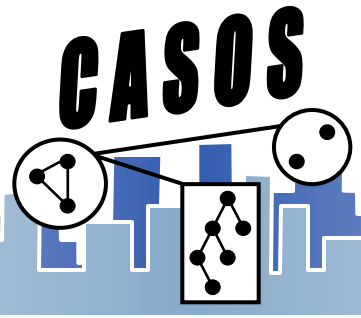


Social Network Modeling and Simulation of Integrated Resilient Command and Control (C2) in Contested Cyber Environments

Prime Award: FA8750-08-2-0020
Sub-Award: E2016762

Michael J. Lanham
Geoffrey P. Morgan
Kathleen M. Carley

DTRA
HDTRA11010102

MURI: FA9550-05-01-0388

Carnegie Mellon

Center for Computational Analysis of Social and Organizational Systems
http://www.casos.cs.cmu.edu/

Outline

- Problem Statement
- An Approach
  - DoD Background
  - Research Environment
  - Planning Phases
  - Scenarios of Interest
- Model Development
- Assessing Resilience
- Network Analytics
- Diffusion Simulation & Analysis
- Future Work

Problem Statement

- General: How do leaders assess the inter- and intra-organizational resilience of their organization's operations in a contested cyber environment?

- Specific: How does USAF leadership assure itself and its field commanders that its Air Operations Centers can continue to accomplish their missions in contested cyber environments?

Carnegie Mellon
institute for SOFTWARE RESEARCH

An approach to solution(s)

- "What if" system for assessing the impact(s) of different types of cyber attacks on integrated C2 & identifying mitigation strategies
  - Contested cyber environment - Multiple types of attacks
  - Integrated C2 – Alternative organizational structures
    - Doctrine based
    - Human + IT
- Why simulate? Why not inter- and intra-organizational war games, exercises and rehearsals?
  - Expense
    - Must expose broad sets of stakeholders to gauge broad impacts
    - Segregated training environments
  - Training Distractor
  - Extrapolation of lack-of-impact everyday cyber "effects" to long-duration/time-critical impacts
  - Other ideas?

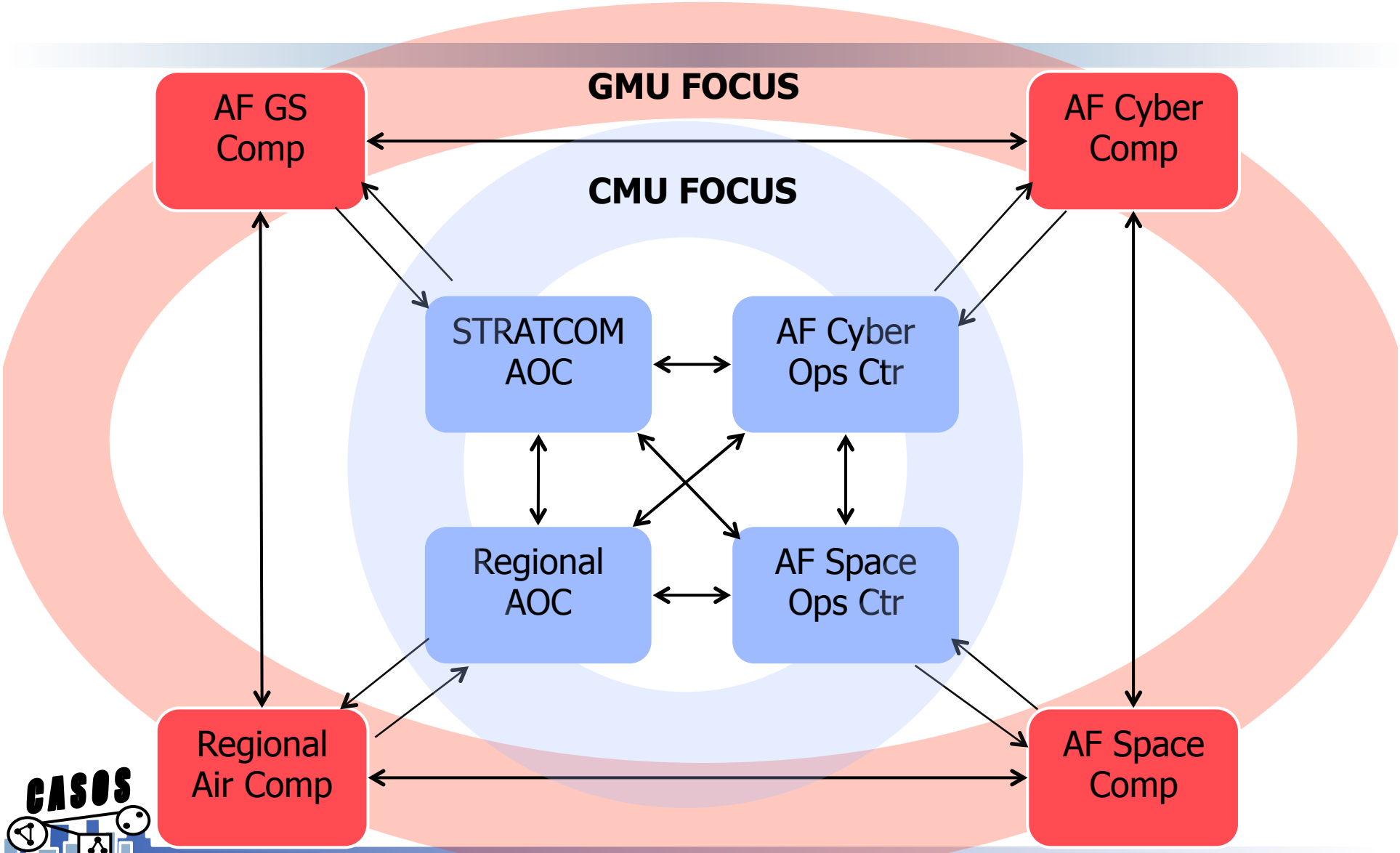
Carnegie Mellon
institute for SOFTWARE RESEARCH

Research Enviroment

- Overall Scenario: four (4) Combatant Commands collaborating on a set of interconnected plans implementing strategic guidance
  - Sub-implementation was at HQs level with colored Petri Nets
  - Sub-implementation was at high-level IT abstraction implemented at packet-level granularity
  - Sub-implementation was with four (4) USAF Air Operations Centers that have to transform "strategic" guidance and plans into orders that set "tactical" efforts in motion
- Model creation via network extraction from USAF Doctrine/texts
- Network analytics using CMU's *ORA*
  - People (and role and groups)
  - IT systems
- Initial dynamic network immediate impact also via ORA for two types of cyber effects: integrity and availability
- More robust dynamic network assessment through agent-based modeling using CMU's *Construct* for same cyber effects: integrity and availability

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Research Enviroment



Carnegie Mellon
institute for SOFTWARE RESEARCH

Scenarios of Interest

- For all scenarios
  - The AOC is engaged in planning
    - Critical to getting an integrated COA
  - Joint Planning Group (JPG) has received a mission order (the OPORD) – task is to distribute that mission order to others within the AOC and gain their input, plan how to meet the intent of the OPORD
- Network Structures
  - Uncontested Cyber Environment - "Normal"
    - Doctrine documents to define agent structure.
    - Doctrine documents and SMEs to define available IT and human to IT links
    - 5 Communication networks – SIPR, NIPR, VoIP, JWICS and sneaker (face-to-face)
  - Contested Cyber Environments - "Under Attack"
    - The network is changed by a cyber attack.
    - Multiple cyber attack scenarios are considered (e.g. DNS availability, Integrity Attacks, single AOC, multiple AOCs, single IT systems, multiple IT systems)
- Environment Features
  - Communications – Perfect/Damaged/Destroyed
  - Information – accurate or inaccurate

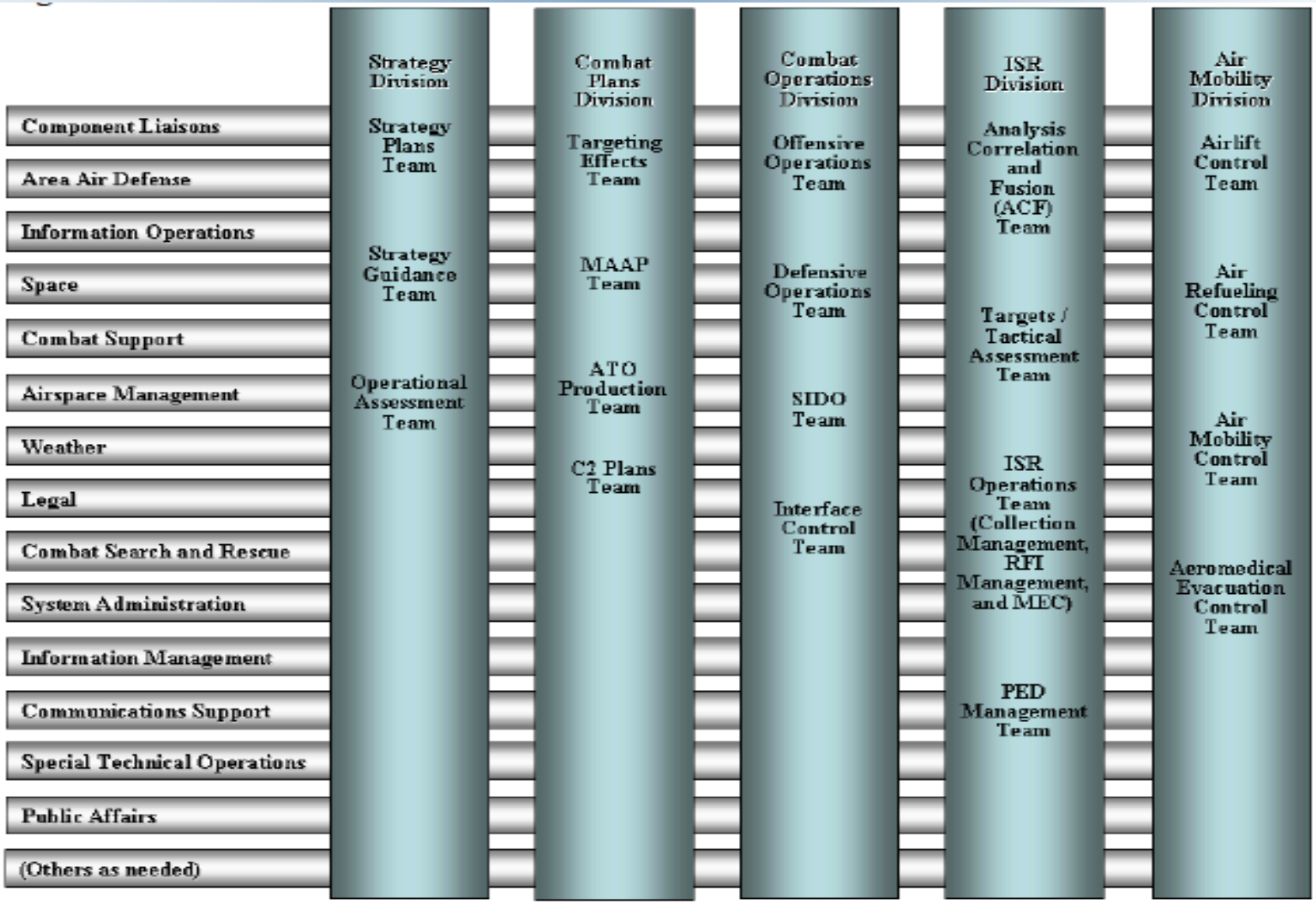
Carnegie Mellon
institute for SOFTWARE RESEARCH

Scenarios (27 cases)

1. Baseline – Normal operations no attacks
2. DNS/Denial of Service
   a. Attack reduces DNS availability by 30%
   b. Attack can be against Regional AOC/All AOCs
   c. Attack can be against TBMCS, GCCS, C2PC, JADOCS or all
   d. Attack can be against limited combos (TG, GC, CJ, TGCJ)
3. Integrity Attack
   a. Attack injects 'bad' JPG knowledge to key IT systems, 2-5 bits per interaction, 2 interactions per turn
   b. Attack can be against Regional AOC/All AOCs
   c. Attack can be against TBMCS, GCCS, C2PC, JADOCS
   d. Attack can be against limited combos (TG, GC, CJ, TGCJ)
4. DNS and Integrity paired in each combination

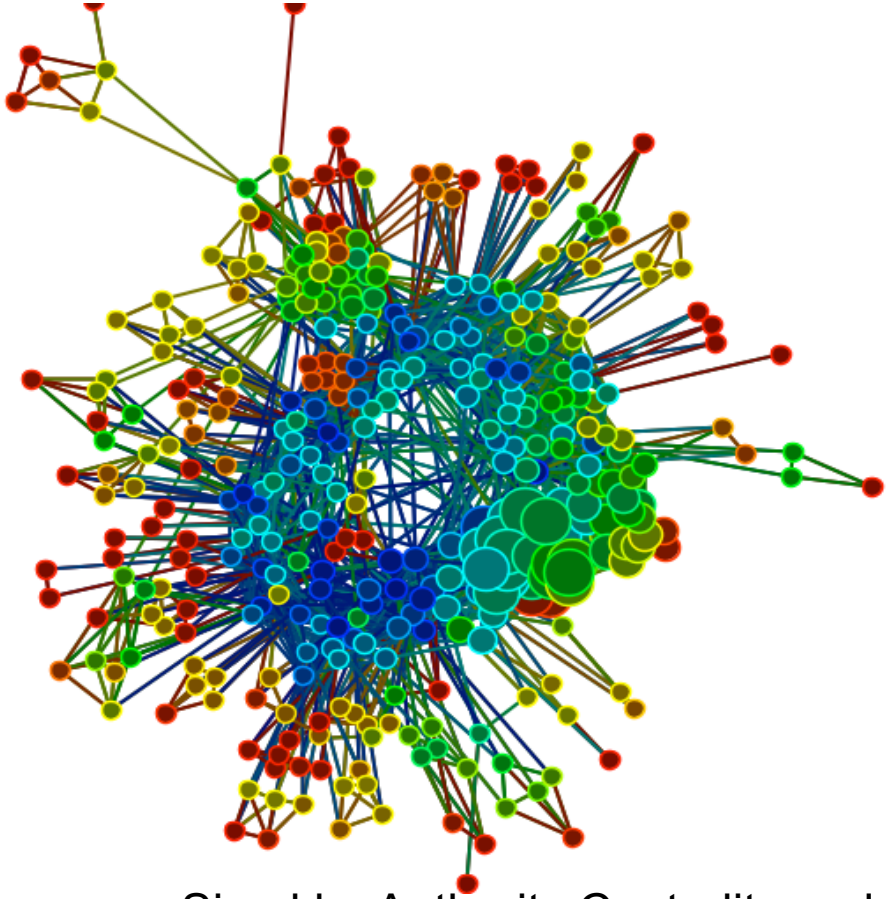
Carnegie Mellon
institute for SOFTWARE RESEARCH

Model Development - AOCS

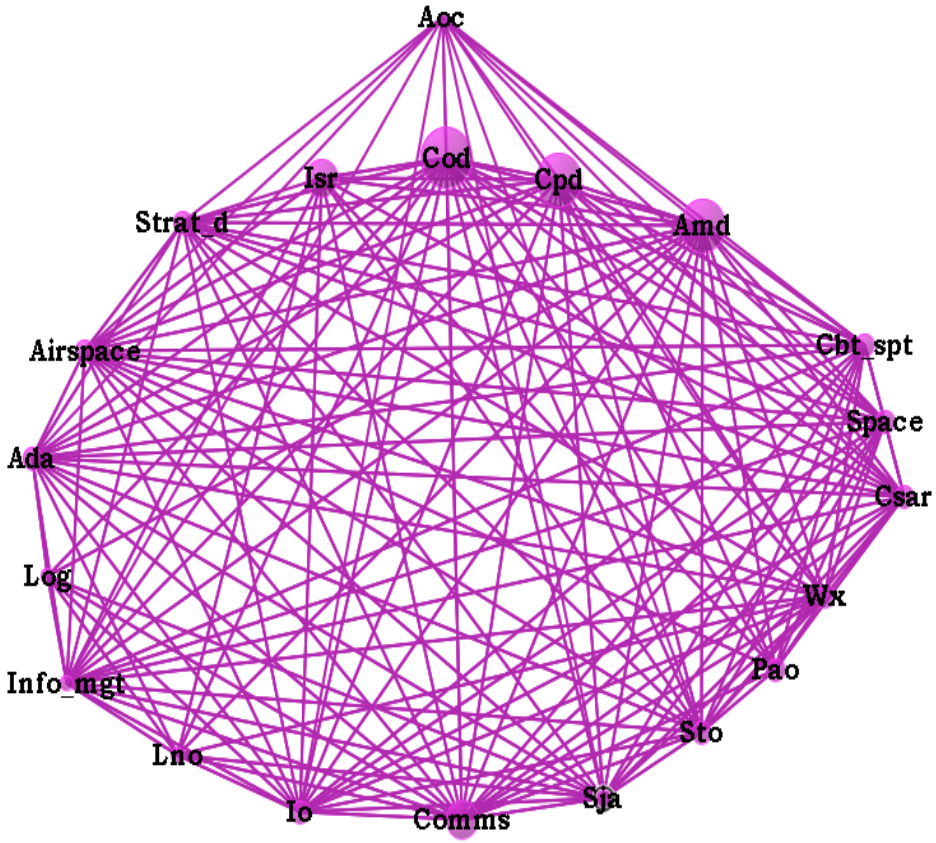


Carnegie Mellon
institute for SOFTWARE RESEARCH

People to People Network Structure for 'Regional AOC'



Sized by Authority Centrality and Colored by Betweeness Centrality (Blue is most central)



Divisions and Functional Groups' Agents collapsed into 'meta-nodes'

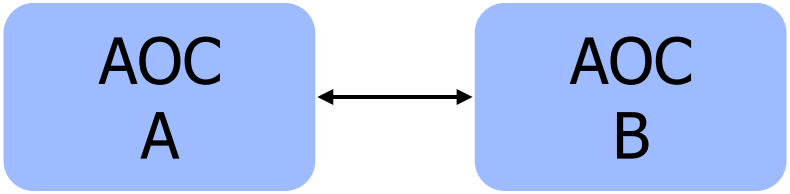
Carnegie Mellon
institute for SOFTWARE RESEARCH

IT Systems

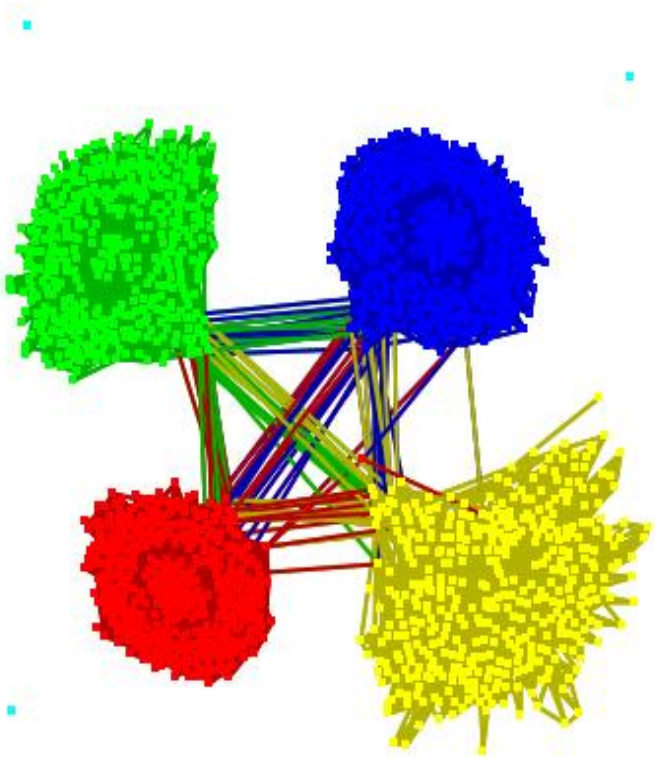
- 468 IT systems in the simulation
  - 117 per AOC
  - Distinct named systems identified in doctrinal references
  - Modeled as "agents" capable of receiving, sending and storing information
  - All are modeled as push agents
- 58 IT resources, not explicitly discussed in doctrine
  - E.g., SIPR, NIPR, JWICS, and VoIP – terminal and phone links
  - These systems don't 'store' knowledge in the sim, but provide mechanisms for agents to communicate with when they are not communicating face-to-face
  - These are modeled as communication modes each of which operates at a particular level of classification, and can be separately attacked

Carnegie Mellon
institute for SOFTWARE RESEARCH

Inter-AOC Communication



- Each division head can send and receive messages from his or her counterpart other AOCs
  - Strategy, Combat Plans, Combat Ops, ISR, Air Mobility
- There are IT to IT direct links between AOCs
  - These are through SIPR, NIPR, VoIP and JWICS
  - In addition there are system to system links
    - E.g. TBMCS in different AOCs connect through SWIC
    - Similarly for GCCS,C2PC & JADOCS

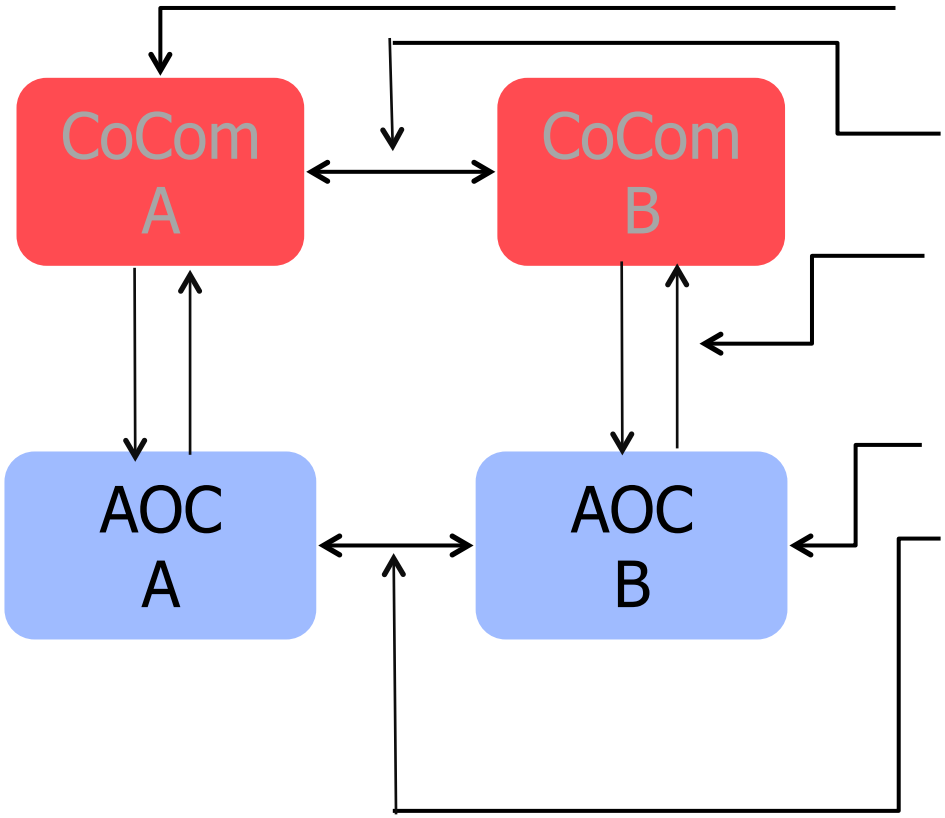


Carnegie Mellon
institute for SOFTWARE RESEARCH

Types of Cyber Effects

- 5 Pillars of Information Assurance as 'buckets' for cyber effects
  - Confidentiality
  - *Integrity*
  - *Availability*
  - Authentication
  - Non-Repudiation
- Target
  - Breadth
    - One AOC
    - All AOC
  - Location
    - Within AOC
    - Between AOC
    - COCOM to AOC

Where Can Cyber Attacks Manifest



- Within CoCom
- Between CoCom
- Between CoCom and AOC
- *Within AOC(s)*
- *Between AOCs*

Assessing Resilience

- Many ways to assess resiliency
  - Percentage change below some threshold(s) from baseline for one or more metrics of interest
  - Degree of degradation in number of personnel or divisions that have minimum knowledge to operate compared to operational levels when there was no cyber attack
- Illustrative specific measures are:
  - Task & Resource Congruence
  - Fragmentation through loss of agent(s)
  - Communication speed degradation
  - Diffusion degradation
  - Performance degradation
  - Number of people with minimum ability to operate
  - Ability to complete planning

Carnegie Mellon
institute for SOFTWARE RESEARCH

Assessment via ORA (1 of 2)

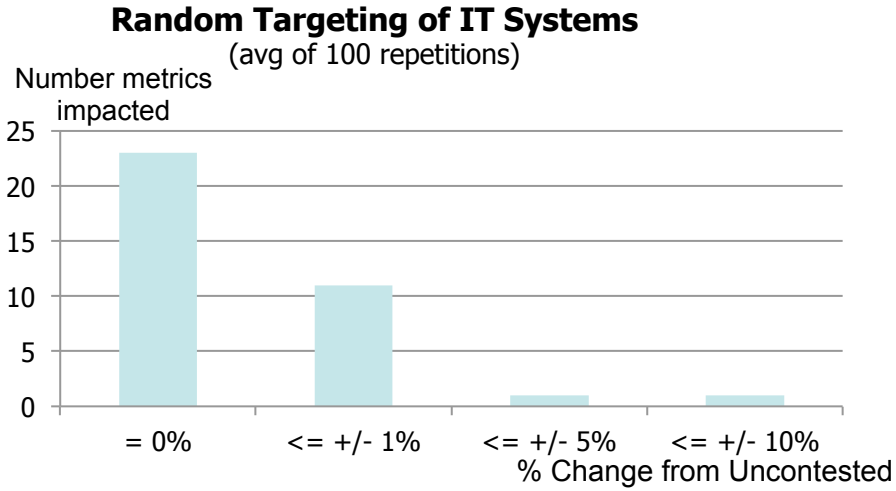
- **Key Take Aways:**
  - An AOC, as described in doctrinal sources, is very resilient
  - Integrated AOCs are more resilient
  - Its harder to trigger cascading effects than intuition might suggest
  - IT personnel may think the system is less resilient than it is
  - Integration within and across commands via additional communications mechanisms, social links, shared knowledge and resources counter-act specific loss of IT systems
  - Additional resiliency can be achieved by
    - Increased social networking
    - Training selected personnel to handle increased communication when under attack

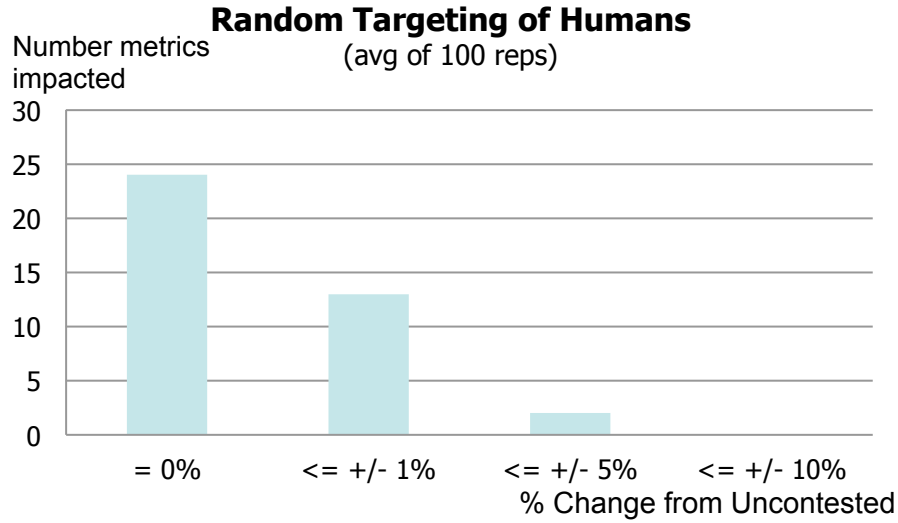
- Key Results
  - **Not** highly reliant on top four IT systems
  - **Not** highly reliant on top leader
  - **Combinations of system losses**, even when not crossing 5% thresholds, **were generally positive non-linear**
  - For AOC as a whole it takes large combination attacks to cross 5% threshold
  - For IT-system ecosystem, most attacks resulted in over 10% degradation

Carnegie Mellon
institute for SOFTWARE RESEARCH

Assessment via ORA (2 of 2)

- Immediate Impact reports for loss of single and combinations of key IT systems & humans
  - Random targeting of IT or Humans – little impact
    - <= 4 IT systems across hundreds of runs
  - Why:
    - Distribution of links between IT-systems and Agents appears exponential
    - Therefore: high probability that random attack does not hit key systems
  - AOC's resilient to random attacks
  - AOC's more impacted by targeted attacks





Carnegie Mellon
institute for SOFTWARE RESEARCH

Effects of Targeting TBMCS: Based on Doctrinal Model of AOC (1 of 4)

Network Level Measures (for IT Systems only)			
Name	**Unconteste d**	**Contested**	**% Change**
Performance As Accuracy	0.045	0.028	-38.77%
Clustering coefficient	0.275	0.250	-9.10%
Characteristic Path Length	2.956	3.415	+15.53%
Social Density	0.021	0.018	-12.63%
Communication Congruence	-0.490	-0.556	+13.53%

- IT Systems only: 39% decrease in accuracy when TBMCS targeted
- Human-IT system: <5% decrease in accuracy when TBMCS targeted

- AOC remains functional in face of TBMCS loss
- Resiliency is provided by "human power"

Chief of Combat Ops (cco) and Senior Operations Duty Officer (sodo) increase in criticality as "GO TO" people when TBMCS offline

Betweenness Centrality (for AOC)					
Name	**Rank Before**	**Value Before**	**Rank After**	**Value After**	**% Change**
air_mob_div	2	0.088	2	0.093	6.36%
tbmcs	1	0.088	Entity removed		
gccs	5	0.029	3	0.052	+77.72%
strategy_div	7	0.041	7	0.043	5.82%
c2pc	8	0.034	6	0.045	32.23%
c_c_o	9	0.029	8	0.034	17.27%
sodo	10	0.026	10	0.027	6.93%

Betweenness Centrality (for IT Systems only)					
Name	**Rank Before**	**Value Before**	**Rank After**	**Value After**	**% Change**
tbmcs	1	0.088	Entity removed		
c2pc	2	0.069	1	0.103	+48.87%
gccs	5	0.029	3	0.052	+77.72%

C2PC and GCCS will become next critical IT systems

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Effects of Targeting Top 4 IT Systems (2 of 4)

Network Level Measures (for IT Systems only)			
Name	**Uncontested**	**Contested**	**% Change**
Performance As Accuracy	0.043	0.025	-42.08%
Diffusion	0.225	0.130	-42.01%
Clustering Coefficient	0.261	0.173	-33.71%
Characteristic Path Length	2.853	4.380	+53.48%
Social Density	0.020	0.012	-38.30%
Communication Congruence	-0.465	-0.547	+17.63%
Average Communication Speed	0.350	0.228	-34.85%
Fragmentation	0.773	0.867	+13.22%
Overall Fragmentation	0.004	0.007	+75.22%

- For the IT System ecosystem:
- Strategic Targeting of 4 high degree IT systems critically degrades ability to support the missions
- System fragments and 35% drop in communication speed

- AOC as a whole takes a performance hit apx 5%
- Resiliency provided by human communication – which suffers less than 5% drop in communication speed despite fragmentation

Network Level Measures (for entire AOC)			
Name	**Uncontested**	**Contested**	**% Change**
Performance As Accuracy	0.299	0.283	-5.44%
Diffusion	0.62	0.571	-8.03%
Clustering Coefficient	0.377	0.349	-7.42%
Social Density	0.013	0.012	-6.30%
Number of Isolated Agents	85	97	14.12%
Fragmentation	0.377	0.427	13.22%
Overall Fragmentation	0.004	0.007	75.22%

Carnegie Mellon
isr institute for SOFTWARE RESEARCH

Effects of Targeting Top 4 IT Systems (3 of 4)

- Resiliency can be enhanced by:
  - AOCs rehearsing fail-over to these systems
  - Training SODO in how to respond when in contested environment
  - Providing SODO with backup
- Simultaneous attacks on TBMCS, C2PC, COP and GCCS results in a shift to:
  - the Intel/JWICS network
  - the portable flight planning system in the face

Centrality (total degree centrality) (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	% Change
pfps	5	0.111	1	0.093	-16.43%
gdss	6	0.097	2	0.071	-26.53%
g_t_n	7	0.083	3	0.057	-31.43%
trac2es	8	0.083	6	0.057	-31.43%
gates	9	0.076	4	0.057	-25.19%
jopes	10	0.063	7	0.050	-20.00%

Betweenness Centrality (for AOC)

Name	Rank Before	Value Before	Rank After	Value After	Value Change(%)
c_c_o	9	0.029	9	0.024	-16.62%
sodo	10	0.026	8	0.031	20.53%

Betweenness Centrality (for IT Systems Only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change(%)
tacs	3	0.037	6	0.028	-24.50%
adsi	4	0.030	10	0.019	-34.25%
stars	6	0.019	11	0.015	-23.19%
pfps	8	0.018	4	0.030	+68.03%
i_w_s	9	0.017	5	0.028	+65.84%
jwics	10	0.016	1	0.071	+331.99%

Carnegie Mellon
institute for SOFTWARE RESEARCH

Effects of Targeting CJFACC & CCO (4 of 4)

Network Level Measures			
Name	**Uncontested**	**Contested**	**% Change**
Performance As Accuracy	0.299	0.264	-11.72%
Clustering Coefficient	0.377	0.342	-9.25%
Social Density	0.013	0.012	-8.57%
Number of Isolated Agents	86.000	94.000	+9.30%
Fragmentation	0.381	0.408	+7.29%

- AOC remains functional in face of a key leader loss (< 5% drop in performance and communication)
- AOC suffers 12% drop in performance when both CJFAC & CCO are impacted

- Without CJFACC & CCO
  - all divisions are more critical
  - SODO rises the most in criticality
- Resiliency can be supported by training SODO to handle this shift in responsibility

Betweenness Centrality					
Name	**Rank Before**	**Value Before**	**Rank After**	**Value After**	**% Change**
air_mob_div	2	0.087	1	0.098	+11.64%
tbmcs	3	0.067	4	0.066	-0.83%
isrd	4	0.058	2	0.071	+21.77%
cbt_ops_div	5	0.049	3	0.067	+36.07%
c_p_d	6	0.045	5	0.054	+19.34%
strategy_div	7	0.041	6	0.054	+32.55%
c2pc	8	0.034	8	0.034	+0.23%
sodo	10	0.026	7	0.036	+41.06%

Carnegie Mellon
institute for SOFTWARE RESEARCH

Information Diffusion Simulation

- Construct - An agent-based simulation developed at CMU
- Validated model of agent interaction
  - In use for projects with US DoD
  - In use for projects with US IRS
  - Validated against classic social network models as well as organizational behavioral models for binary classification tasks

Planning Phases

- General Mission Planning Phases
  - Mission analysis – identify constraints
  - COA analysis – run through war-gaming
  - COA selection - operationalize
- At AOC difference in activity within and across the phases can be operationalized in terms of which actors are active
  - FOCUS: AOC planning process that occurs in all three phases is modeled:
    - Joint planning group – JPG
    - JPG starts off with all Operations Order (OPORD) knowledge
    - JPG operates in a cycle of plan-brief-plan-brief
      - Operationalized as periodic changes in who JPG members talk to as they brief other members of the AOC about the OPORD

Carnegie Mellon
institute for SOFTWARE RESEARCH

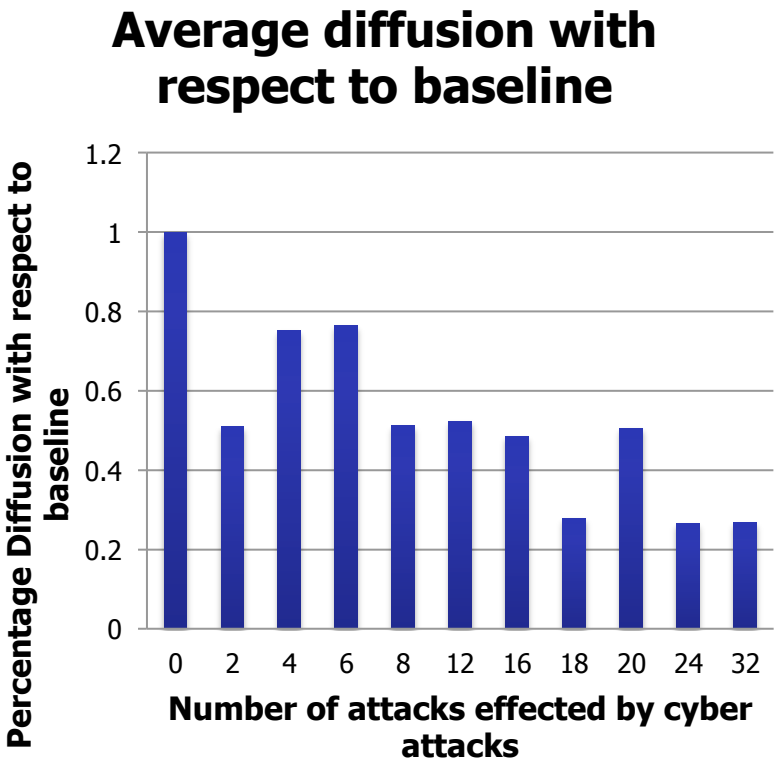
Model Development - AOCs

- All AOCs are currently modeled as structurally identical
  - This is easily modifiable based on data (same people and IT)
- AOCs are modeled:
  - As a network of people and IT systems
  - People have tasks to do
  - Knowledge flows between people, between people and IT systems, and between IT systems
  - Has five divisions each with a head person and a sub-head
    - Strategy, Combat Plans, Combat Ops, ISR, and Air Mobility
  - Has a JPG with 5 members
    - 2 from ISR and 2 from Combat Plans and a lawyer (functional group)
    - JPG has specialized knowledge – the OPORD
  - Has 15 functional areas each with a head person & supporting personnel
  - Divisions and functional areas cross each other

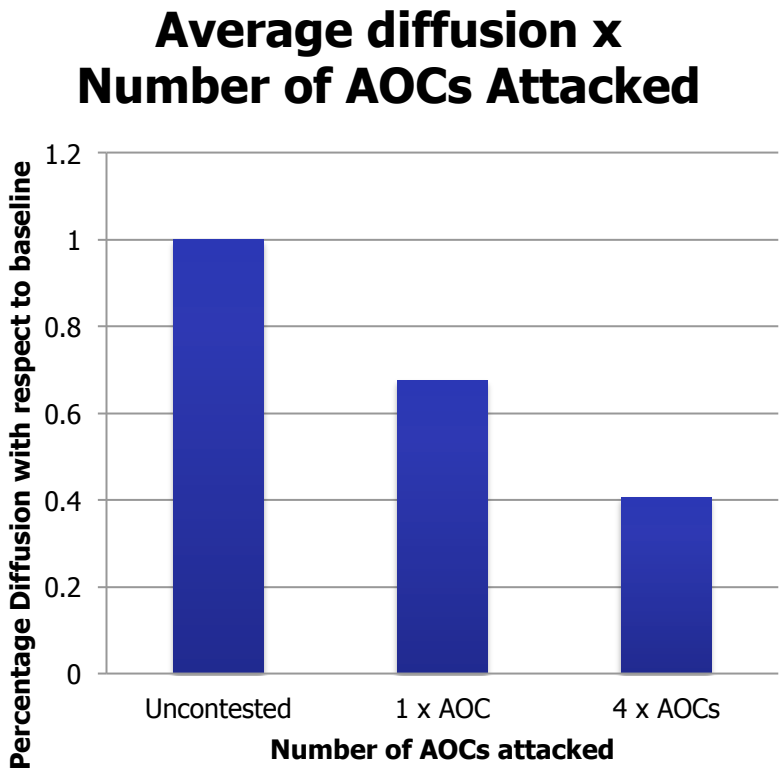
Carnegie Mellon
institute for SOFTWARE RESEARCH

Integrated System is Resilient to a few attack or attacks on only a regional AOC

More attacks the less resilient
Degradation is nonlinear

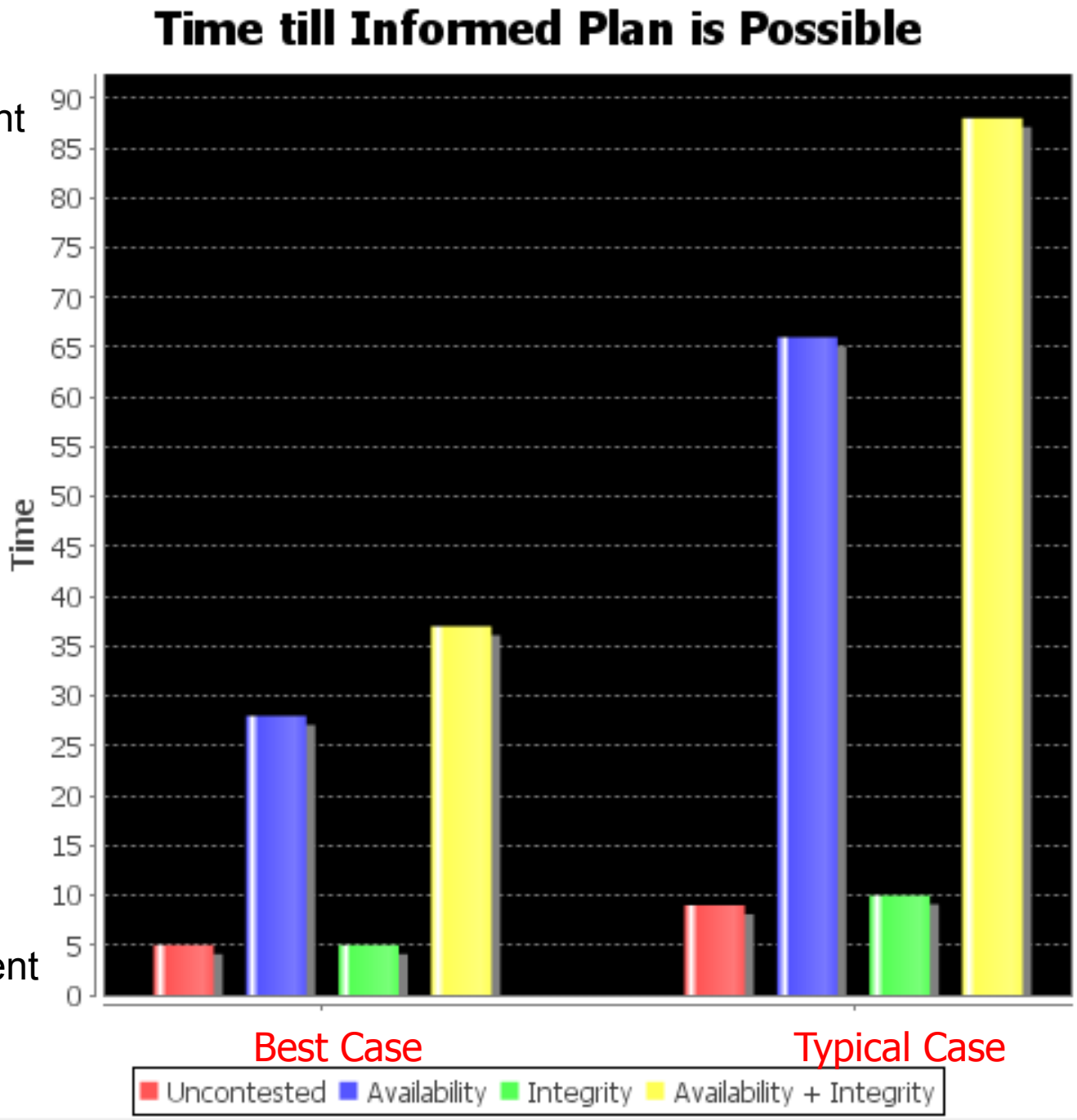


More AOCs attacked the less resilient
Degradation is nonlinear



Carnegie Mellon
institute for SOFTWARE RESEARCH

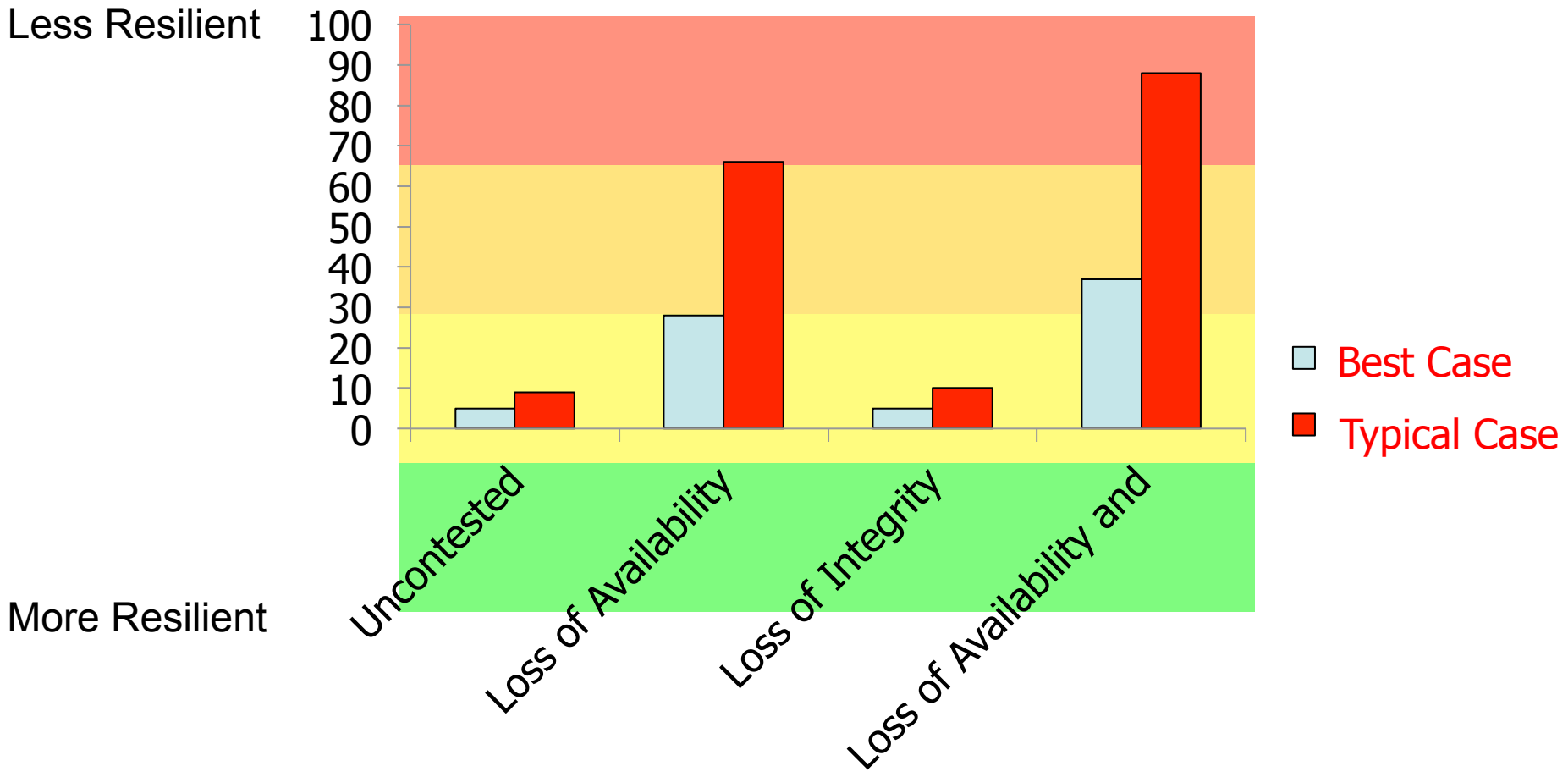
Less Resilient



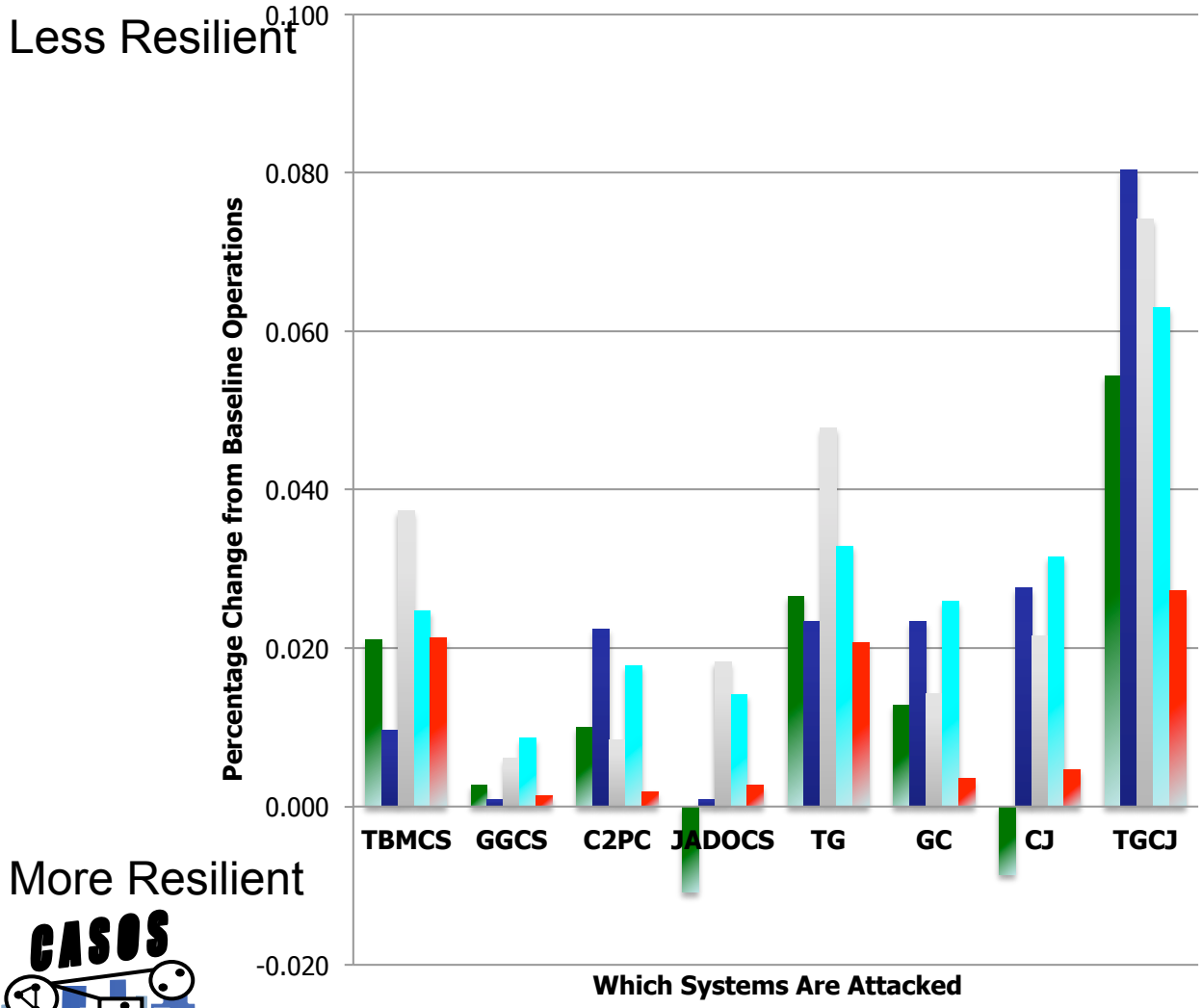
More Resilient

Carnegie Mellon
institute for SOFTWARE RESEARCH

Resiliency – Time to Plan



Resiliency as the breadth of the attack (more systems) are impacted



Nonlinear Effects
JADOCS focused attack might help
Both performance and communication will degrade

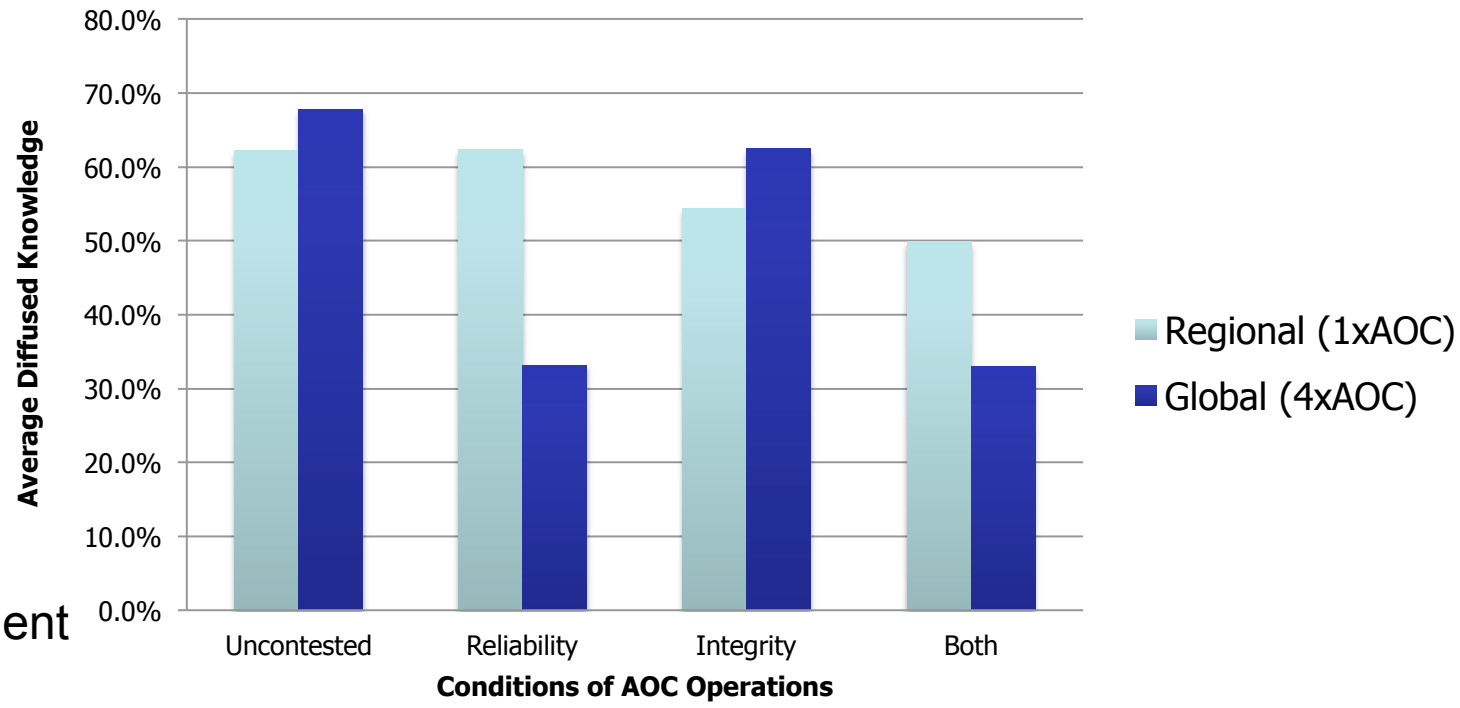
- Performance As Accuracy
- Diffusion
- Clustering Coefficient
- Density
- Average Communication Speed

Carnegie Mellon
institute for SOFTWARE RESEARCH

Diffusion Resiliency

Getting the right information to the right people in time

More Resilient



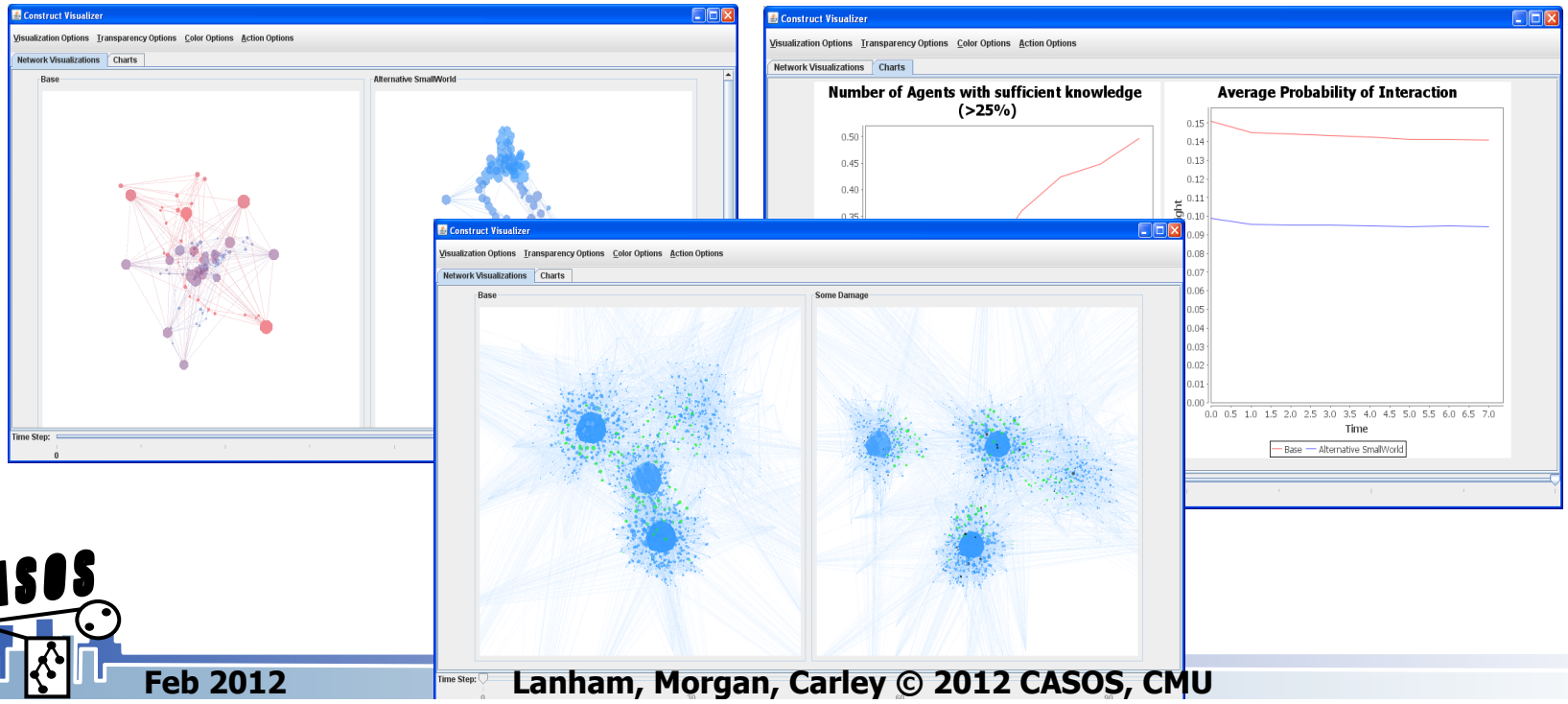
Less Resilient

Nonlinear Effects
Integrated system is fairly robust against regional attacks

Carnegie Mellon
institute for SOFTWARE RESEARCH

Viewing Model in Operation

- Visualizations of information diffusion is available (talk with me during the conference)
- The color of the nodes will change based on whether they are compromised or not
- Dynamic bar graphs for resiliency measure
- Dynamic line graphs for knowledge acquisition resiliency



Future Work

- Identify key differences between AOCs and implement
- Adjust for cyber attacks that impact flow from COCOMs and/ or other external organizations (other "lines of authority")
- Take into account shift work
  - Run the following three scenarios in addition to the attacks – these are remediation strategies
  - "Day/Mid/Swing" and "Day/Night Cycles"
    - Doctrine documents to define agent structure. Agents are separated into shifts are not always available to each other.
  - "All Hands on Deck"
    - Doctrine documents define agent structure. Agents interact with all available agents at all times. Shifts no longer separate agents.
  - "Preventative Measures"
    - Hypothetical "ideal" structure for rapidly transmitting information. Agents are separated into 3 shifts and are not always available.

Future Work

- Operation Model
  - Phasing of different tasks
  - Task based interaction
  - Better differentiation of IT as mediator for communications
    - synchronous (e.g., phone, chat) and asynchronous (e.g., email, web page(s), database(s))
    - Mediator as perfect/imperfect/dysfunctional communications aid
- Planning and execution modeled
  - Impact differential based on phase of operation to be examined
- Impact differential based on severity of attack to be examined
- Alternate measures of resiliency

Carnegie Mellon
institute for SOFTWARE RESEARCH

Points of Contact

Lieutenant Colonel Michael J. Lanham
Wean 5117
Carnegie Mellon University
5000 Forbes Ave.
Pittsburgh, PA 15213 USA
Tel: 412-268-4681
mlanham@cs.cmu.edu
Michael.lanham@us.army.mil

Geoffrey P. Morgan
Wean 5117
Tel: 412-268-4681
gmorgan@cs.cmu.edu

Prof. Kathleen M. Carley
Wean 5130
Tel: 412-268-6016
Fax: 412-268-1744
kathleen.carley@CS.CMU.EDU