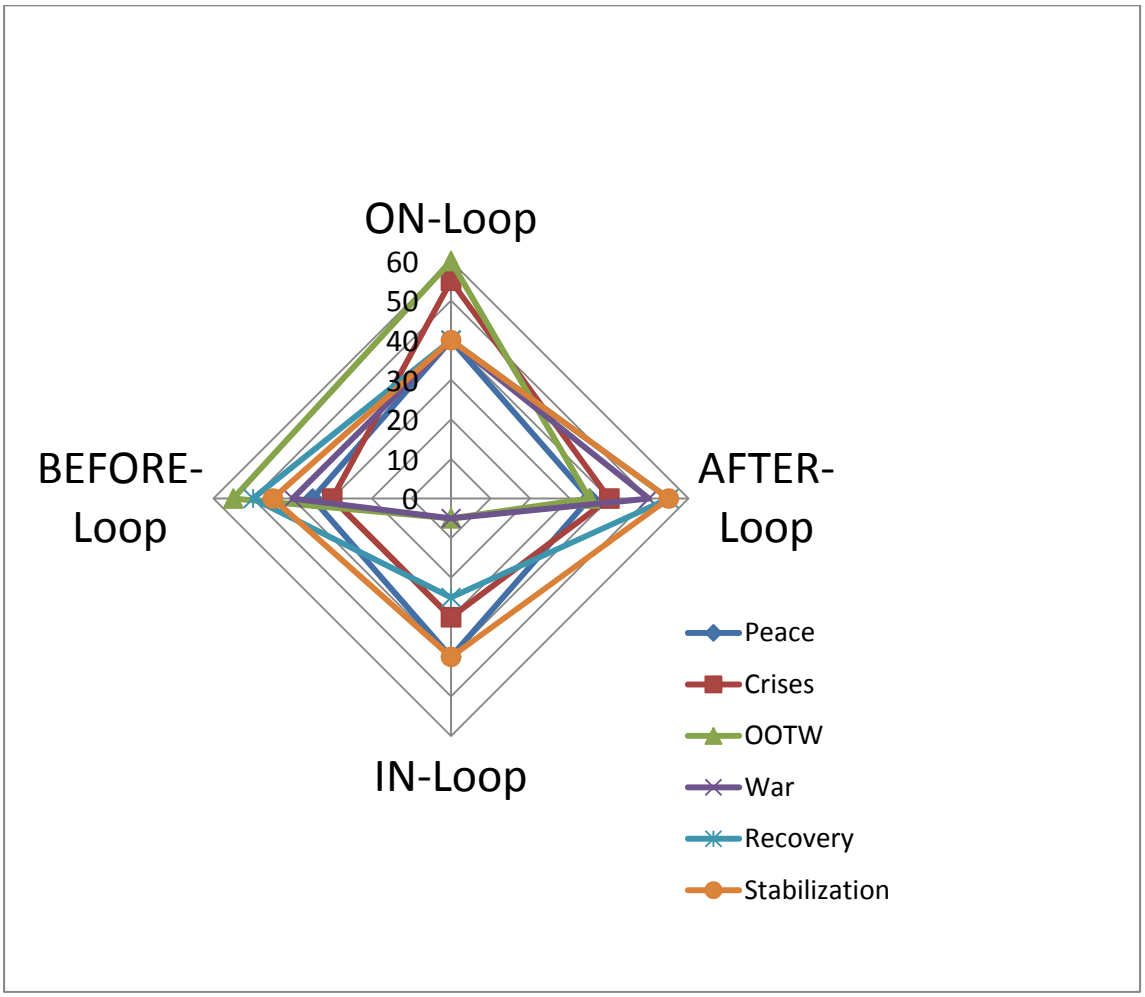


Figure 12: Phases of Conflict and Human Responsiveness[18]

Figure 12 illustrates a hypothetical example regarding human responsiveness as a function of the six phases of conflict. It is postulated that by having a "Human-IN-the-Loop" during crises, OOTW and especially War will actually be a determent to overall mission performance. The

[18] Data does not represent actual values. They are included for illustrated purposes only.

Human simply can't collect, process, decide and act fast enough to keep up with a cyber high-paced engagement.

Figure 12 can also be used to represent the level of cyber agility, as a function of human responsiveness, for each phase of conflict. For example, a low score could represent little to no agility and a high score could represent high agility for a set of human interactions.

Conclusions

The role of humans within the cyber domain definitely is related to the particular mission that needs to be accomplished. It is postulated that:

a) Human-BEFORE-the-Loop will perform better in the areas of discovery and prediction agility; where, "security agility" would play a major role during this interaction phase. Considering coalition operations, "classify by default" vice share by default" needs to be the norm to improve "security agility."

b) Human-ON-the-Loop is best when periodic injection of decisions can be performed. However as mission challenges become more complex, Human-IN-the-Loop may not be as optimal as Human-ON-the-Loop due to the rapid cognitive requirements necessary in a fast paced cyber engagement.

c) Human-IN-the-Loop is best when time is not a critical factor for mission success. Measures of cyber agility are also dependent on the "C2 approach" and its effectiveness in the "Endeavor Space" with respect to human involvement. It is postulated that, again, Human-IN-the-Loop would display the least cyber agility as compared to the other three.

d) Human-AFTER-the-Loop is best during the assessment phase of operations.

References

Alberts, David S.; Hayes, Richard E., "NATO NEC C2 Maturity Model," CCRP Publication, Feb 2010, p 48-49, p 66.

Alberts, David S., Hayes, Richard E., "Planning: Complex Endeavors," CCRP Publication, Apr 2007, page 123

Denny, Nathan, "Mission Profiles and Evidential Reasoning for Estimating Information Relevancy in Multi-Agent Supervisory Control Applications," 15th ICCRTS, Paper 113, June 2010, page 4, 10, and 13.

Jøsang, A; Artificial Reasoning with Subjective Logic. In *Proceedings of the 2nd Australian Workshop on Commonsense Reasoning*, 1997.

Jøsang, A; Conditional Reasoning with Subjective Logic. *Journal of Multiple-Valued Logic and Soft Computing* 15(1), 2009.

Pontius, Ronald, Director, C2 Programs and Policy OASD NII/DoD CIO, Plenary briefing titled: "Coalition C2/Multinational Information Sharing: Current Capabilities and Challenges," 16th ICCRTS, 21-23 Jun 2011, Quebec City, Canada, Slide 4.

Appendix A: Operational Timelines and Relationships

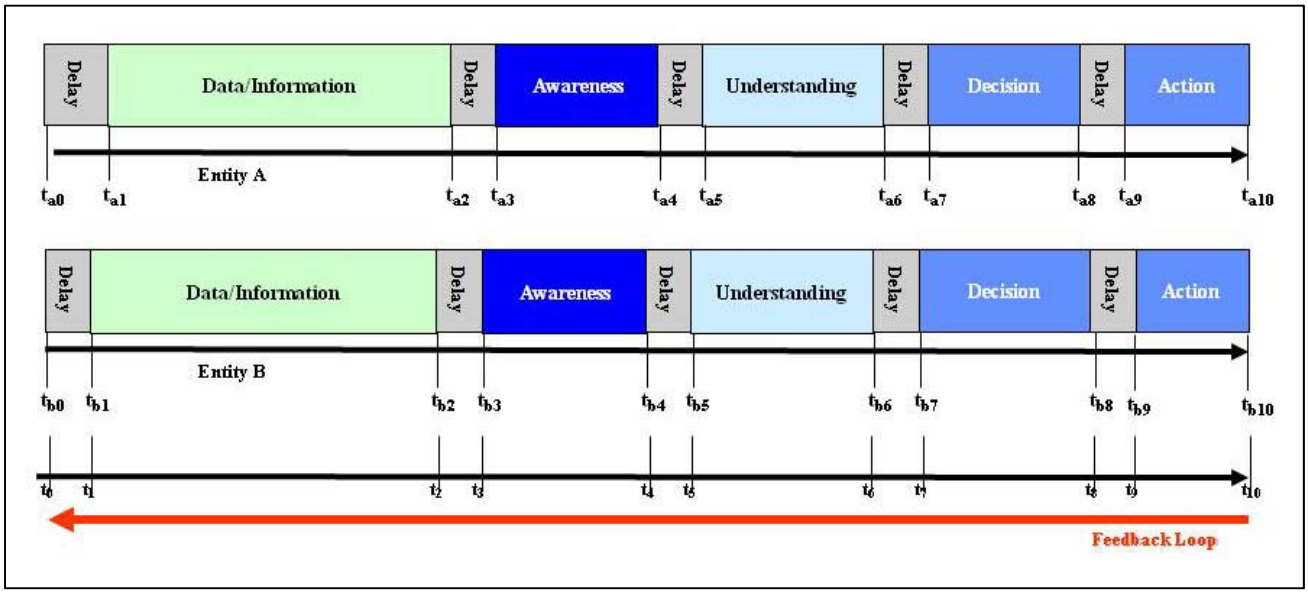


Figure A-1: Timeline From Data/Information (t_0) to Action (t_{10})

Timeline	Relationship
Definitions	
t0	Start of particular time reference
t8	Time collaborative decision is made
ta8	Time entity A decision is made
tb8	Time entity B decision is made
ta10	Time to Action for entity A
tb10	Time to Action for entity B
ta3-ta0 or tb3-tb0	Currency of the data/information
MAX(ta3,tb3) – t0	Currency of the Shared Information
MAX(ta5,tb5) – t0	Currency of Shared Awareness
MAX(ta7,tb7) – t0	Currency of Shared Understanding
MAX(ta9,tb9) – t0	Currency of Shared Decisions
MAX(ta10,tb10) – t0	Currency of Shared Actions
Basic Times	
ta2 – ta0, tb2 – tb0	Time to receive, process, disseminate data/information
ta4 – ta2, tb4 – tb2	Time to analyze and gain Awareness
ta6 – ta4, tb6 – tb4	Time to analyze and gain Understanding
ta8 – ta6, tb8 – tb6	Time to analyze and make a decision (Speed of Decision)
Individual Times	
ta4 – ta0, tb4 – tb0,	Time to Awareness
ta6 – ta0, tb6 – tb0,	Time to Understanding
ta8 – ta0, tb8 – tb0,	Time to make a Decision (Speed of Command)
ta10 – ta0, tb10 – tb0	Time to Action (Speed of Action)
Collaboration Times	
MAX(ta4,tb4) – t0	Time to Shared Awareness (time to achieve a Collective Awareness)
MAX(ta6,tb6) – t0	Time to Shared Understanding (time to achieve a Collective Understanding)
MAX(ta8,tb8) – t0	Time to make a Shared Decision (Joint Speed of Decision)
MAX(ta10,tb10) – t0	Time to Shared Action (Joint Speed of Action)

Table A-1: Net-Centric Operations Timeline and Relationships

Appendix B: Net-Centric Operations Levels of Metrics

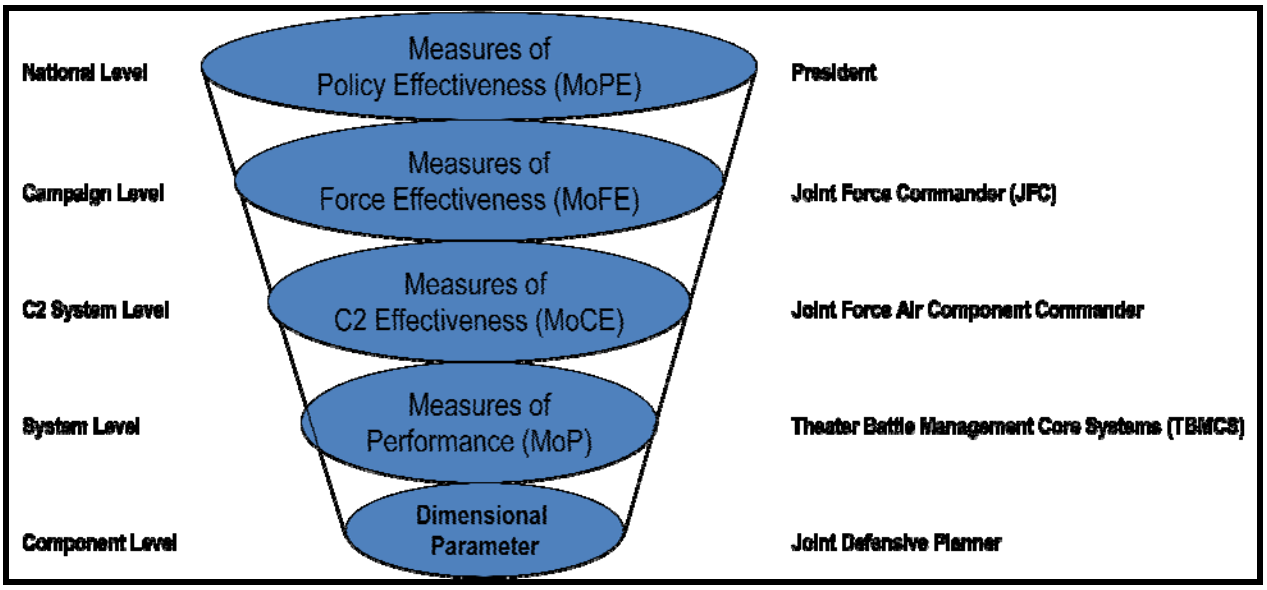


Figure B-1: Hierarchical View of Measures of Effectiveness[19]

Where:
MoM = Set of variables that focus the assessment on the issues of interest.
MoPE = focus on policy and societal outcomes
MoFE = focus on how a force performs its mission or the degree to which it meets its objectives
MoCE = focus on the impact of C2 systems within the operational context
MoP = focus on internal system structure, characteristics and behavior
DP = focus on the properties or characteristics inherent in the physical C3 systems

[19] NATO COBP, 2002, page 92.

Appendix C: Net-Centric Factors/Criteria Metrics

Metrics taken from the AF FY10 Command and Control Capabilities Analysis Team Final Report, dated 15Oct 2007, Appendix B.[20]

FACTORS CRITERIA	CHARACTERISTICS/EXAMPLES
Accessibility: data/information	Percent of time users are provided with (or retrieve from) needed products under various loading conditions.
Accessibility: network	Percent of time a network is available for use by users to provide needed products under various loading conditions.
Accountability: individual decisions	Measures the degree to which individual decisions are "accountable" given the situation. Metric is an accountability scale in percent (0%=not accountable of individual decisions needed and what is available, 100%=max accountability between individual decisions needed and available.
Accountability: collaborative decisions	Measures the degree to which collaborative decisions are "accountable" given the situation. Metric is an accountability scale in percent (0%=not accountable of collaborative decisions needed and what is available, 100%=max accountability between collaborative decisions needed and available.
Accuracy: data/information	Measure of error. Metric is a percent scale (0%=no match between precision level needed and what is available, 100%=high degree of matching between precision level needed and available. Examples: avg miss distance: +/-x feet; MHz: +/- x hertz
Accuracy: shared data/information	Measure of error regarding shared information between entities. Metric is a percentage scale (0%=no match between shared data/information needed and what is available, 100%=high degree of matching between shared information needed and available.
Accuracy: shared awareness	Measure of error regarding shared awareness between entities. Metric is a percentage scale (0%=no match between shared awareness needed and what is available, 100%=high degree of matching between shared awareness needed and available.
Accuracy: shared understanding	Measure of error regarding shared understanding between entities. Metric is an ordinal scale (0=no match between shared understanding needed and what is available, 10=high degree of matching between shared understanding needed and available.
Availability: data/information	Percent of time users are provided with needed products under various loading conditions. Squadron, wing, base, NAF, MAJCOM, Air Force level, Joint level
Availability: shared awareness	Percent of time individuals "share" awareness.
Availability: individual decisions	Percent of time individuals "share" decisions.
Availability: collaborative decisions	Percent of time individuals "share" collaborative decisions.
Availability: individual understanding	Percent of time individuals "share" understanding.
Availability: shared understanding	Percent of time individuals "share" understanding
Awareness	Awareness is a process state existing in the cognitive domain. It takes place in the minds of key leaders and their supporting battlestaffs, not in computers. Awareness is achieved through a complex interaction of available information (e.g., COP) with prior knowledge and beliefs representing the experience and expertise of the battlestaff. Awareness relates to the operational situation as it currently is or was in the past. Human perception of the situation as it is and as it is becoming.
Collective Awareness	Collective awareness is the sum of the elements of situational awareness held by all the actors within a military, interagency, or coalition structure.

[20] The AF FY12 Command and Control Capabilities Final Report is FOUO; however, the metrics used in the final report are a compilation of open literature regarding network centric operations analysis and is public releasable.

FACTORS CRITERIA	CHARACTERISTICS/EXAMPLES
Collective Knowledge	Degree to which team members have the knowledge, skills, attributes, and abilities that they need to accomplish the task at hand
Combat Assessment	Battle Damage Assessment (BDA) + Munitions Effectiveness Assessment (MEA), a subset of which is Bomb Impact Assessment (BIA) + Mission Assessment (MA); Re-attack recommendation.
Completeness: data/information	Measures the completeness of the data/information provided. Metric is the percentage of relevant data/information received to a ground truth containing all the data/information
Completeness: shared data/information	Measures the completeness of the data/information shared between entities. Metric is the percentage of relevant shared data/information received to a ground truth containing all the data/information
Completeness: shared awareness	Measures the shared awareness between entities. Metric is the percentage of relevant shared awareness received to a ground truth containing all the data/information
Completeness: shared understanding	Measures the shared understanding between entities. Metric is the percentage of relevant shared understanding received to a ground truth containing all the data/information
Computer Intrusion Detection	Denial of service; scanning and probing; password attacks; privilege grabbing; hostile code insertion; cyber vandalism; proprietary data theft; fraud, waste and abuse; audit trail tampering; security admin attacks.
Consistency: data/information	Measures the degree of "deviation" from previous data/information gained from previous time period. Measure is a percentage deviation.
Consistency: shared data/information	Measures the degree of "deviation" from previous data/information shared gained from previous time period. Measure is a percentage deviation.
Consistency: shared awareness	Measures the degree of "deviation" from shared awareness gained from previous time period. Measure is a percentage deviation.
Consistency: shared understanding	Measures the degree of "deviation" from shared understanding gained from previous time period. Measure is a percentage deviation.
Correctness: Organic Information	Measure to determine the correctness of organic information. Metric is a convergence index (0=no correspondence with ground truth, 1=full correspondence with ground truth) Data matrix comprised of relevant information items estimates (for instance: detection, ID, velocity, location, heading, etc.)
Correctness: Shared Information	Measures the correctness of the data/information that is shared between two entities. Metric is a convergence index (0=no convergence, 1=full convergence) between shared information and ground truth
Correctness: Shared Awareness	Measures the level of shared awareness between two entities. Metric is a convergence index (0=no awareness, 1=full awareness) between shared awareness and ground truth
Correctness: Shared understanding	Measures the level of shared understanding between two entities. Metric is a convergence index (0=no awareness, 1=full awareness) between shared understanding and ground truth
Currency: data/information	Measures the age of the data/information from the time it was originally created
Currency: shared data/information	Measures the age (time lag) of the shared data/information from the time it was originally shared between entities
Currency: shared awareness	Measures the age (time lag) of the shared awareness from the time it was originally shared between entities
Currency: shared understanding	Measures the age (time lag) of the shared understanding from the time it was originally shared between entities
Decision Maker: Leadership	Measures the ability of the decision maker to motivate and inspire individuals and build teams to achieve mission objectives. Metric is a five level scale (VL, L, M, H, and VH) of a decision maker's leadership capability.
Decision Maker: Confidence	Measures the ability of the decision maker to gain the trust of superiors, peers, and subordinates by demonstrating integrity, professional competence, and dedication to successfully completing the current mission. Metric is a five level scale (VL, L, M, H, and VH) of a decision maker's confidence factor.

FACTORS CRITERIA	CHARACTERISTICS/EXAMPLES
Decision Maker: Balance	Measures the ability of the decision maker to balance personal health and mental well being with the demands of the job in order to stay fresh, alert, and effective. Metric is a five level scale (VL, L, M, H, and VH) of a decision maker's ability to balance numerous factors in order to conduct mission operations.
Decision Maker: Decisiveness	Measures the ability of the decision maker to provide decisive decisions in the conduct of military operations. Metric is a continuous level scale (0%=not decisive 50%=somewhat decisive, 100%=extremely decisive).
Decision Maker: Adaptability	Measures the ability of the decision maker to adaptive to withstand or adjust to changes in the battlespace. Metric is a continuous level scale (0%=not adaptable 50%=somewhat adaptable, 100%=extremely adaptable).
Decision Maker: Interpersonal Communications Skills	Measures the interpersonal communications skills of the decision maker. Metric is a continuous level scale (0%=little to no interpersonal communications skills, 50%=medium interpersonal communications skills, 100%=high degree of interpersonal communications skills).
Decision Maker: Projection	Measures the ability of a decision maker to conceptualize future actions and events based on relevant factors. Metric is a continuous level scale (0%=little to no ability to project, 50%=medium projection skills, 100%=high degree of projection skills).
Decision Maker: Multi-Tasking Ability	Measures the ability of the decision maker to multi-task to effectively manage time and priorities to accomplish multiple activities simultaneously within the battlespace. Metric is a continuous level scale (0%=does not have any multi-tasking abilities, 50%=demonstrates some multi-tasking abilities, 100%=exhibits extreme multi-tasking abilities).
Decision Maker: Concentration	Measures the ability of a decision maker to maintain focus and deal with uncertainty through the "fog of war". Metric is a continuous level scale (0%=little concentration ability, 50%=medium concentration ability, 100%=high degree of concentration ability).
Decision Maker: Negotiation Ability	Measures the ability of the decision maker to tactfully resolve difficult situations when internal and external partners disagree due to contrasting opinions, goals, priorities, methods, and /or solutions. Metric is a five level scale (VL, L, M, H, and VH) of the decision maker's negotiation ability or skill.
Decision Maker: Courage	Measures the decision maker's ability to do the right thing at the right time in spite of pressure to do otherwise. Includes the ability to talk about doubt, uncertainty, and bad news. Metric is a continuous level scale (0%=exhibits little to no courage, 50%=exhibits sufficient courage, 100%=demonstrates extreme courage).
Decision Maker: Objectivity	Measures the ability of the decision maker to clearly look at the operational situations (Blue, Red, Gray, and White) as they unfold within the battlespace. Metric is a continuous level scale (0%=exhibits little to no objectivity, 50%=exhibits sufficient objectivity, 100%=demonstrates extreme objectivity).
Decisions: Collaborative Accuracy	Measures the degree to which collaborative decisions are "accurate" given the situation. Metric is a percentage scale (0%=no match between collaborative decisions needed and what is available, 100%=high degree of matching between collaborative decisions needed and available.
Decisions: Collaborative Adaptability	Measures the ability of a decision maker to alter collaborative decisions when necessary as the situation changes. Metric is a percentage scale (0%=cannot adapt, 50%= show some adaptability, 100%=shows significant adaptability)
Decisions: Collaborative Appropriateness	Measures the degree to which collaborative decisions are appropriate given the situation. Metric is a percentage scale (0%=collaborative decision not appropriate to situation, 50%=collaborative decision may or may not be appropriate to situation, 100%=high degree of appropriateness between collaborative decisions needed and available)
Decisions: Collaborative Consistency	Measures the degree of collaborative decision "consistency". Metric is a percentage index that relates the degree of "deviation" from previous collaborative decisions (0%= no consistency, 50%=some consistency, 100%=maximum consistency)
Decisions: Collaborative Completeness	Measures the degree of decision "completeness". Metric is the percentage of individual decision relevant to the situation at hand (0%=no relevance, 50%=somewhat relevant, 100%=maximum relevancy)
Decisions: Collaborative Currency	Measures the time to make a collaborative decision. Metric is an index that measures the time it takes a decision maker to make a collaborative decision given a situation.
Decisions: Collaborative Flexibility	Measures the ability of a decision maker to make collaborative decisions in different situations. Metric is a percentage flexibility scale (0%=not flexible, 50%=some flexibility, 100%=significant flexibility)
Decisions: Collaborative Innovation	Measures the ability of a decision maker to make collaborative decisions in new ways or to understand new things. Metric is a percentage scale (0%=shows no innovation, 50%=shows some innovation, 100%=shows significant innovation)
Decisions: Collaborative	Measures the controlling nature of the decision maker in a collaborative situation. Metric is a percentage scale (0%=no control, 50%=some control, 100%=total control).

FACTORS CRITERIA	CHARACTERISTICS/EXAMPLES
Mode of Decision Making	
Decisions: Collaborative Precision	Measures the level of detail of a particular collaborative decision given a situation. Metric is a percentage scale (0%=no detail, 50%=some details, 100%=significant detail)
Decisions: Collaborative Relevance	Measures the degree to which collaborative decisions are "relevant" given the situation. Metric is a percentage collaborative relevance scale (0%=collaborative decisions not relevant, 50%=collaborate decisions somewhat relevant, 100%=high degree of relevancy between collaborative decisions needed and available.
Decisions: Collaborative Responsiveness	Measures the ability of a decision maker to make effective collaborative decisions given a situation. Metric is a percentage scale (0%=does not make effective collaborative decisions, 50%=makes some effective collaborative decisions, 100%=makes significant effective collaborative decisions)
Decisions: Collaborative Risk Propensity	Measures the decisions makers "collaborative risk taking" ability given a situation. Metric is a percentage risk level (0%=minimal risk, 100%=maximum risk) or risk interval (95%, 90%) of collaborative decisions
Decisions: Collaborative Robustness	Measures the ability of a decision maker to use levels of collaborative decisions across a range of missions that span the spectrum of conflict. Metric is a percentage scale (0%=no robustness, 50%=some robustness, 100%=significant robustness)
Decisions: Collaborative Timeliness	Measures the timeliness to which a decision maker makes "collaborative decisions" given a situation. Metric is a percentage scale (0%=does not make collaborative decisions in time to influence an outcome of a given situation, 100%=always makes collaborative decisions in time to influence an outcome to a given situation)
Decisions: Collaborative Uncertainty	Measures the uncertainty level of a collaborative decision given a situation. Metric is a percentage confidence scale (0%=uncertain, 100%=certain) or confidence interval (95%, 90%) of collaborative decisions.
Decisions: Individual Accuracy	Measures the degree to which decisions are "accurate" given the situation. Metric is a percentage accuracy scale (0%=no match between individual decisions needed and what is available, 50%=medium match between individual decisions needed and what is available, 100%=high degree of matching between individual decisions needed and available.
Decisions: Individual Adaptability	Measures the ability of a decision maker to alter individual decisions when necessary as the situation changes. Metric is a percentage scale (0%=cannot adapt, 50%= show some adaptability, 100%=shows significant adaptability)
Decisions: Individual Appropriateness	Measures the degree to which decisions are appropriate given the situation. Metric is a appropriate scale in percentages (0%=individual decision not appropriate to situation, 100%=high degree of appropriateness between individual decisions needed and available)
Decisions: Individual Consistency	Measures the degree of decision "consistency". Metric is a percentage index that relates the degree of "deviation" from previous decisions (0%=no deviation, 50%=some deviation, 100%=max deviation).
Decisions: Individual Completeness	Measures the degree of decision "completeness". Metric is the percentage of individual decision relevant to the situation at hand
Decisions: Individual Currency	Measures the time to make a decision. Metric is an index that measures the time it takes a decision maker to make a decision given a situation
Decisions: Individual Flexibility	Measures the ability of a decision maker to make individual decisions in different situations. Metric is a percentage flexibility scale (0%=not flexible, 50%=some flexibility, 100%=significant flexibility)
Decisions: Individual Innovation	Measures the ability of a decision maker to make individual decisions in new ways or to understand new things. Metric is a percentage scale (0%=shows no innovation, 50%=shows some innovation, 100%=shows significant innovation)
Decisions: Individual Mode of Decision Making	Measures the controlling nature of the decision maker. Metric is a percentage scale (0%=no control, 50%=some control, 100%=total control).
Decisions: Individual Precision	Measures the level of detail of a particular decision given a situation. Metric is a percentage scale (0%=no detail, 50%=some details, 100%=significant detail)

FACTORS CRITERIA	CHARACTERISTICS/EXAMPLES
Decisions: Individual Relevance	Measures the degree to which decisions are "relevant" given the situation. Metric is a percentage scale (0%=individual decisions not relevant, 100%=high degree of relevancy between individual decisions needed and available.
Decisions: Individual Responsiveness	Measures the ability of a decision maker to make effective individual decisions given a situation. Metric is a percentage scale (0%=does not make effective decisions, 50%=makes some effective decisions, 100%=makes significant effective decisions)
Decisions: Individual Risk Propensity	Measures the decisions makers "risk taking" ability given a situation. Metric is a percentage scale measuring the risk level (0%=minimal risk, 100%=maximum risk) or risk interval (95%, 90%) of individual decisions
Decisions: Individual Robustness	Measures the ability of a decision maker to use levels of decisions across a range of mission that span the spectrum of conflict. Metric is a percentage scale (0%=no robustness, 50%=some robustness, 100%=significant robustness)
Decisions: Individual Timeliness	Measures the timeliness to which a decision maker makes "decisions" given a situation. Metric is a percentage timeliness scale (0%=does not make decisions in time to influence an outcome of a given situation, 50%=makes decisions most of the time to influence an outcome of a given situation, 100%=always makes decisions in time to influence an outcome to a given situation)
Decisions: Individual Uncertainty	Measures the uncertainty level of a decision given a situation. Metric is a percentage that measures confidence scale (0%=uncertain, 100%=certain) or confidence interval (95%, 90%) of individual decisions.
Effectiveness: Achievement of Objectives	Measures the degree to which mission objectives are achieved. Metric is an ordinal scale (0%=no achievement, 100%=maximum achievement) or achievement interval (95%, 90%) of mission objectives.
Effectiveness: Agility	Measures the ability to modify forces objectives in a timely manner. Metric is an ordinal scale (0=not agile, 100=maximum agility)
Effectiveness: Mission	Measures the degree to which a force accomplishes its assigned military mission. It is multi-attributed. These metrics exist largely at the operational level and below when thinking inside the context of "traditional" military missions. Metric is percentage of mission effectiveness.
Effectiveness: Timeliness	Measures the ability to achieve a mission objective in a timely manner. Metric is achieved mission objectives divided by total mission objectives over a given time interval.
Effectiveness: Efficiency	Measures the ability to achieve a mission objective in an efficient manner. Metric is an ordinal scale (0=not efficient, 100=maximum efficiency)
Extent: degree of data/information	Measures the extent of shared data/information
Extent: degree of Shared Awareness	Measures the extent of shared awareness
Interaction: Individual Adaptability	Measures the ability to alter interactions when necessary as the situation changes. Metric is a percentage scale (0%=no adaptability, 50%=some adaptability, 100%=significant adaptability)
Interaction: Individual Confidence	Measures the state of being certain. Metric is a percentage index of confidence in the individual ranging from 0%=no confidence to 100%=total confidence.
Interaction: Individual Latency	Measures the time lag to conduct interactions from the start of a particular situation. Metric is a time interval that measures the time lag.
Interaction: Individual Quality	Measures the quality of the interactions present during a particular situation. Metric is a percentage scale (0%=poor quality, 50%=medium quality, 100%=high quality)
Interaction: Individual Quantity	Measures the quantity of interactions present during a particular situation. Metric is a percentage scale that measures the quantity of interactions per interval of time.
Interaction: Individual Reach	Measures the end-to-end distance interaction occurs. Metric is a percentage of nodes (locations) that can interact in desired access modes.
Interaction: Organization Confidence	Measures the state of being certain. Metric is a percentage index of confidence in the organization ranging from 0%=no confidence to 100%=total confidence.

FACTORS CRITERIA	CHARACTERISTICS/EXAMPLES
Inter-cooperability: Organization-to-Organization	The ability of an organization(s) to function together essentially as a single organization to essentially achieve shared understanding among each other and to use the information exchanged to interact effectively, interdependently and adaptively toward a common and valued set of goals. The metric would measure the level of inter-cooperability (0-none, 50%-average, 100%-maximum) between each of the organizations involved.
Inter-cooperability: Individual-to-Individual	The ability of individual(s) to function together essentially as a single entity to essentially achieve shared understanding among each other and to use the information exchanged to interact effectively, interdependently and adaptively toward a common and valued set of goals. The metric would measure the level of inter-cooperability (0-none, 50%-average, 100%-maximum) between each of the individual involved.
Inter-cooperability: Individual-to-team	The ability of an individual and teams to function together essentially as a single entity to essentially achieve shared understanding among each other and to use the information exchanged to interact effectively, interdependently and adaptively toward a common and valued set of goals. The metric would measure the level of inter-cooperability (0-none, 50%-average, 100%-maximum) between the individual and team.
Inter-cooperability: Individual-to-Organization	The ability of individual(s) and organizations to function together essentially as a single entity to essentially achieve shared understanding among each other and to use the information exchanged to interact effectively, interdependently and adaptively toward a common and valued set of goals. The metric would measure the level of inter-cooperability (0-none, 50%-average, 100%-maximum) between the individual and organization.
Inter-cooperability: Team-to-Organization	The ability of a team and organization to function together essentially as a single entity to essentially achieve shared understanding among each other and to use the information exchanged to interact effectively, interdependently and adaptively toward a common and valued set of goals. The metric would measure the level of inter-cooperability (0-none, 50%-average, 100%-maximum) between the team and organization.
Inter-cooperability: Team-to-Team	The ability of teams to function together essentially as a single entity to essentially achieve shared understanding among each other and to use the information exchanged to interact effectively, interdependently and adaptively toward a common and valued set of goals. The metric would measure the level of inter-cooperability (0-none, 50%-average, 100%-maximum) between teams.
Maintainability: data/information	Measures the maintainability of the data/information. Metric, depicted as a percentage, is the ease to which the data/information is maintained within the specified system (0%=not maintainable by pre-defined standards, 50%=somewhat maintainable by pre-defined standards, 100%=totally maintainable within pre-defined standards).
Maintainability: system	Measures the maintainability of a particular system. Metric, depicted as a percentage, is the ease to which the system is maintained within pre-defined standards – e.g., equipment accessibility, shop replaceable unit, line replaceable units, and depot level repair. (0%=not maintainable by pre-defined standards, 50%=somewhat maintainable by pre-defined standards, 100%=totally maintainable within pre-defined standards).
Maintainability: network	Measures the maintainability of a particular network. Metric, depicted as a percentage, is the ease to which the network is maintained within pre-defined standards – e.g., equipment accessibility, shop replaceable unit, line replaceable units, and depot level repair. (0%=not maintainable by pre-defined standards, 50%=somewhat maintainable by pre-defined standards, 100%=totally maintainable within pre-defined standards).
Network Agility	Measures the ability to modify an entire network un a timely manner. Metric is a percentage rating of agility (0% = no agility, 50% = medium agility, 100%=maximum agility)
Network Assurance	Measures the security of an entire network. Metric is a percentage rating of network security (100% = highly secure, 90% = secure, 0% = not secure) based on network and node encryption levels, type of security management systems provided, etc.
Network Availability	Measures the time all authorized users have access to the network. This is necessary if current information is to be shared and if the user community is to develop trust and confidence in using the information in the system. Metric is percentage of time network is available to users.
Network Reach	Measures the end-to-end extent (or reach) of the network. Metric is the percent of nodes that can communicate in desired access modes, information formats, and applications
Network Richness	Measures the quality and breath of the information found in the network. Metric is a percentage scale (0%=not rich, 50%= some richness, 100%=maximum richness) or interval scale (95%, 90%) of network richness.
Network Reliability	Measures the network's ability to consistently produce the same results. Metric is a percentage scale (0%=not reliable, 50%= somewhat reliable, 100%=maximum reliability) or interval scale (95%, 90%) of network reliability.
Precision: data/information	Measures the level of measurement detail of a data/information item. For example, Measure of repeatability, probability of damage/kill (Pd/Pk)
Precision: shared data/information	Measures the level of granularity of a shared data/information item. Measure is percentage deviation from actual "truth", for example Frequency +- 5%.
Precision: shared awareness	Measures the level of granularity of shared awareness. Measure is percentage deviation from actual "truth", for example, 9/10 commanders have the same awareness equates to 90% of shared awareness.

FACTORS CRITERIA	CHARACTERISTICS/EXAMPLES
Precision: shared understanding	Measures the level of granularity of shared understanding. Measure is percentage deviation from actual "truth", for example, 9/10 commanders have the same understanding equates to 90% of shared understanding.
Relevance: data/information	Measures the proportion of information collected that is related to the task at hand
Relevance: shared data/information	Measures the proportion of shared information collected that is related to the task at hand. Metric is a percentage scale that measures the relevance of the shared data/information (0%=no relevance, 50% = some relevance, 100%=maximum relevance)
Reliability: data/information	Information - trusted/proven source, new/unproven source; Computer - Mean-Time Between Failures (MTBF), ID faults to board level 95% accuracy;
Reliability: system	The probability a system will perform satisfactorily for a period of time under a set of conditions. Metric is a percentage scale (0%=not reliable, 50%=somewhat reliable, 100%=highly reliable).
Reliability: individual decisions	Measures the reliability of the decisions made by an individual over a period of time under a set of conditions. Metric is a percentage scale (0%=not reliable, 50%=somewhat reliable, 100%=highly reliable)
Reliability: collaborative decisions	Measures the reliability of collaborative decisions made by a team of individuals over a period of time under a set of conditions. Metric is a percentage scale (0%=not reliable, 50%=somewhat reliable, 100%=highly reliable)
Robustness	Ability to maintain effectiveness across a range of tasks, situations, and conditions across a range of missions that span the spectrum of conflict. Metric would be a percentage scale (0%=no robustness, 50%=some robustness, 100%=maximum robustness)
Shared Awareness	Shared awareness is the human perception of the situation as it is and as it is becoming. The elements of military situations include: physical environment, the capabilities and intentions of red, blue, and other forces and effectors, and the political, military, social, economic, and information contexts.
Shared Understanding	Shared understanding is the recognition of patterns, cause and effect relationships, dynamic futures, and opportunities and risks that are shared between individuals, organizations, or other entities.
Situational Awareness	Situational awareness is the "who's", "where" category. It includes friendly, enemy, and neutrals location, status; vulnerabilities and capabilities. It also includes weather and terrain features. For targeting it includes detect, locate, ID, track, and display.
Situational Understanding	Situational understanding is the "what does it mean?" category. It includes understanding of enemy intent, likely and dangerous courses of action, and actions. It includes the assessment of friendly opportunities for favorable actions and the associated risks. Situation understanding also includes resolving and dealing with uncertainty.
Speed of Command	Measures the time lag between an occasion for action and the implementation of action or a decision not to respond.
Speed of Decision	Measures the amount of time it takes for a decision to be made beginning with the time a need for some action (or decision not to act) is identified through the time where a decision is made.
Strike or Attack Mission Cycle Functions	Detection, location, identification, decision, execution, assessment.
Survivability: data/information	Measures the ability of data/information to survive and operate in various environments. Measurement is a percent scale (0%=not survivable, 100%=totally survivable).
Survivability: network	Measures the ability of the network to survive and operate in various environments (at least one complete path). Measurement is a percent scale (0%=not survivable, 100%=totally survivable).
Synchronization: Actions	Degree to which actions are synchronized. Metric is an synch action level (0%=no synchronization, 100%=maximum synchronization) or synchronization interval (95%, 90%) of actions
Synchronization: Decisions	Degree to which decisions are synchronized. Metric is an synch decision level (0%=no synchronization, 100%=maximum synchronization) or synchronization interval (95%, 90%) of decisions
Synchronization: Entities	Degree to which entities are synchronized. Metric is an synch entity level (0%=no synchronization, 100%=maximum synchronization) or synchronization interval (95%, 90%) of entities

FACTORS CRITERIA	CHARACTERISTICS/EXAMPLES
Synchronization: Plans	Degree to which plans are synchronized. Metric is an synch plan level (0%=no synchronization, 100%=maximum synchronization) or synchronization interval (95%, 90%) of plans
Timeliness: data/information	Measures the utilization of the data/information as a function of time. Metric is an ordinal scale (0=no match between currency level needed and what is available, 10=high degree of matching between currency level needed and available
Timeliness: shared data/information	Measures the utilization of the shared data/information as a function of time. Metric is a percentage scale (0%=no match between shared data/information needed and what is available, 50%= some degree of matching between shared data/information needed and what is available, 100%=high degree of matching between shared data/information needed and available.)
Timeliness: shared awareness	Measures the utilization of the shared awareness as a function of time. Metric is a percentage scale (0%=no match between shared awareness needed and what is available, 50%= some degree of matching between shared awareness needed and what is available, 100%=high degree of matching between shared awareness needed and available.)
Timeliness: shared understanding	Measures the utilization of the shared understanding as a function of time. Metric is a percentage scale (0%=no match between shared understanding needed and what is available, 50%= some degree of matching between shared understanding needed and what is available, 100%=high degree of matching between shared understanding needed and available.)
Trust: Peer-to-Peer	Measures the extent of trust between entities that are at the same level. Metric is a percentage scale (0%=no trust, 50%=some trust, 100%=significant trust)
Trust: Supervisor-to-Subordinate	Measures the ability of a supervisor to demonstrate trust in a subordinate by a willingness to delegate and allow subordinates to work without constant supervision. Metric is a percentage scale (0%=no trust, 50%=some trust, 100%=significant trust).
Trust: Subordinate-to-Supervisor	Measures the extent of trust to which a subordinate has with its supervisor. Metric is a percentage scale (0%=no trust, 50%=some trust, 100%=significant trust)
Trust: data/information	Measures the extent of trust to which an entity is willing to rely on the data/information. Metric is a percentage scale (0%=no trust, 50%=some trust, 100%=significant trust)
Trust: Organization	Measures the extent of trust to which an organization is willing to rely on other organizations. Metric is an ordinal scale (0=no trust, 5=some trust, 10=significant trust)
Trust: System	Measures the extent of trust of the system by individuals and/or organizations. Metric is a percentage scale (0%=no trust, 50%=some trust, 100%=significant trust)
Uncertainty: shared awareness	Measures the confidence level (0%=uncertain, 100%=certain) or confidence interval (95%, 90%) of shared awareness
Uncertainty: shared understanding	Measures the confidence level (0%=uncertain, 100%=certain) or confidence interval (95%, 90%) of shared understanding
Understanding	Understanding is defined as the process state of drawing inferences about possible consequences of the operational situation. It is based on the ability of the battlestaff acting individually and collaboratively to predict possible future patterns of the battlespace. That is, whereas awareness deals with the battlespace as it was, understanding deals with the battlespace as it is becoming. Interpreting these patterns spatially, functionally, temporally in the context of the goals/objectives, constraints, and planned courses of action envisioned for the operation, the battlestaff begins to identify potential threats and opportunities that demand a response change or decision from the command authorities.

Appendix D: Subjective Logic (Denny, 2010, Paper 113)

Subjective reasoning is based purely on one personal beliefs, ideals, preference opinion or culture. For example when you watch the news and see a story about incest, one might be offended at the very thought while others would not be as shocked because it is "natural" for their way of life. Another example regarding some religious sects that have incestual marriages and believe it is right where others do not. These are just two examples of subjective reasoning.

Subjective Logic (Josang, 1997) (Josang, 2009) is a type of probabilistic logic that is often used in evidential reasoning where belief (b), disbelief (d), and uncertainty (u) must be explicitly and simultaneously accounted. In contrast to systems described by Boolean Logic, for those systems described by Subjective Logic the basic object is an opinion rather than a fact. An *opinion* $\omega A(x)$ about some proposition "x" held by source "A" is a 4-tuple of the belief (b_x^A), disbelief (d_x^A), uncertainty (u_x^A), and relative atomicity (a_x^A)[21]. Mathematically, it is not necessary to specify all three of the values; however, the sum of the values always equal one ($b_x + d_x + u_x = 1$).

Subjective Logic algebra provides an array of operations that can be used to manipulate opinions. These operators have many applications in evidential reasoning and data fusion. The consensus operator (written as) is used for belief fusion, providing the capability to fuse possibly conflicting opinions while still forming coherent, summary judgments. The underlying calculations on the belief tuple elements are given in Figure D-1.

$$K = u_x^A + u_x^B - u_x^A u_x^B$$

$$b_x^{A,B} = (b_x^A u_x^B + b_x^B u_x^A) / K$$

$$d_x^{A,B} = (d_x^A u_x^B + d_x^B u_x^A) / K$$

$$u_x^{A,B} = (u_x^A u_x^B) / K$$

$$a_x^{A,B} = (a_x^A u_x^B + a_x^B u_x^A - (a_x^A + a_x^B) u_x^A u_x^B) / (K - u_x^A u_x^B)$$

Figure D-1: Subjective Logic Consensus Operation (Denny, 2010, Paper 113)

Subjective logic also provides a well developed "discount" operation (written as) that can be used for modifying the contribution of evidence based upon a subjective measure of confidence in the source of the evidence. The discount operator thus provides a rather general means of describing degrees influence and can be used to represent semantic similarity, relevance, trust, etc. The calculations for implementing a discount operator over belief tuples is shown in Figure D-2.

[21] Atomicity is the base-rate of the proposition.

$$b_x^{A,B} = b_B^A \, b_x^B$$

$$d_x^{A,B} = b_B^A \, d_x^B$$

$$u_x^{A,B} = d_B^A + u_A^B + b_B^A \, u_x^B$$

$$a_x^{A,B} = a_x^B$$

Figure D-2: Subjective Logic Discount Operation (Denny, 2010: 4)

An algorithm can be established to measure the bias to a situation as shown in Figure D-3. (Denny, 2010: 13)

Algorithm 1: Assign bias to situation elements:
For each **SituationElement**, *e*:
Instantiate **Impact** statement, *i*, that refers to *e*.
Instantiate **Conviction** statement, c_i, set to (the default) ignorance (b=0, d=0, u=1.0)
Set *i* to refer to *c*

Algorithm 2: Fuse propagation paths into Impact accumulator
for each **Judgment** *j* (where the author of *j* is not "ARID"):
if *j.about*, is of type **SituationElement**; then...
get **SituationElement** *e* to which *j.about* refers
for each **Propagation** *p* that refers to *e*:
get the **Impact**, *i*, associated to *e*
let *cp* be the **Conviction** of the *p*
let *ci* be the **Conviction** of the *i*.
accumulate *cp* into *ci* by consensus*: ci* ← *ci* ⊕ *c*p

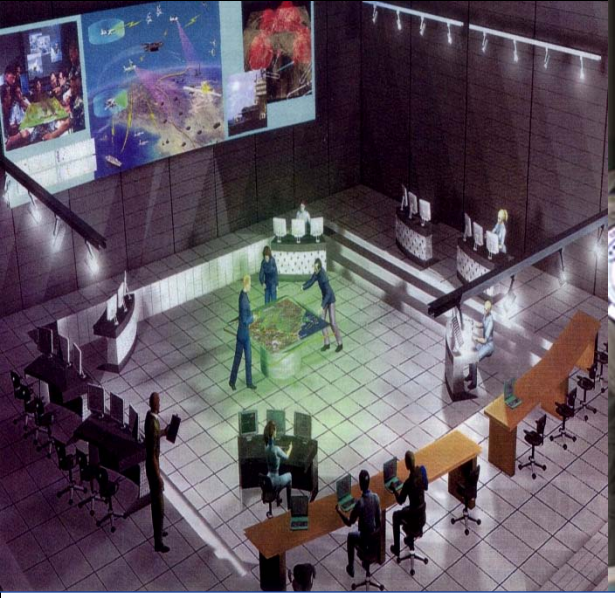
Algorithm 3: Back propagate influence to supporting evidence
for each **Evidence** statement, *s*:
let *j* be the **Judgment** that *s* supports
let *cj* be the **Conviction** of *j*
let **SituationElement** *e* be evidence of *s*
let *i* be the **Impact** of *e*
let *ci* be the **Conviction** of *i*.
let *d* be the strength of *s*
accumulate cj into ci: ci ← ci ⊕ *(d* ⊕ c_j*)*

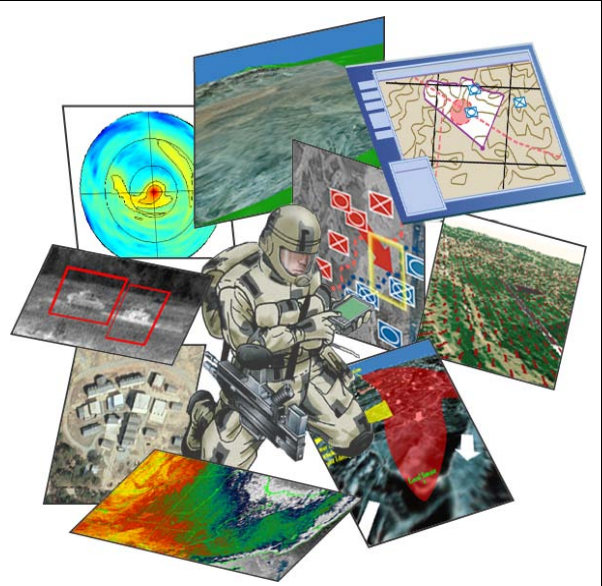
Bibliography

Paul W. Phister, Jr., Ph.D., P.E.

Dr. Phister is the Chief of the Special Programs Division at the AF Research Laboratory's Information Directorate headquartered in Rome, New York. Dr. Phister spent 25 years in the military (Lt Col, retired) where he worked primarily in space systems development and operations. Dr. Phister is a recognized subject matter expert in information technologies, C2, net-centric warfare and space operations. Over the past two decades, Dr. Phister has published 35 technical publications and has served as technical chair at numerous C2 conferences. Dr. Phister holds two Masters Degrees (Electrical Engineering and Systems Management), a Ph.D in Engineering as well as four AF Acquisition Level-3 certifications (Program Management, Test and Evaluation, Systems Engineering, and Systems Engineering-Manager). Dr. Phister is a senior member of both AIAA and IEEE and holds a dual engineering license in software and electrical engineering from the State of Texas.


AIR FORCE RESEARCH LABORATORY

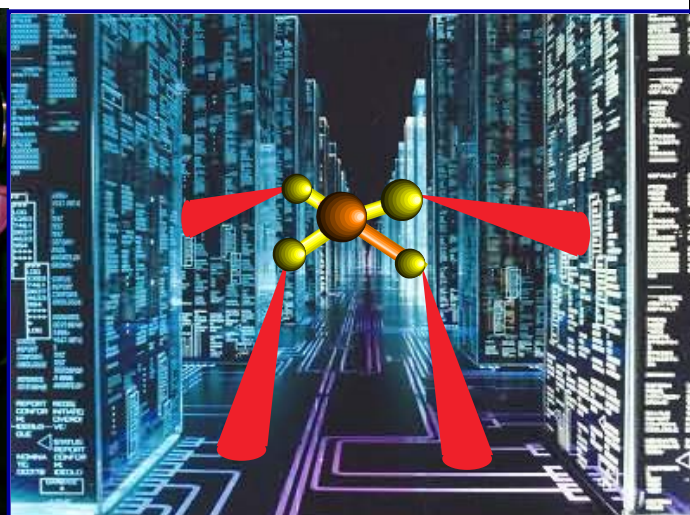




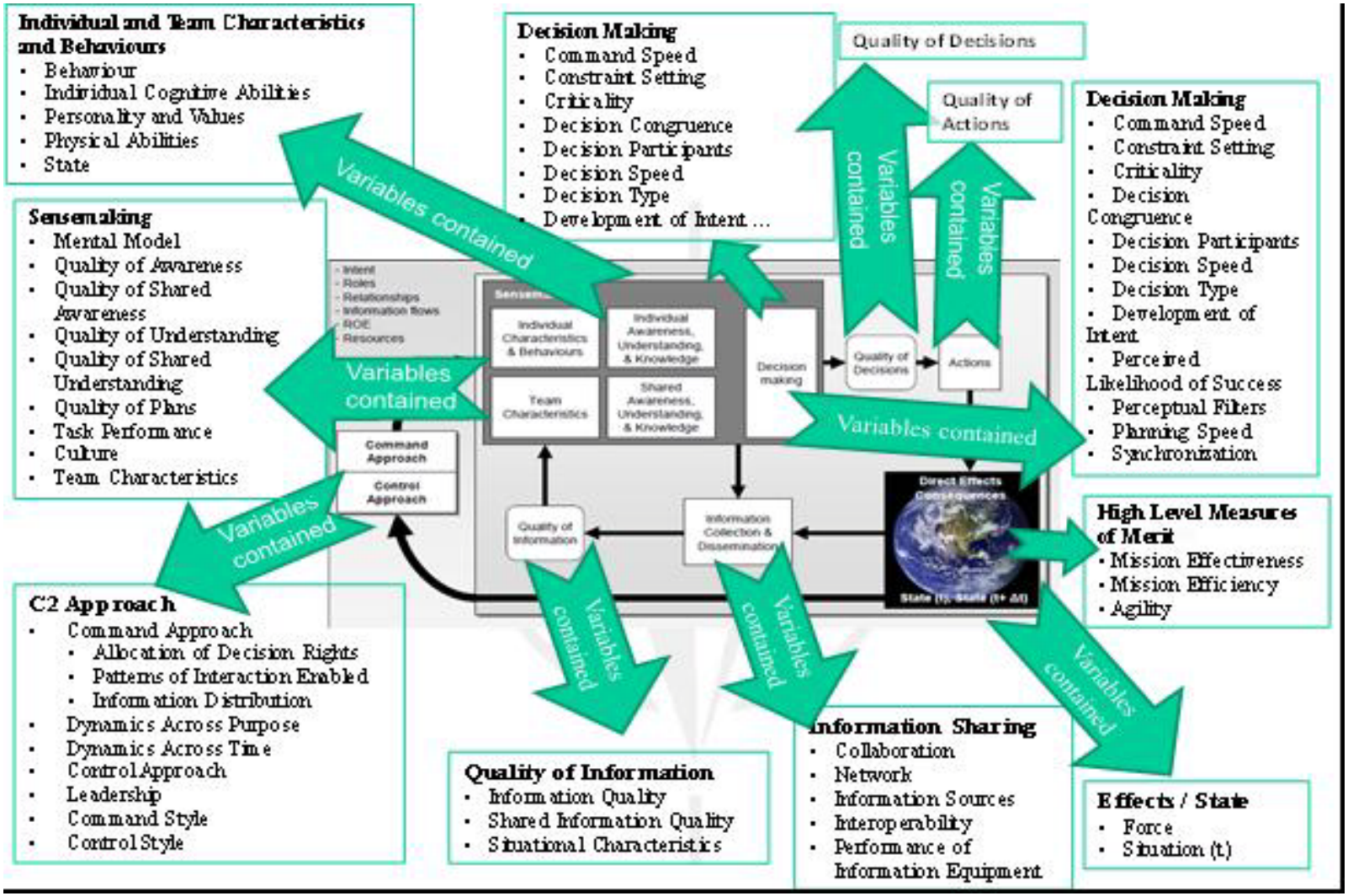
Humans and their Impact on Cyber Agility
-- Concepts, Theory, and Policy --

Dr. Paul W. Phister, Jr., P.E.

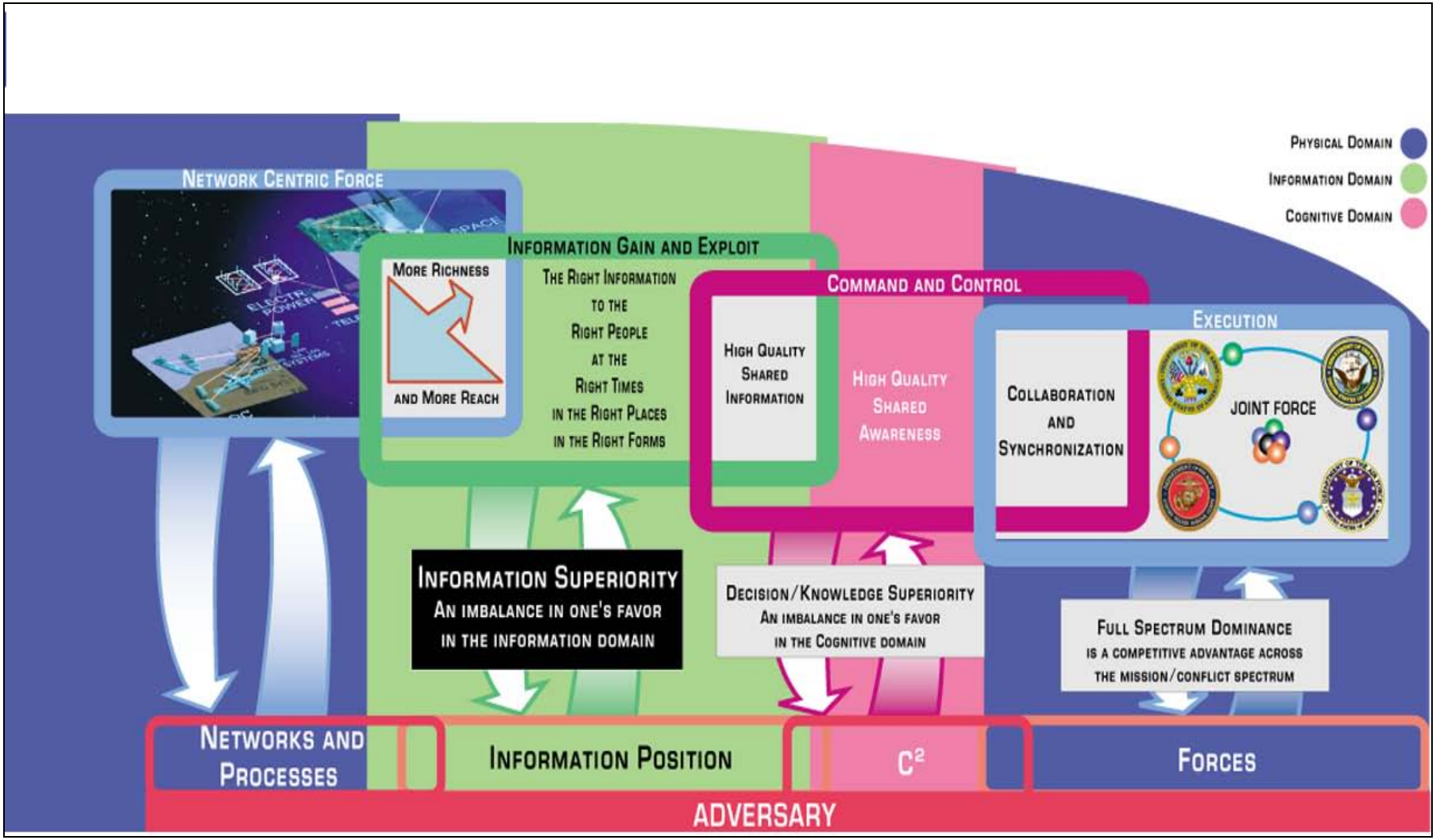
AF Research Laboratory's Information Directorate, Rome, NY



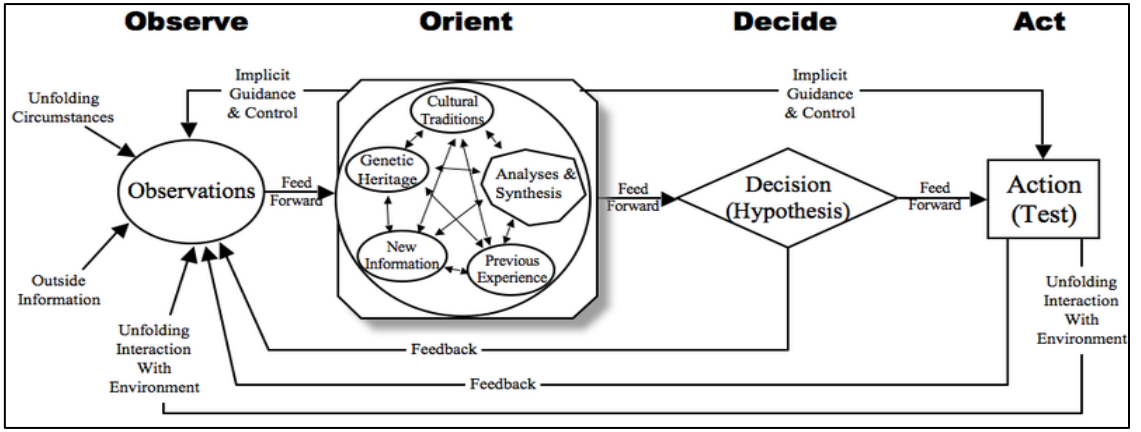
Network Centric Warfare
- C2 Conceptual Reference Model -



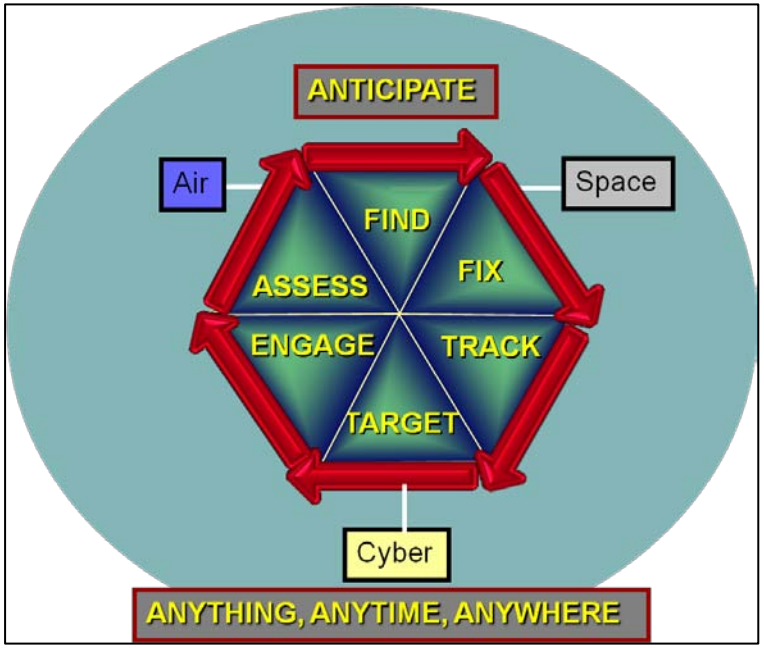
Network Centric Warfare
- Value Chain -



Human-Centric Loops



Observe-Orient-Decide-Act

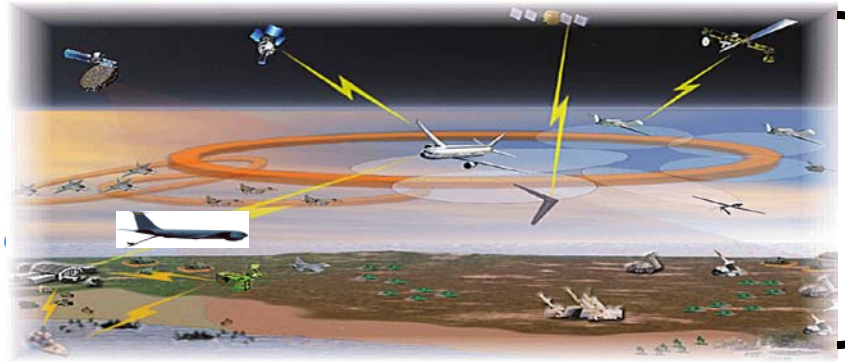


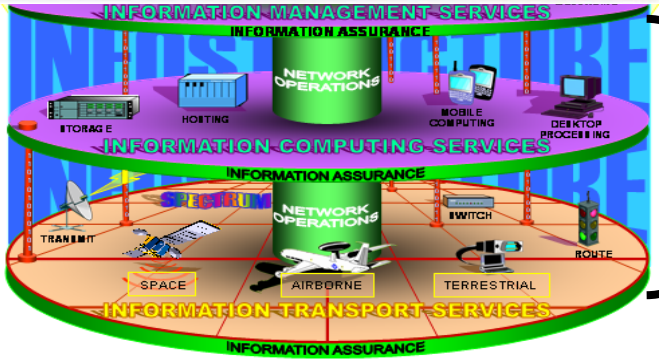
AFRL-F2T2EA4

Changing Landscape
- "The Loop" -

Network Centric Warfare

- Humans and "The Loop" -





Network Centric Operations

Network Centric Infrastructure

Human – BEFORE – the – Loop

-- Predictive Agility
-- Discovery Agility
-- Information Agility

Human – ON – the – Loop

-- Cognitive Agility
-- Synchronized Agility
-- Organization Agility

Human – IN – the – Loop

-- Execution Agility
-- Synchronized Agility
-- Organizational Agility

Human – AFTER – the – Loop

-- Assessment Agility

Metrics: Robustness, Resilience, Responsiveness, Flexibility, Innovation, Adaption

Mathematical Representation
- Cyber Agility and "The Loop" -

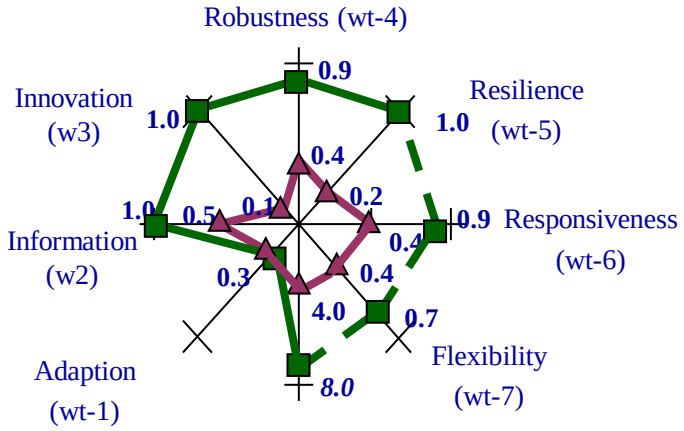
MOE (cyber agility) = f(belief) + f(disbelief) + f(uncertainty)

Scoring Metric:

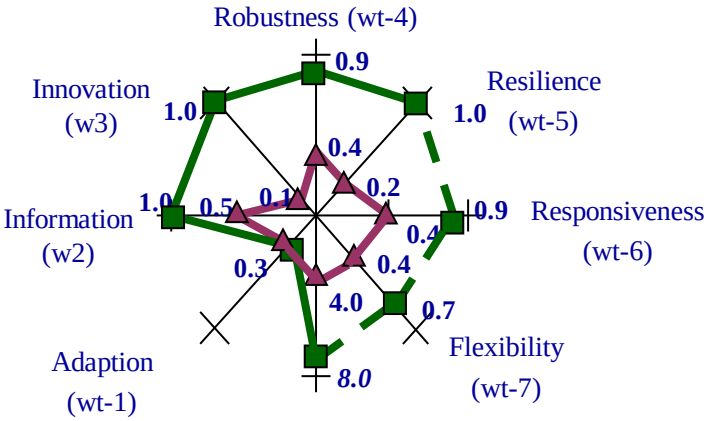
0.00 = Detrimental to Mission Operations,
0.25 = Unacceptable to Mission Operations,
0.50 = Acceptable to Mission Operations,
0.75 = Very Acceptable to Mission Operations,
1.00 = Significantly Acceptable to Mission Operations

Denny, Nathan,
"Mission Profiles and Evidential Reasoning for Estimating Information Relevancy in Multi-Agent Supervisory Control Applications,"
15th ICCRTS, Paper 113, June 2010, page 4, 10, and 13.

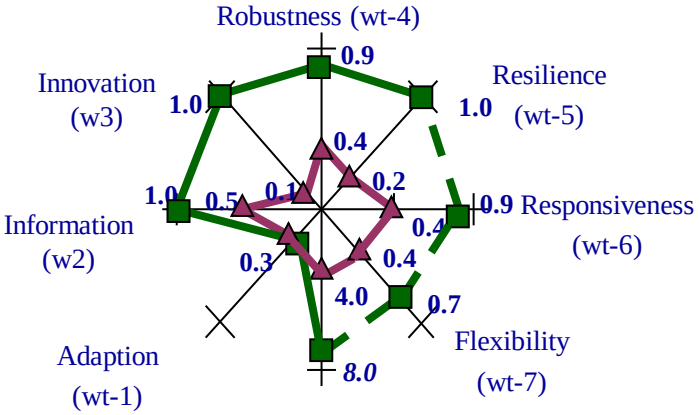
Mathematical Representation
- Cyber Agility and "The Loop" -



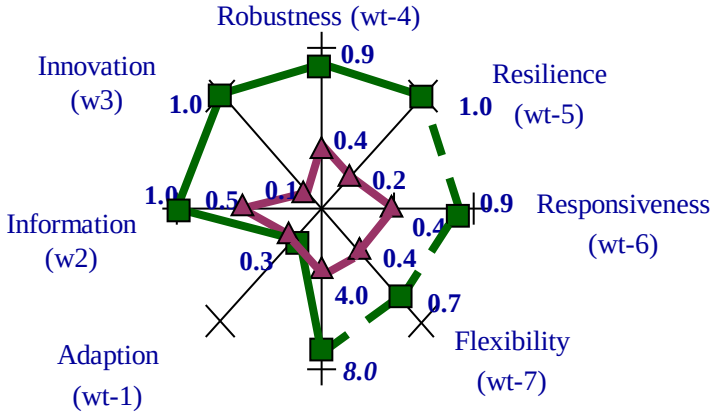
a) Resultant "BEFORE" Effectiveness With Risk



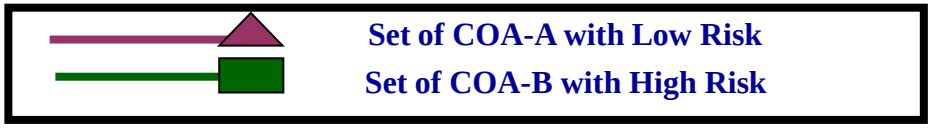
c) Resultant "ON" Effectiveness With Risk



b) Resultant "AFTER" Effectiveness With Risk

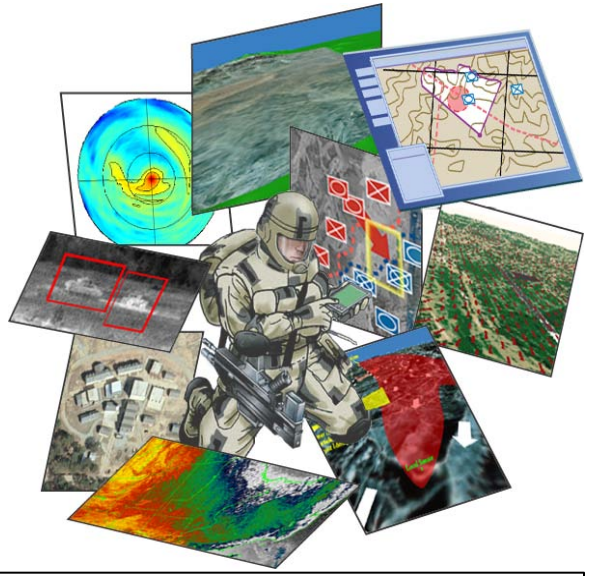


d) Resultant "IN" Effectiveness With Risk

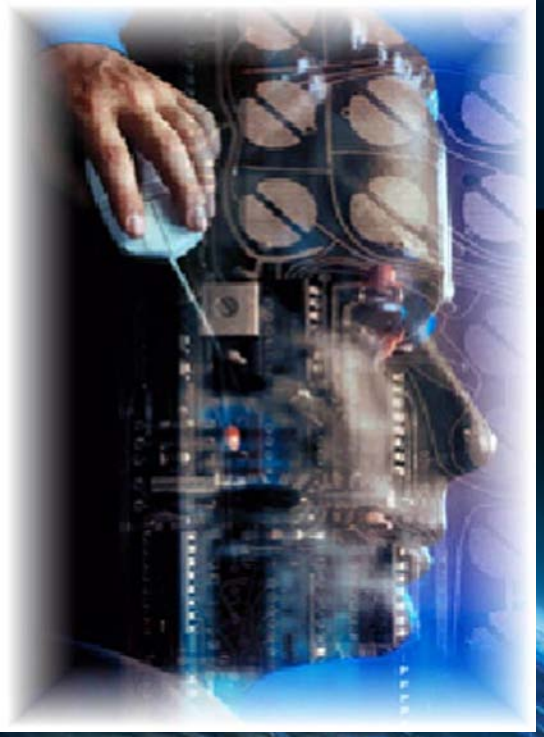


Conclusions

- Human-BEFORE-the-Loop performs better:
  - When conducting Discovery and Prediction
- Human-ON-the-Loop performs better:
  - When periodic "Decision Injections" are required
- Human-IN-the-Loop performs better:
  - When Time is not a critical factor
- Human-AFTER-the-Loop performs better:
  - When conducting detailed Assessments



Human-IN-the-Loop is worst case for optimal "Cyber Agility"



Questions?

AFRL “Inside”