Integrating the Workforce into the National Security System

Nancy J. Cooke

Human Systems Engineering

ARIZONA STATE UNIVERSITY

January 24, 2018

National Academies of Science, Engineering, and Medicine

Overview

- What is HSI?
  - How is HSI different from human factors?
  - Characteristics of HSI
- HSI and National Security Challenges and Solutions
- An HSI Approach to Improving Cyber Security Analysis
- Conclusion

What is Human Systems Integration?

Human-Systems Integration (HSI) is a framework in which human capabilities and limitations across various dimensions are considered in the context of a dynamic system of people, technology, environment, tasks, and other systems with the ultimate goal of achieving system resilience and adaptation, approaching joint optimization.

The human dimensions considered include human factors, manpower, training, personnel, safety, survivability, and habitability.

How is HSI Different from Human Factors?

- ❖ HSI is more than Human Factors → Human-centered systems engineering
- ❖ But…Human Factors has always been a proponent of a systems approach
  - Yes, but the systems have typically been narrow in scope
  - …And the methods are suited for smaller systems
- ❖ Human-Machine Interface→ System →System of systems
  - Human-computer interface→ Nuclear control room
  - Shipboard radar interface →Shipboard command and control
  - Design of medical device →Coordination of patient care
  - Unmanned aerial system ground control station → Integration of UAS
  - into the National Airspace

Characteristics of HSI

- Appreciation for multidisciplinarity
- Appreciation for a systems perspective
- Value of HSI

Appreciation of Multidisciplinarity

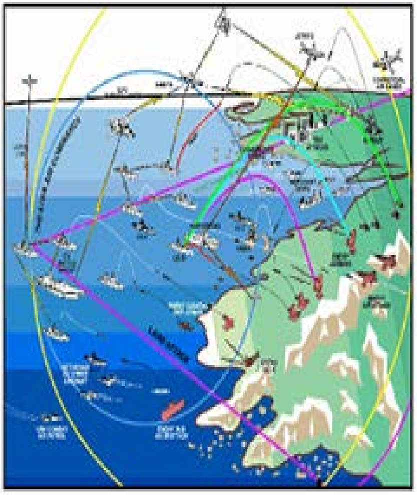
With such a broad array of human considerations coupled with their integration into complex and dynamic systems, it is essential that multiple disciplines (including social sciences) collaboratively address HSI problems (including cognitive psychologists, industrial engineers, system engineers, physicians, sociologists, organizational psychologists, etc.)

ENHANCING THE EFFECTIVENESS OF
TEAM SCIENCE
NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

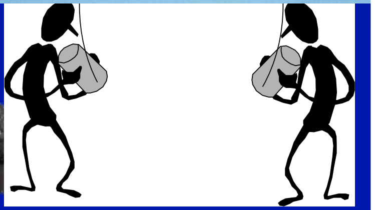
2015

When the Larger System is Not Considered…
There is potential for unintended consequences

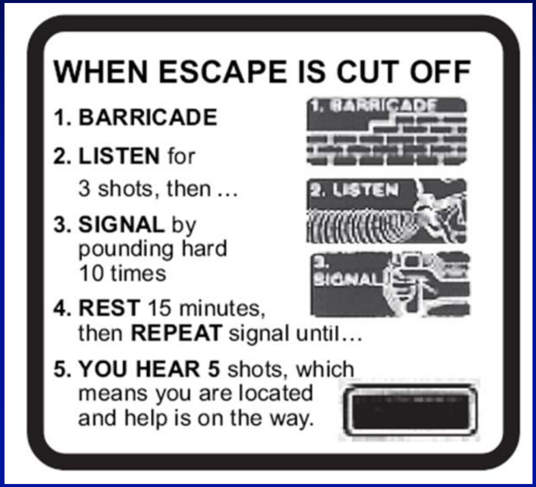
Multiple UAS Control and Sensor Data Proliferation



Laptop UAS Controller that Lacks Communication Device



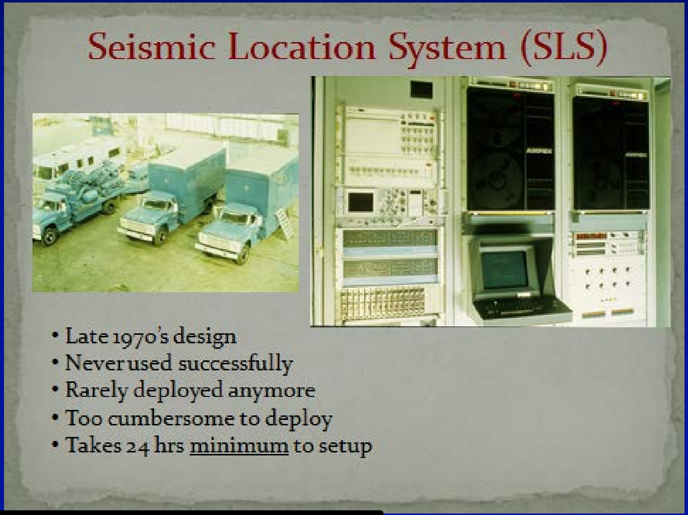
When the Larger System is Not Considered…
There is potential for unintended consequences



WHEN ESCAPE IS CUT OFF

1. BARRICADE
2. LISTEN for 3 shots, then …
3. SIGNAL by pounding hard 10 times
4. REST 15 minutes, then REPEAT signal until…
5. YOU HEAR 5 shots, which means you are located and help is on the way.

1. BARRICADE
2. LISTEN
3. SIGNAL



Seismic Location System (SLS)

- Late 1970's design
- Never used successfully
- Rarely deployed anymore
- Too cumbersome to deploy
- Takes 24 hrs minimum to setup

The system as defined here is the mining community including the mining industry, equipment suppliers, state, and federal governments.

The mitigation of any one of multiple failures at Sago would have likely resulted in all of the miners safely exiting the mine (and we would have never heard anything about the accident).

How many other mine incidents/accidents approach this tipping point but don’t result in a disaster?

Sago Mine Disaster

The Perfect Storm of HSI Failures

The Value of HSI

- HSI when done early in system development
  - Can avoid unintended consequences
  - Can make systems more effective
  - Can save money
- USAF estimates that not doing HSI can increase life cycle system costs by 35–70%

An Airport Incident Command Center

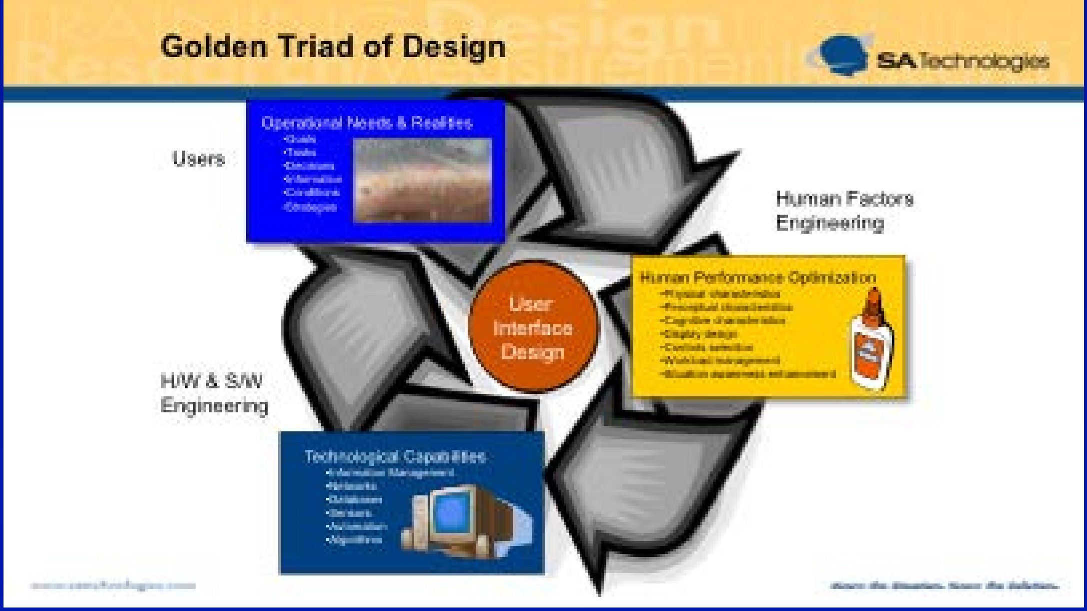
HSI and National Security Challenges

- ❖ Need for integrating selection, training, and work requirements across enterprise
- ❖ Technology is often pushed on users
  - Much technology is not used or useful according to the analysts
  - The need for better technology to aid the analyst
  - Challenge of a confederation of tools individualized for each analyst
- ❖ Push for increasing automation of analyses
  - Automation changes the user’s task
  - Automation can lead to complacency, misuse, and distrust Need for multidisciplinary teaming and communication
- ❖ Collaboration tools needed
  - Collaboration tools do not work well
  - Tools do not overcome stove pipe problem
  - Classification level is an issue

HSI Solutions for National Security Challenges

- ❖ HSI to understand larger system and interdependencies
  - Selection x Training x Technologies
  - Teamwork x Classification x Workload x Technologies
- ❖ HSI as the “glue” : CIA reports need for IC-savvy methodologists to work with those developing tools to better integrate IC with technology

- ❖ Golden Triad of Design
  - Engineers
  - HSI Specialists – the glue
  - Users (IC)



An HSI Approach to Improving Cyber Security Analysis

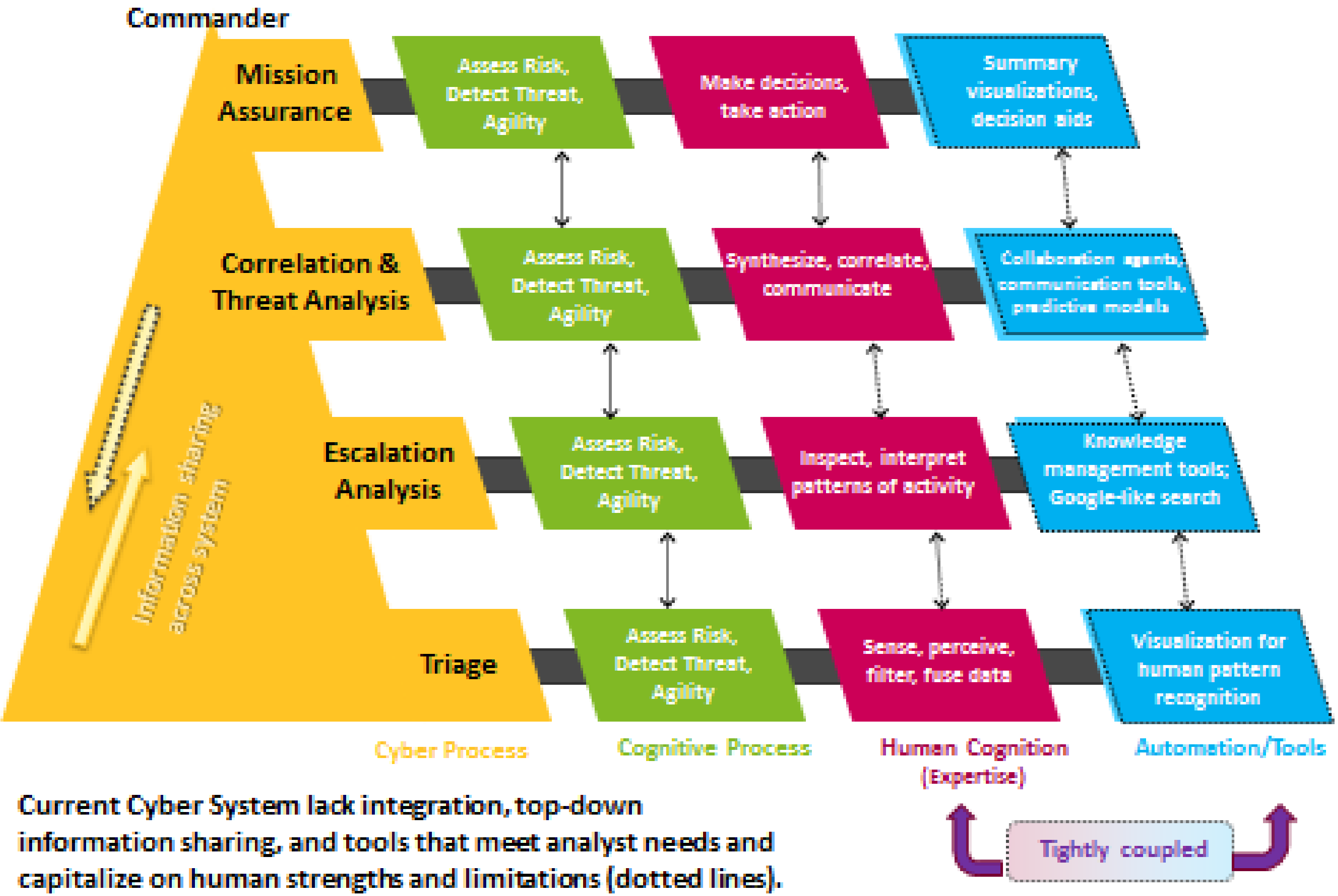
- Understanding system through…
  - Cognitive task analyses
  - Interviews
  - CTF observations
  - Surveys
  - Modeling
- Empirical testing of hypotheses and possible interventions in testbeds
- Extension of empirical results through Agent-Based Modeling

Supported by Army Research Office MURI grant

Cyber Defense as a Sociotechnical System

- Cyber defense functions involve cognitive processes allocated to
  - Human Operators
  - Tools/Algorithms
- Human Operators
  - Different roles and levels in hierarchy
  - Heterogeneity (Information, skills and knowledge)
- Tools
  - For different kinds of data analysis and visualization
  - For different levels of decision making
- Together, human operators and tools are a sociotechnical system

Cyber Security Analysis as a Sociotechnical System


Commander
Mission Assurance
Assess Risk, Detect Threat, Agility
Make decisions, take action
Summary visualizations, decision aids
Correlation & Threat Analysis
Assess Risk, Detect Threat, Agility
Synthesize, correlate, communicate
Collaboration agents, communication tools, predictive models
Escalation Analysis
Assess Risk, Detect Threat, Agility
Inspect, interpret patterns of activity
Knowledge management tools; Google-like search
Information sharing across system
Triage
Assess Risk, Detect Threat, Agility
Sense, perceive, filter, fuse data
Visualization for human pattern recognition
Cyber Process
Cognitive Process
Human Cognition (Expertise)
Automation/Tools
Tightly coupled

Current Cyber System lack integration, top-down information sharing, and tools that meet analyst needs and capitalize on human strengths and limitations (dotted lines).

EAST

Event Analysis of Systemic Teamwork framework

(Stanton, Baber, & Harris, 2012)

- Integrated suite of methods allowing the effects of one set of constructs on other sets of constructs to be considered
  - Make the complexity of socio-technical systems more explicit
  - Interactions between sub-system boundaries may be examined
  - Reduce the complexity to a manageable level
- Social Network
  - Organization of the system (i.e., communications structure)
  - Communications taking place between the actors working in the team.
- Task Network
  - Relationships between tasks
  - Sequenced interdependences of tasks
- Information Network
  - Information that the different actors use and communicate during task performance

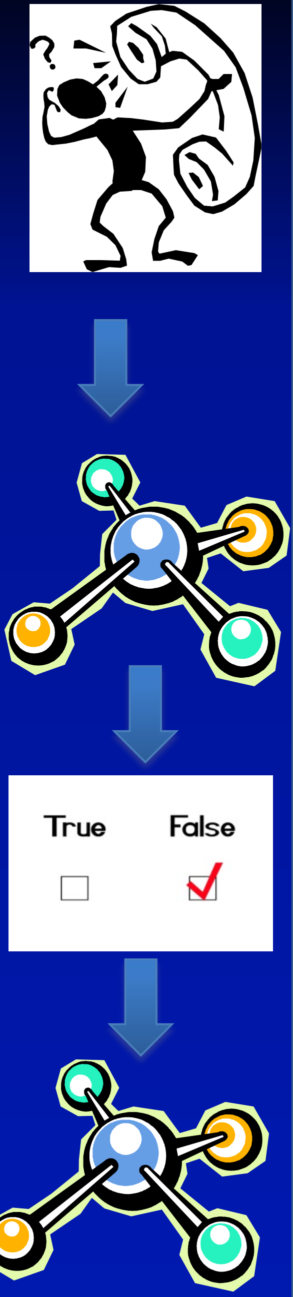
EAST Approach

❖ Interviews with cyber network defense leads from two organizations on social structure, task structure, and information needs

❖ Hypothetical EAST models created

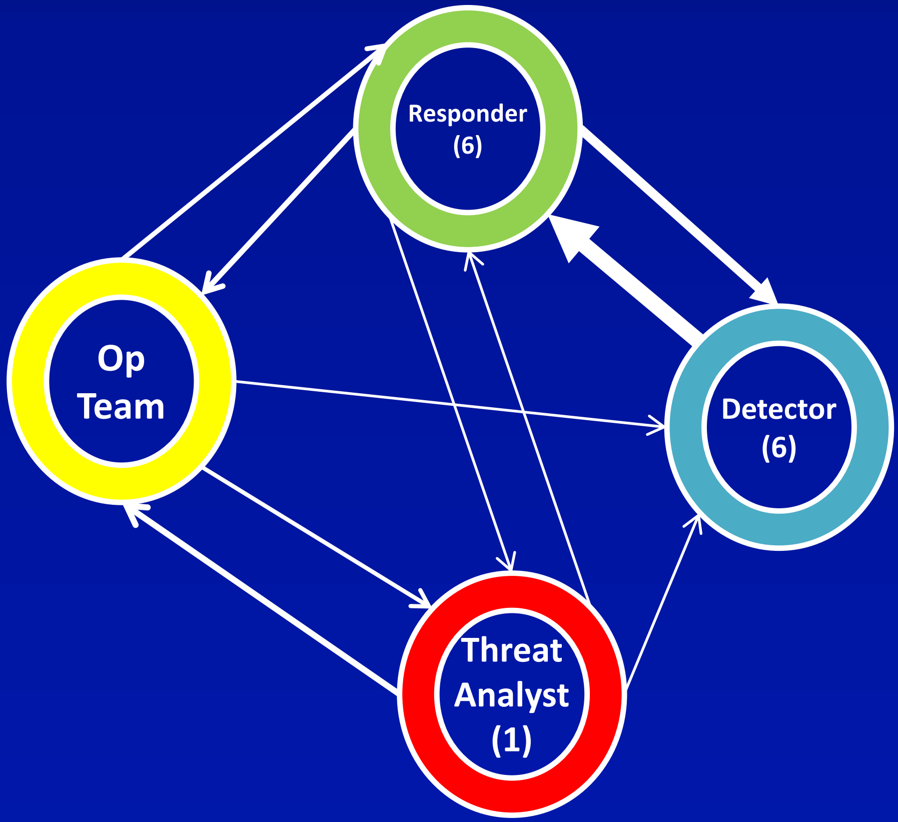
❖ Surveys specific to organization for cyber defense analysts developed

❖ Surveys administered to analysts in each organization to refine models

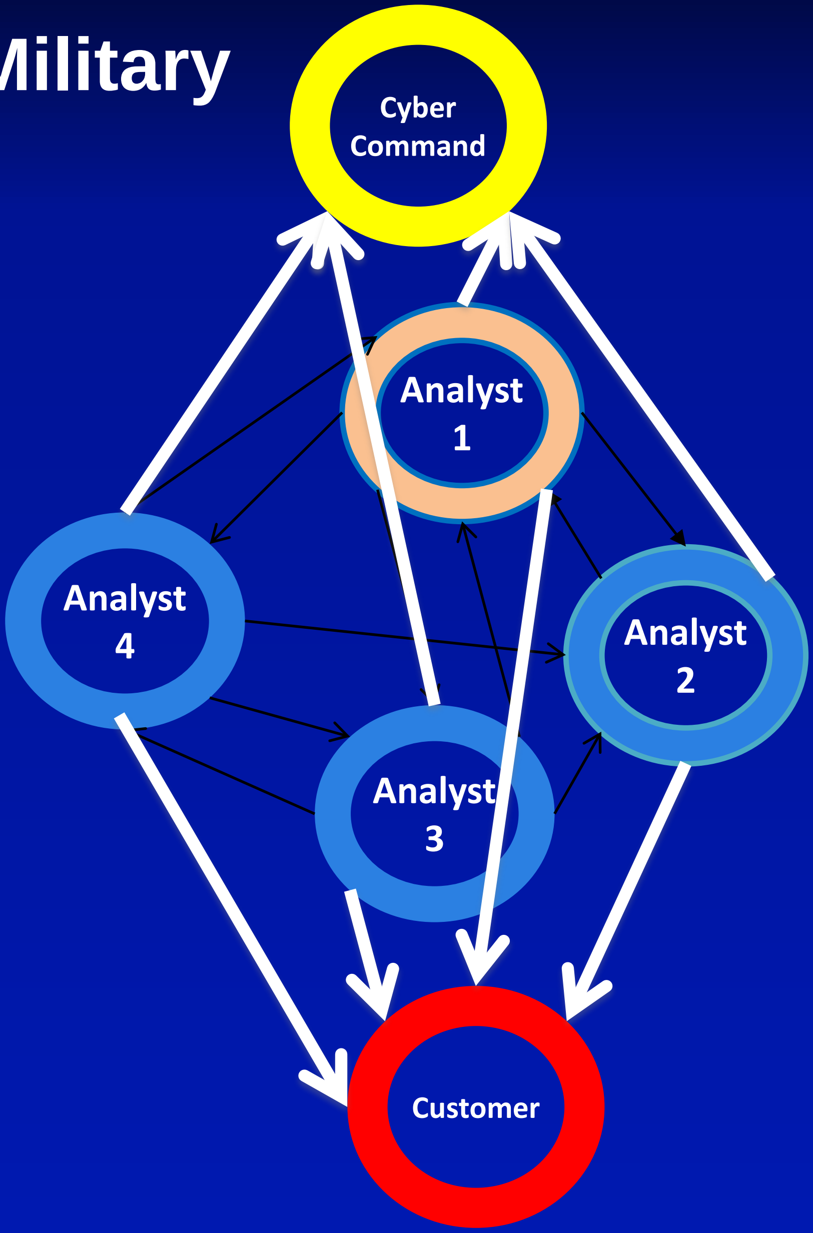


Social Network Diagrams of Incident Response/Network Defense Teams

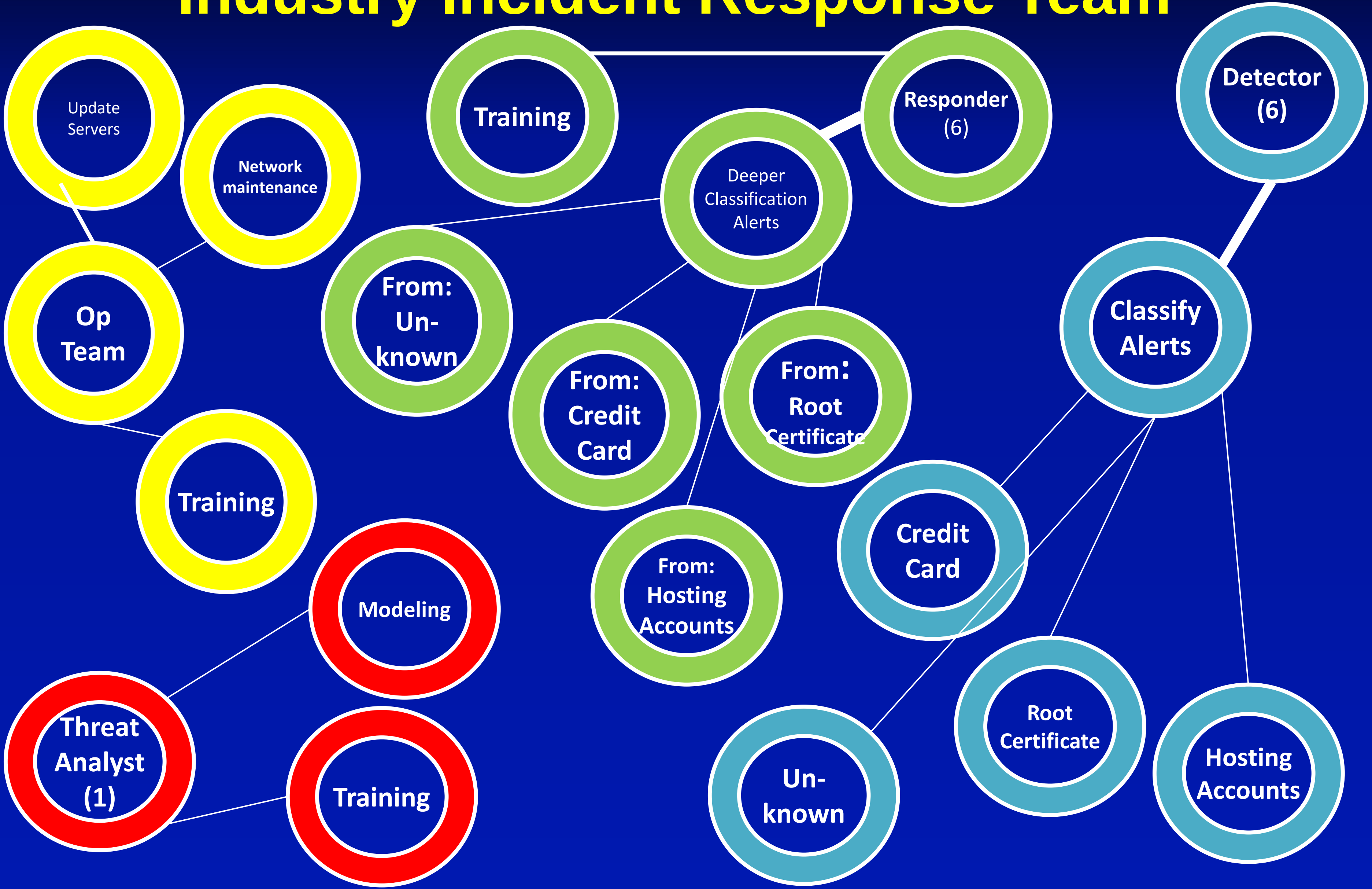
Industry



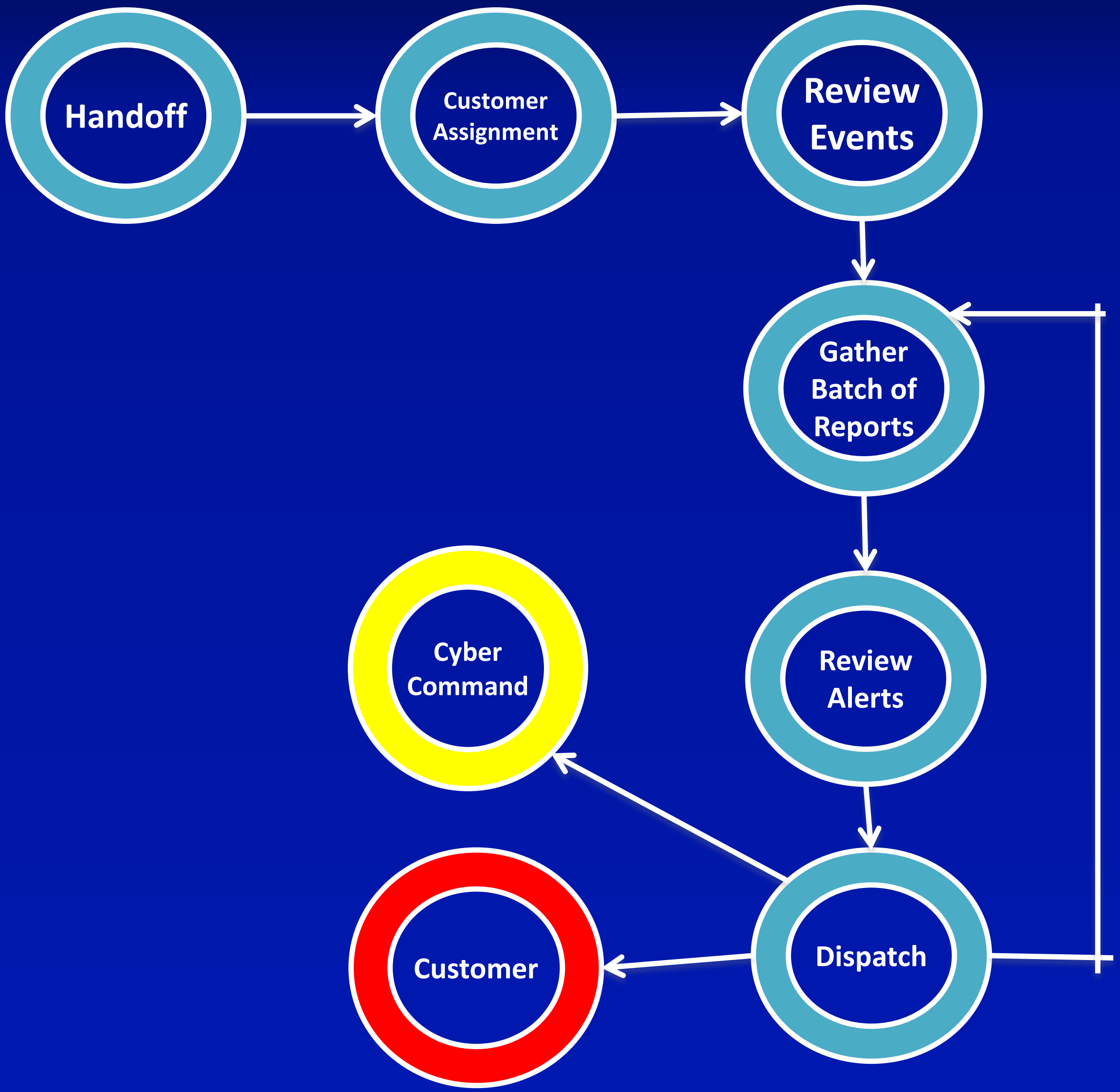
Military



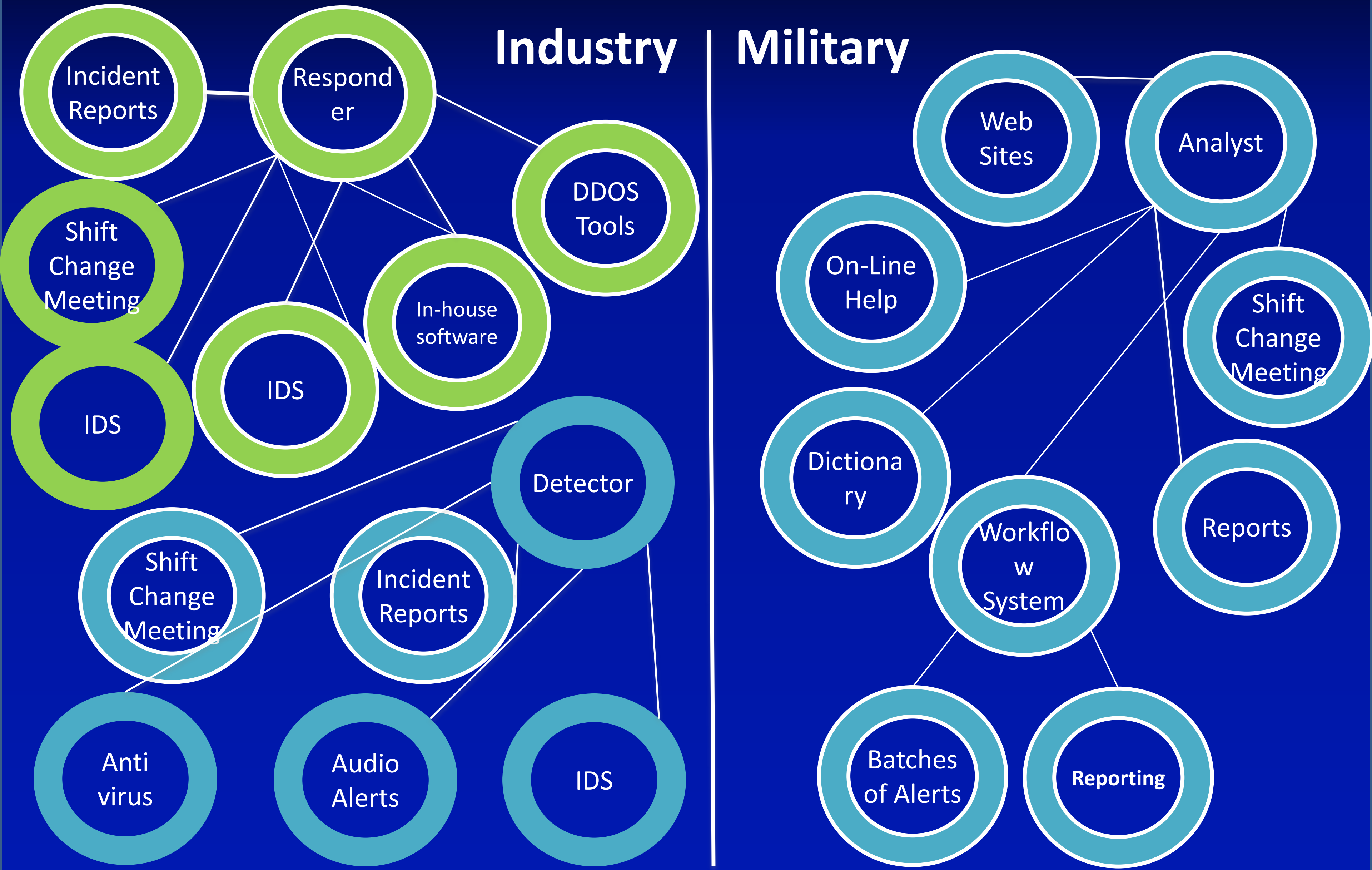
Sequential Task Network Diagram
Industry Incident Response Team



Sequential Task Network Diagram
Military Network Defense Team



Information Network Diagram of Incident Response/Network Defense Teams



Empirical Study on Teams vs. Groups

- Cyber analysts work as a group – Not as a team

❖ From CTA

- Collaboration among cyber operators is minimal
- Little role differentiation
- Bottom-up information flow

❖ Hypothesized Reasons

- Cognitive overload
- Organizational reward structures
- “Knowledge is Power”
- Lack of effective collaboration tools

Hypotheses

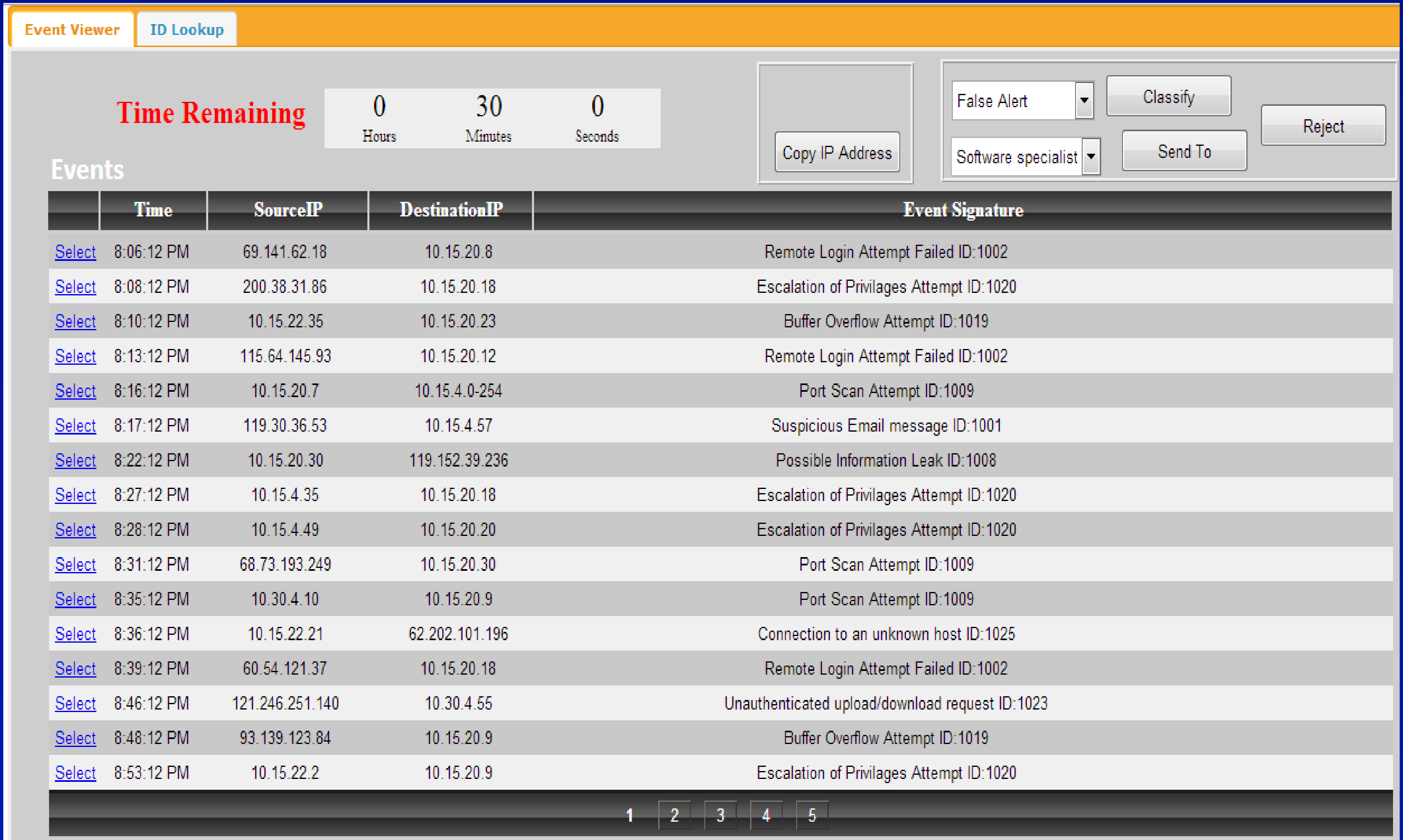
- Reward structures conducive to team work in cyber defense analyst groups performing triage level analysis will lead to higher signal detection performance.
- Improving interactions between analysts (micro level) can improve overall cyber defense performance (macro level emergence)

CyberCog -Synthetic Task Environment

- ❖Task: team based triage analysis using CyberCog
- ❖Synthetic Task Environment
  - Simulation environment
  - Recreate team and cognitive aspects of the task

Synthetic task environment

CyberCog STE Alert Screen



False Alert

Software specialist

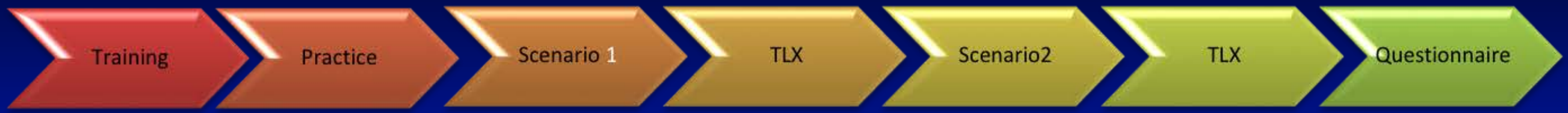
Time Remaining 0 Hours 30 Minutes 0 Seconds

Events

	Time	SourceIP	DestinationIP	Event Signature
Select	8:06:12 PM	69.141.62.18	10.15.20.8	Remote Login Attempt Failed ID:1002
Select	8:08:12 PM	200.38.31.86	10.15.20.18	Escalation of Privilages Attempt ID:1020
Select	8:10:12 PM	10.15.22.35	10.15.20.23	Buffer Overflow Attempt ID:1019
Select	8:13:12 PM	115.64.145.93	10.15.20.12	Remote Login Attempt Failed ID:1002
Select	8:16:12 PM	10.15.20.7	10.15.4.0-254	Port Scan Attempt ID:1009
Select	8:17:12 PM	119.30.36.53	10.15.4.57	Suspicious Email message ID:1001
Select	8:22:12 PM	10.15.20.30	119.152.39.236	Possible Information Leak ID:1008
Select	8:27:12 PM	10.15.4.35	10.15.20.18	Escalation of Privilages Attempt ID:1020
Select	8:28:12 PM	10.15.4.49	10.15.20.20	Escalation of Privilages Attempt ID:1020
Select	8:31:12 PM	68.73.193.249	10.15.20.30	Port Scan Attempt ID:1009
Select	8:35:12 PM	10.30.4.10	10.15.20.9	Port Scan Attempt ID:1009
Select	8:36:12 PM	10.15.22.21	62.202.101.196	Connection to an unknown host ID:1025
Select	8:39:12 PM	60.54.121.37	10.15.20.18	Remote Login Attempt Failed ID:1002
Select	8:46:12 PM	121.246.251.140	10.30.4.55	Unauthenticated upload/download request ID:1023
Select	8:48:12 PM	93.139.123.84	10.15.20.9	Buffer Overflow Attempt ID:1019
Select	8:53:12 PM	10.15.22.2	10.15.20.9	Escalation of Privilages Attempt ID:1020

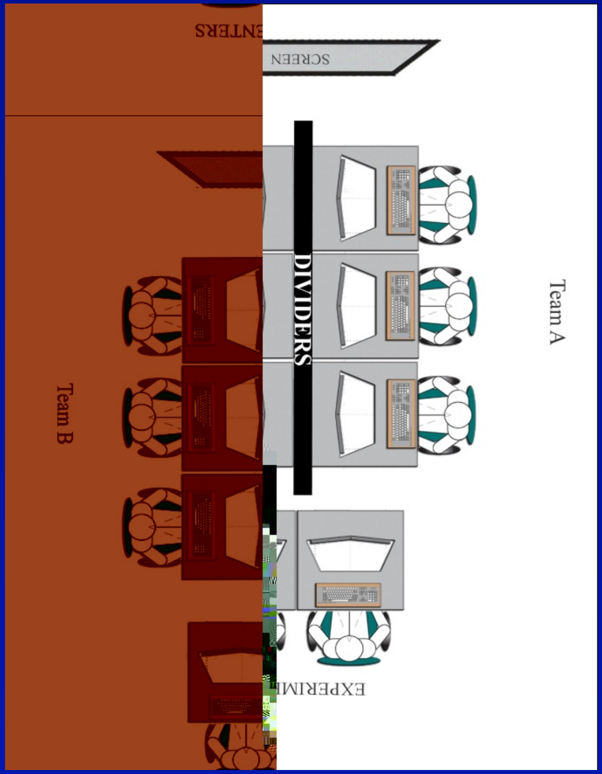
1 2 3 4 5

The Experiment



Training → Practice → Scenario 1 → TLX → Scenario2 → TLX → Questionnaire

- 3-person teams/groups in which each individual is trained to specialize in types of alerts
- 2 conditions:
  - Team Work (Primed & Rewarded for team work)
  - Group Work (Primed & Rewarded for group work)
- 6 individuals at a time
  - Team Work - Competition between the 2 teams
  - Group Work - Competition between the 6 individuals
- Experimental scenarios:
  - 225 alerts
  - Feedback on number of alerts correctly classified - constantly displayed on big screen along with other team or individual scores
- Measures
  - Signal Detection Analysis of Alert Processing
  - Amount of Communication
  - Team situation awareness
  - Transactive Memory
  - NASA TLX – workload measure

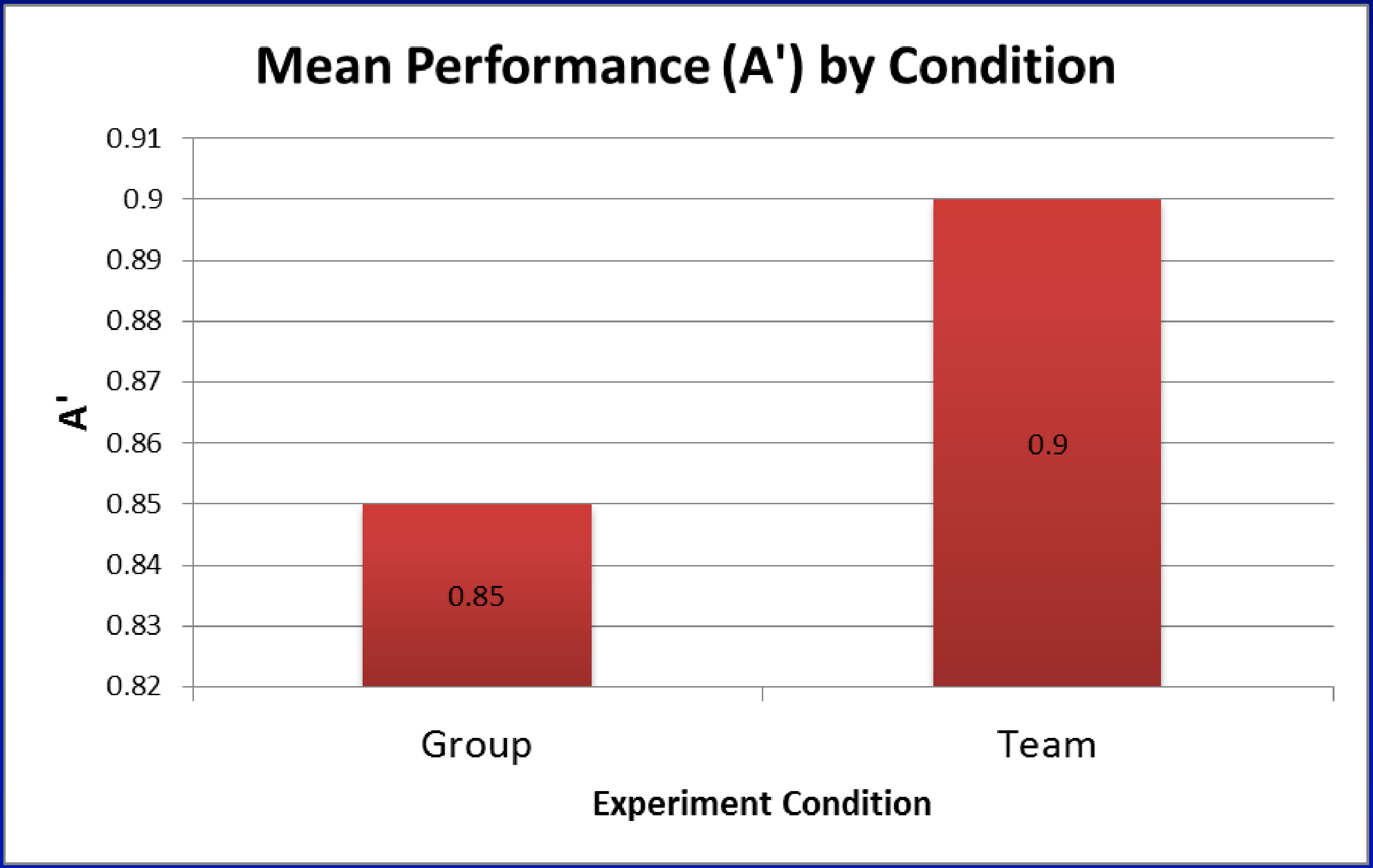


Cyber Teaming is Beneficial for Analyzing Novel and Difficult Alerts

- Working as team helps when alerts are novel and involve multi step analysis, not otherwise.
- Signal Detection Measure: A' as performance measure
- A' ranges from values 0.5 and 1 with 0.5 indicating lowest performance possible and 1 indicating highest performance possible.

Cyber Teaming Helps When the Going Gets Rough

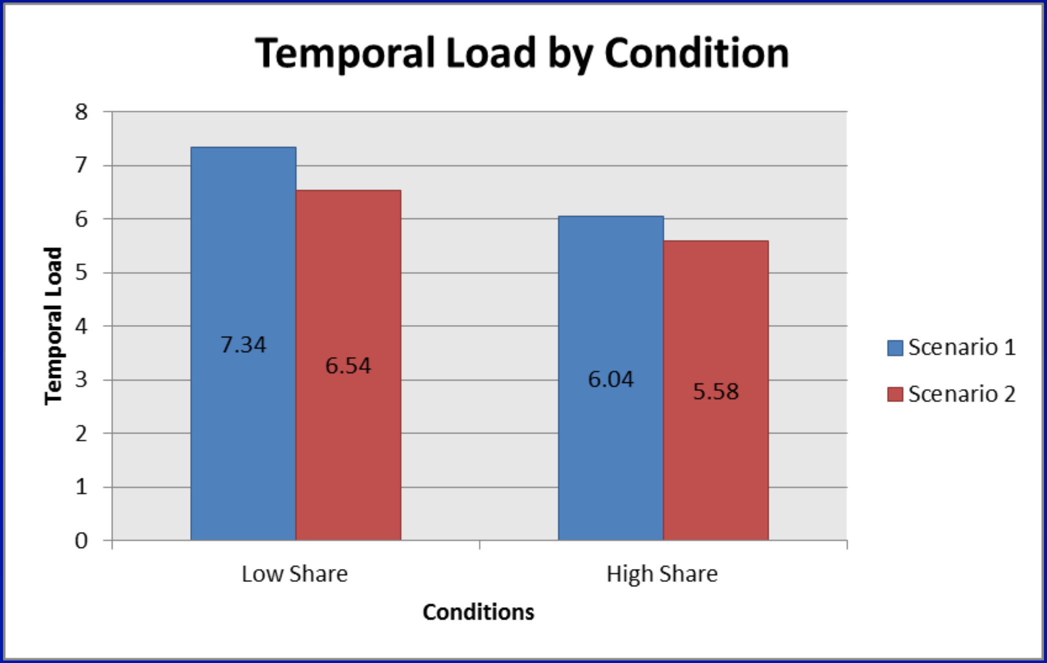
Sensitivity to true alerts



F(1,18) = 5.662, *p* = .029** (Significant effect of condition)

Groups that Share Less Information Perceive More Temporal Demands than High Sharers

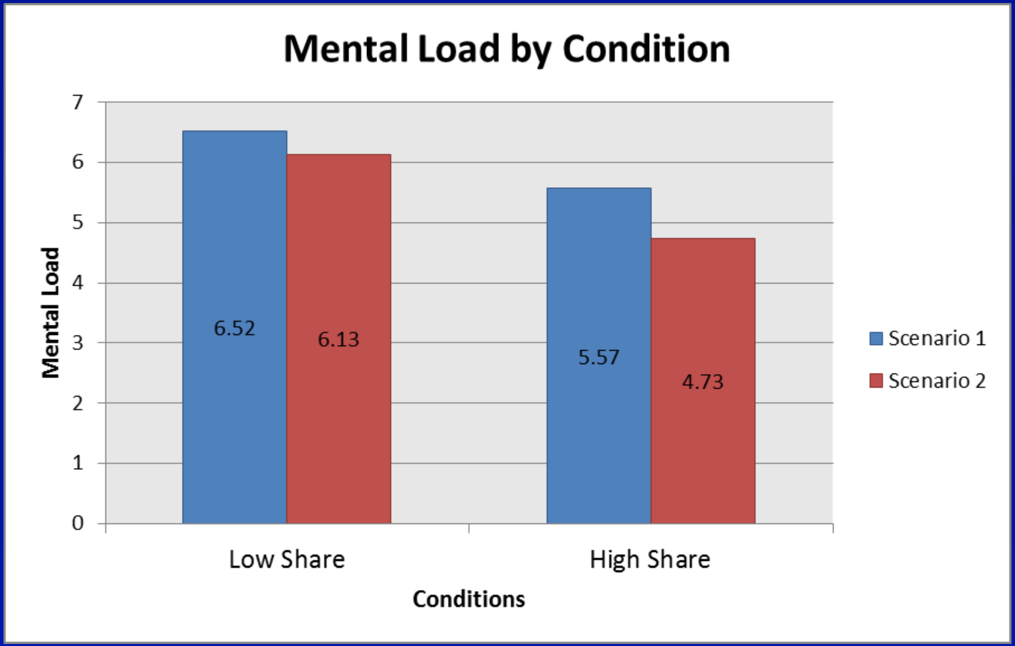
- NASA TLX Workload Measure: Temporal Demand
- Measures perception of time pressure
- Higher the value higher the task demand



Statistically significant across scenarios and conditions (p-value = 0.020)

Groups that Share Less Information Perceive Work to be More Difficult than High Sharers

- NASA TLX Workload Measure: Mental Effort
- Measures perception of mental effort
- Higher the value, more mental effort required



Statistically significant across scenarios and conditions (p-value = 0.013)

Additional Results from Other Cyber Studies

- Collaboration also comes with biases
  - Information Pooling Bias
  - Collaboration Tool Developed to Address Bias shown to be effective
- Agent-based models extend benefit of teaming to larger scale teams

HSI Cyber Security Conclusions

- There is a need to break the “Silos”
- Use the power of human teams to offset information overload problems in cyber defense
- Simply encouraging and training analysts to work as teams and providing team level rewards can lead to better triage performance
- Need collaboration tools and group decision making systems

HSI and National Security

- HSI can benefit the National Security System by
  - Understanding system interdependencies
  - Avoiding unintended consequences
  - Aligning technology with IC need and capabilities
- IF…
  - HSI is considered early in system design, technology acquisition and throughout the system life cycle
  - And HSI process includes IC
- The cost of not doing HSI can be 35-70% of system life-cycle costs
- The benefits of doing HSI include more effective system and national security

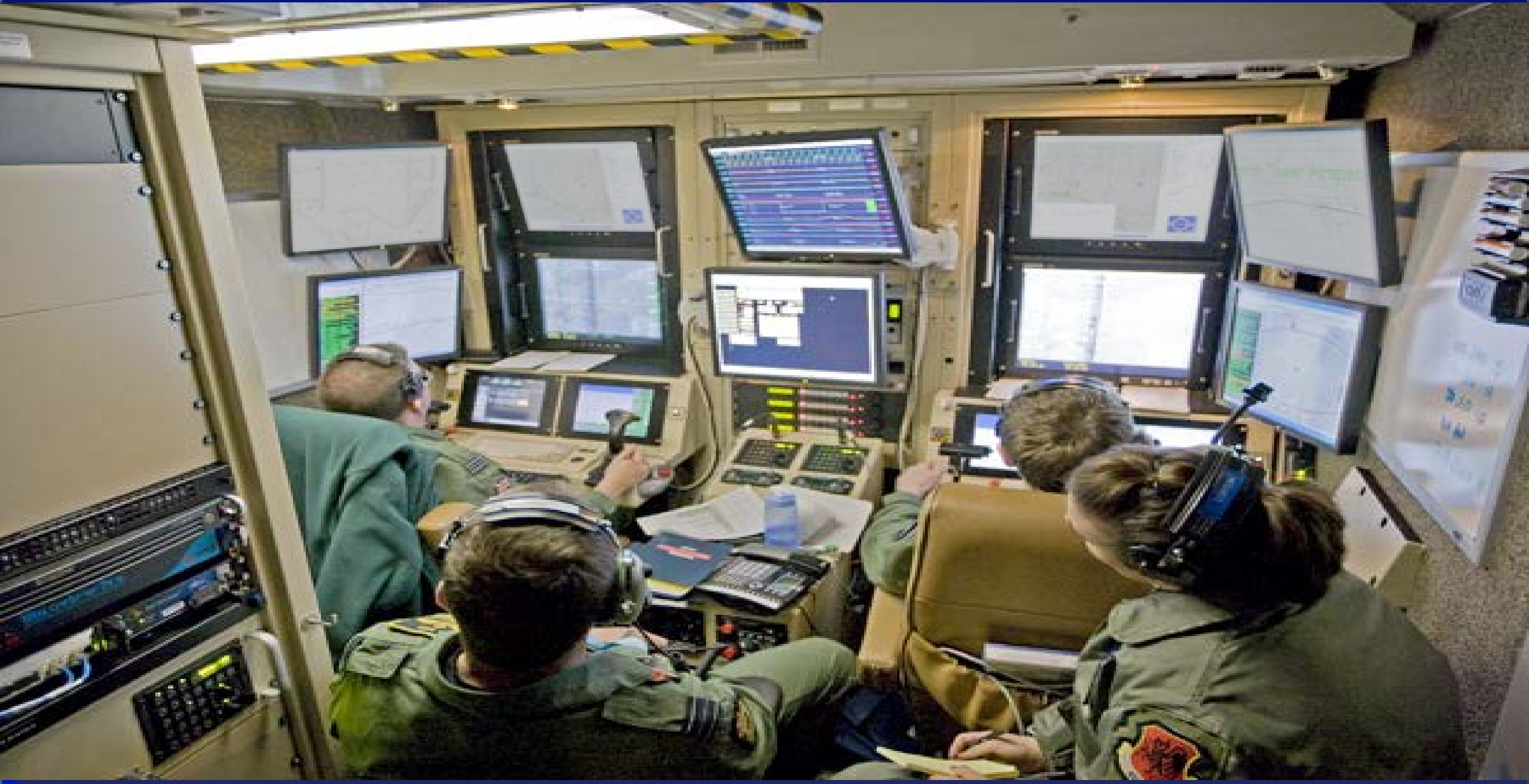
Thank You!

Nancy J. Cooke

ncooke@asu.edu

Back-up Slides

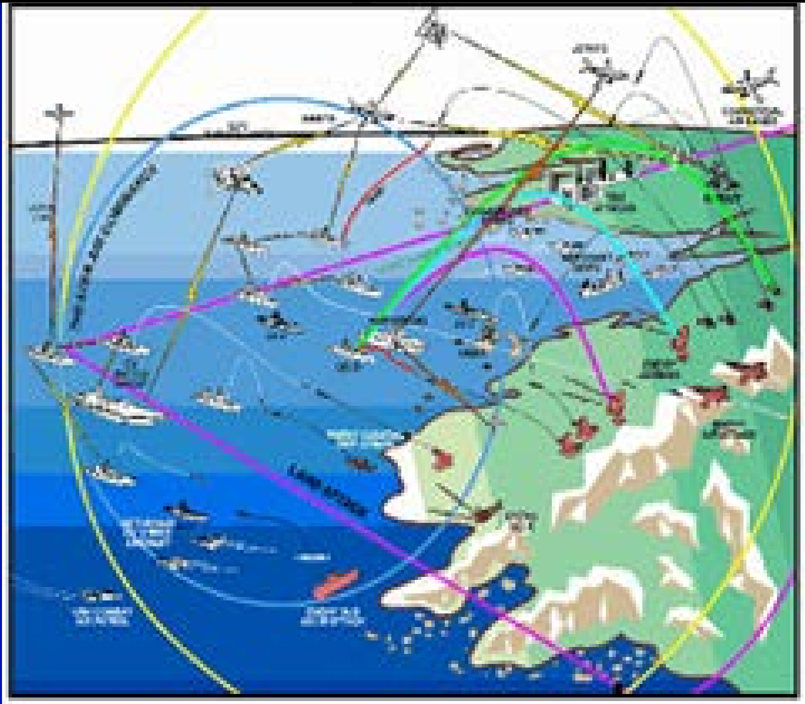
An Example from My Work: MQ-1/9 Operator Control Station



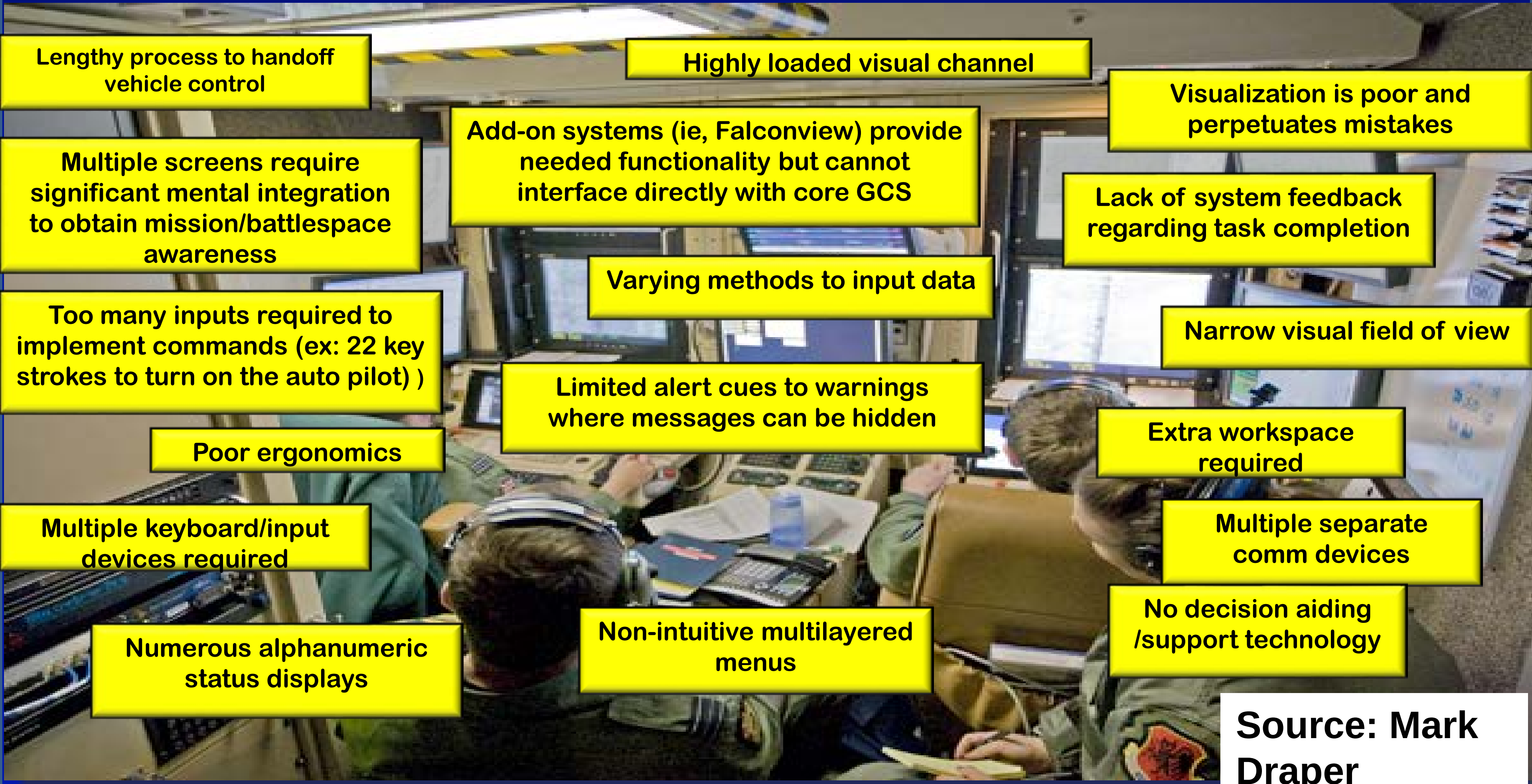
UAV vs. UAS

- A system that includes the vehicle, the ground control station, and the payload which is typically part of a larger system → e.g., NAS

- And the human is an important part of that system



HF/E Issues with the MQ-1/9 Operator Control Station



Lengthy process to handoff vehicle control

Multiple screens require significant mental integration to obtain mission/battlespace awareness

Too many inputs required to implement commands (ex: 22 key strokes to turn on the auto pilot))

Poor ergonomics

Multiple keyboard/input devices required

Numerous alphanumeric status displays

Highly loaded visual channel

Add-on systems (ie, Falconview) provide needed functionality but cannot interface directly with core GCS

Varying methods to input data

Limited alert cues to warnings where messages can be hidden

Non-intuitive multilayered menus

Visualization is poor and perpetuates mistakes

Lack of system feedback regarding task completion

Narrow visual field of view

Extra workspace required

Multiple separate comm devices

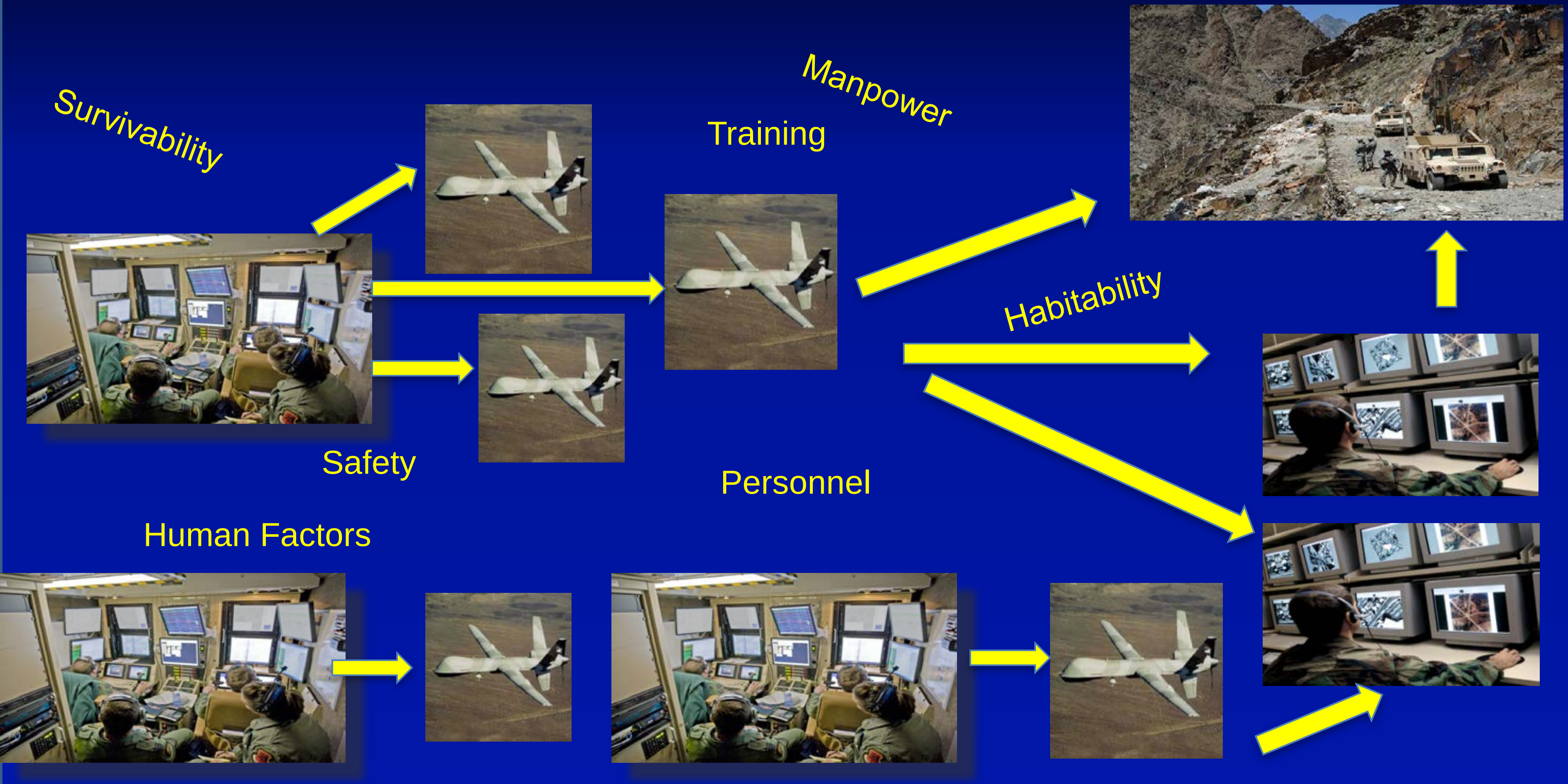
No decision aiding /support technology

Source: Mark Draper

MQ-1/9 Operator Control Station

<u>Industry program officer:</u> “It has been 10 years now since the Predator has been fielded and it might be time to start thinking about human factors.”

HSI ISSUES



Manpower

Survivability

Training

Habitability

Safety

Personnel

Human Factors