AFRL-RI-RS-TM-2008-12
In House Final Technical Memorandum
March 2008

CYBER AND AIR JOINT EFFECTS DEMONSTRATION (CAAJED)

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

AFRL-RI-RS-TM-2008-12 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/	/s/
CHESTER J. MACIAG Chief, Cyber Offense Branch	WARREN H. DEBANY, JR. Technical Advisor, Information Grid Division Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAR 2008	Final	Jun 07 – Aug 07

4. TITLE AND SUBTITLE

CYBER AND AIR JOINT EFFECTS DEMONSTRATION (CAAJED)

5a. CONTRACT NUMBER
In House

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Raphael S. Mudge Capt, USAF
Mr. Scott Lingley, Rome Research Corporation

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
AFRL/RIGB
525 Brooks Rd
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIGB
525 Brooks Rd
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TM-2008-12

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# WPAFB 08-1043

13. SUPPLEMENTARY NOTES
This work was funded by the Air Force Office of Scientific Research under the AFRL/RI Chief Scientist Minigrant Program.

14. ABSTRACT
The Cyber and Air Joint Effects Demonstration (CAAJED) conceptualized integration of air and cyber assets scoped to a cyber defense exercise environment. Current cyber warfare exercises focus on information systems only. These exercises are limited in scope as there is no process or mission to reason about and defend. This limitation stifles the education of cyberspace warriors and innovation in maturing this domain. To overcome this, we created a process-oriented cyber/kinetic inference model. We used this model to integrate an air battle simulation with a cyber operations exercise. We discuss the positive impact of our technologies and model in 2007 Advanced Course in Engineering (ACE) Cyber Defense Exercise.

15. SUBJECT TERMS
Cyber wargame, strategic attack, centers of gravity model, cyber education

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Raphael S. Mudge, Capt, USAF
U	U	U	UU	16	19b. TELEPHONE NUMBER (*Include area code*) N/A

Table of Contents

1. Introduction 1

2. The Current State of the Art 1
    2.1 Three Levels of Cyber Warfare 1
    2.2 Bulwark Defender 1
    2.3 CAAJED ‘06 2
    2.4 Scope of CAAJED 2

3. Cyber/Kinetic Inference Model 2
    3.1 Cyber/Kinetic Inference Abstraction 2
    3.2 CAAJED Process Model 3
    3.3 How to Populate the Model 3

4. CAAJED 4
    4.1 Architecture 4
    4.2 Modern Air Power 4
    4.3 Simulated Enterprise for Cyber Operations Training (SECOT) 5
    4.4 Cross Domain Effects between MAP and SECOT 6
    4.5 Level 2 and Level 3 Cyber Attacks 8

5. 2007 Cyber Defense Exercise 8
    5.1 Advanced Course in Engineering 8
    5.2 Event Setup 8
    5.3 Results 9

6. Recommendations 11

7. Acknowledgements 11

8. References 11

1. Introduction

Today, there is little integration of the cyber and kinetic domains in Air Force exercises and training. Young officers, when taught modern air power theory, learn about air and space and how these assets work hand in hand. Cyber is usually taught as little more than expansion of a few acronyms.

There is currently no means for air power theorists to experiment with cyber effects in a battle space that includes real targets. Likewise, there is currently no platform to educate future officers on how cyber and kinetic effects can interoperate.

This research lays a theoretical groundwork necessary for the creation of this platform. This platform will serve as a common ground for cyber and kinetic domains to interact and create effects within each other.

2. The Current State of the Art

2.1 Three Levels of Cyber Warfare

In the Summer of 2007, the Air Force Scientific Advisory Board (SAB) conducted a study of cyber warfare implications. Within their report ***[1]*** they define three levels of Cyber Warfare:

> Level 1 is network wars or system administrator versus system administrator. Mobile malicious logic, common exploits, and other typical information technology headaches fall within this category.
>
> Level 2 is labeled cyber adjunct to kinetic combat. A level 2 attack is one where an operator tries to achieve a kinetic effect through a cyber attack. Use of malicious logic to disable a radar site is an example of a level 2 attack.
>
> Level 3, the most dangerous, is malicious manipulation. The SAB report claims these attacks are "the ones to be feared, they are covert, they are planned, they are orchestrated, and they can cause widespread havoc and disruption without the victims realizing their problems are cyber related."

The SAB expresses concern that cyber warfare emphasis is occurring on level 1 and level 2 style attacks. In these next sections we will contrast the current state of the art of cyber/kinetic gaming against these levels.

2.2 Bulwark Defender

Bulwark Defender is a joint service exercise for Information Assurance and computer network defense. A simulator training exercise network (SIMTEX) that mimics an operational network is used to detect, prevent and respond to different types of attacks. These include stealthy efforts to compromise and mine data from network-based resources, as well as all-out actions aimed at total network takeovers. ***[2]***

The SIMTEX range and its uses are discussed in detail in ***[3]***. Bulwark Defender trains network defenders against "Level 1" scenarios. At this time, no Air Force mission is simulated as part of Bulwark Defender. This short coming coincides with current Air Force network operations which has trouble correlating network events with military mission impact. These are discussed in ***[4]***.

Bulwark Defender serves us as an accurate depiction of the shortcomings between defensive cyber and kinetic operations within the DoD. Bulwark Defender has no level 2 or level 3 scenarios. What does this say about our ability to detect and defend against real world level 2 and level 3 attacks?

2.3 CAAJED '06

An early incarnation of an exercise with cyber and kinetic effects was demonstrated during the Advanced Course in Engineering 2006 Cyber Defense Exercise. CAAJED '06 manually integrated Modern Air Power, a kinetic war-game, into the exercise for the purpose of including cyber to kinetic effects ***[5]***. CAAJED '06 used an arbitrary mapping of network services to assets within the simulation. As attacks affected network services, operators were instructed to disable the associated assets. The student network defenders were oblivious to the reality that operators were sitting at consoles conducting a simulated war effort.

2.4 Scope of CAAJED

Here we introduce a cyber/kinetic inference model and appropriate technologies to improve upon CAAJED '06. We scope our cyber/kinetic inference model work to a controlled exercise environment.

Attacking cyber/kinetic inference in an exercise environment has value. Current network defense capabilities do not capture the realities of cyber war that we are dealing with now. As discussed in 2.2, current training techniques fail to deliver as well. By enhancing the way we train, we hope to impact the way we fight.

3. Cyber/Kinetic Inference Model

3.1 Cyber/Kinetic Inference Model Semantics

The cyber/kinetic inference model translates events in one domain to effects in the other. This technique is necessary for CAAJED and hence we introduce it here. Figure 1 describes our view of cyber/kinetic inference.

Figure 1. Cyber/Kinetic Inference Abstraction

Physical assets exist in the kinetic domain. These assets are utilized and coordinated through processes. Processes exist in the cyber domain. Capabilities are the resulting synergy of assets and the processes that utilize them.

Each kinetic capability is associated with one or more processes. We assume the process model defines a finite set of possible states. Cyber to kinetic inference is achieved by mapping states to availability, denial, or degradation of a capability. The mapping between failure points and effects is dependent on the process model used.

An acyclic dependency graph is associated with each state. This graph describes the physical assets the state depends on. Kinetic to cyber inference is achieved by a dependency analysis of this graph at a state transition. Failure to satisfy the physical dependencies of the state results in the failure of the process.

A capability may be associated with an asset. As an example, we would associate the ability to launch a surface-to-air missile with a specific surface-to-air missile (SAM) site. Multiple instances of a capability are differentiated by their associated asset.

3.2 CAAJED Process Model

We use finite-state machines to describe processes. This limits our ability to express redundancy and forces us to assume processes execute asynchronous to one another. This also drives our definition of a process. We define a process as the coordinated synchronous execution of a task between one or more parties. These limitations are not a problem given the scope and implementation of CAAJED.

Future research should investigate the use of some process algebra as a process model language. Process algebra is a tool to describe the interaction of concurrent processes. This will overcome the limitations of finite-state machines and enable a wider definition of processes.

3.3 How to Populate the Model

We first define a set of interesting kinetic capabilities. Examples include the ability to task aircraft mid-sortie, extend range of aircraft through refueling, launch surface-to-air missiles, launch sorties, etc. These capabilities are enabled by processes that control assets.

For each of these capabilities we generate a list of processes the capability depends on. As an example the ability to launch aircraft could be associated with a logistics process (fuel, parts) and a sortie planning process.

We describe each of the processes as a well formed entity in the process model language. Finite-state machines describe the logical flow of a process in terms of states and potential transition paths between states.

We attach a specific effect to each appropriate process state. States that represent failure conditions have a negative effect associated with them. States representing a completion action have an associated positive effect. We define effects in terms of availability, denial, or degradation of a specific capability.

We associate a physical asset dependency graph to appropriate states. Include all assets related to the state in its dependency graph. As an example, a logistics process may include a move materials state. This state could depend on a vehicle, personnel, and specific roads and bridges dependent on the destination.

4. CAAJED

4.1 Architecture

CAAJED is the integration of Modern Air Power, the Simulated Enterprise for Cyber Operations Training, and the cyber/kinetic inference model. Figure 2 depicts the CAAJED architecture.

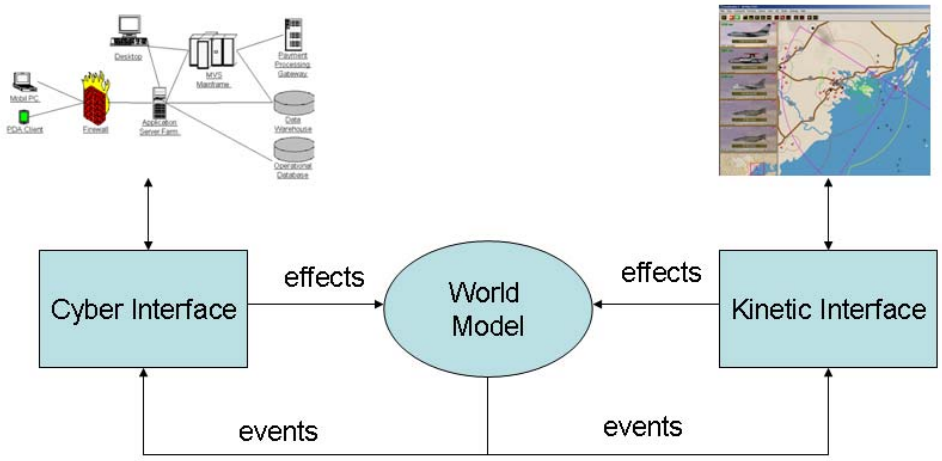

Figure 2. CAAJED Architecture

These technologies provide cyber input, conventional war input, and a model to deliver effects between these domains.

4.2 Modern Air Power

Modern Air Power ***[6]*** (MAP) is a war-game published by John Tiller Games. The MAP series covers air warfare in the missile age, from the Vietnam War to present. MAP is a real time, continuous, strategy game with unit control at flight level. It features many modern air warfare concepts, such as aerial refueling, Unmanned Aerial Vehicles (UAV), satellites and radar controlled ground to air defenses. MAP incorporates a scenario editor allowing a full range of creation and customization of simulations. MAP is used to train Air Force officers in airpower fundamentals by Air University Maxwell AFB, AL.

Modern Air Power is the kinetic piece of CAAJED. We modified MAP to communicate

and receive status changes as XML (extensible mark-up language) transmitted over a network connection. This mechanism enabled us to receive effects against and set effects on assets within the game.

Assets include air bases, surface to air missile sites, command nodes, radar sites, individual aircraft, and a civilian nuclear power facility. Each asset has one or more capabilities associated with it. For example an airbase has anti-aircraft artillery, radar coverage, and the ability to launch aircraft. Our interface enables us to enable, disable, and reduce the effectiveness of the capabilities. The capabilities of each individual asset are open to attack through cyber vectors.

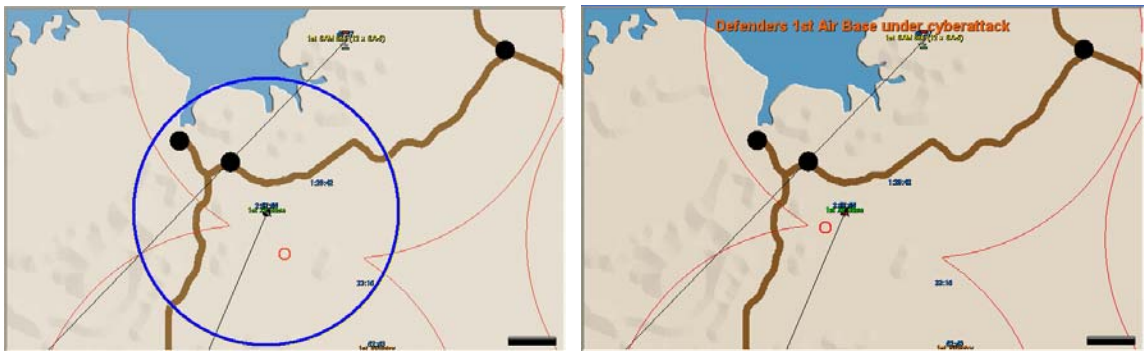

Figure 3. An Airbase Before and After a Cyber Attack

Figure 3 shows an airbase before and after a cyber attack. The dark blue ring represents radar coverage. CAAJED helped students see a physical outcome from their attacks.

MAP supports human vs. human, human vs. computer, and computer vs. computer play.

4.3 Simulated Enterprise for Cyber Operations Training (SECOT)

The SECOT is a combined traffic generator and score system used to host the cyber component of CAAJED. SECOT simulates an active and demanding enterprise community.

The SECOT framework encapsulates processes into mobile agents. Mobile agents ***[7]*** are a natural abstraction for the coordination of synchronous tasks between multiple locations. This property is known as execute-once. Once a task is complete, an agent may migrate to the next location and resume execution with its state intact. This creates the illusion of multiple users coordinating on the same task.

SECOT middleware employs several techniques to protect the execute-once semantic: SECOT agents migrate and communicate through an out-of-band network. This isolates the agents from events on the exercise network. Distributed transaction processing techniques are applied to protect against failures on the out-of-band network.

The SECOT implementation is made possible by the Sleep language ***[8]***. Sleep functions can save their variables, code, and execution state into continuation objects. Serialization of these objects provides a trivial mechanism for strong mobility. The entire SECOT implementation (sans agents) is less than 800 lines of code.

4.4 Cross Domain Effects between MAP and SECOT

The CAAJED world model is a software implementation of the cyber/kinetic inference model. This software receives events from the SECOT and Modern Air Power. We populated the model with assets and capabilities from the Modern Air Power scenario. Modern Air Power has a unique integer id for each asset within the simulation. Figure 4 shows capabilities from MAP, their associated processes, and the assets the processes depend on.

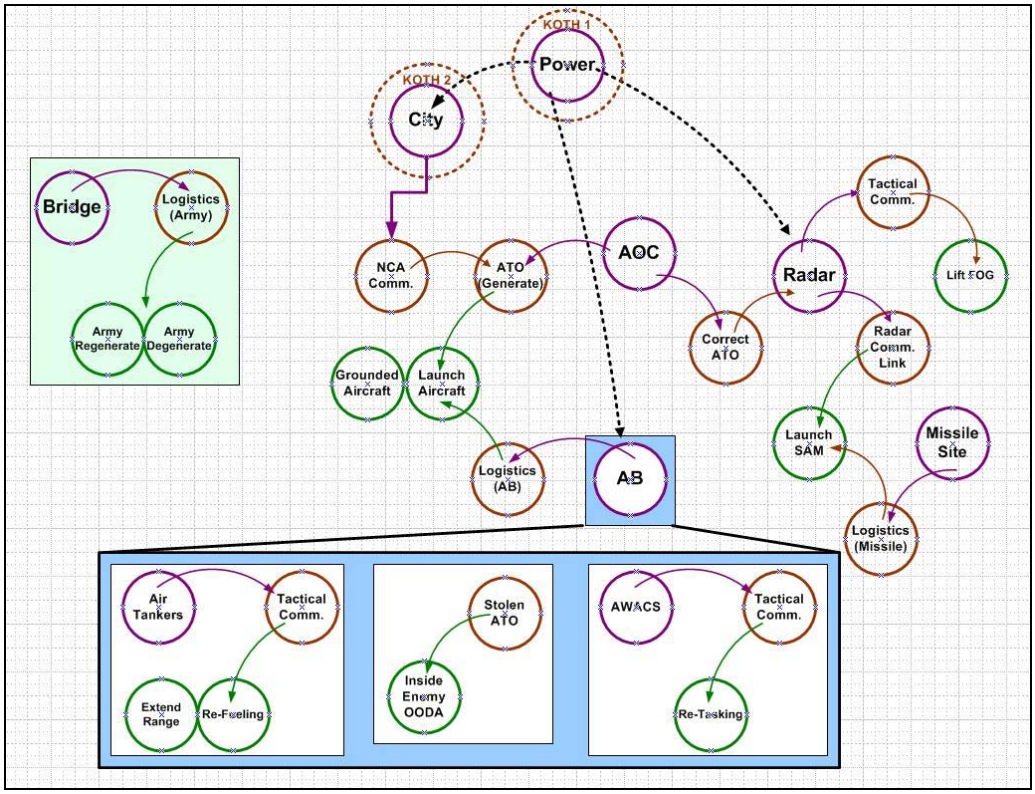

Figure 4. Capabilities with associated processes and physical assets

Modern Air Power connects to the world model via a network socket. Upon connection Modern Air Power provides an XML dump of all assets. MAP also provides hit reports as assets take damage through the simulation. The world model tracks the damage associated with each physical asset in Modern Air Power.

We created SECOT agents to represent several generic processes. We ran several instances of each agent. This allowed us to associate each running agent with a specific asset and capability to effect. Specific asset dependencies were associated within each

agent as well. Agents are responsible for monitoring the success/failure of each state in their process flow.

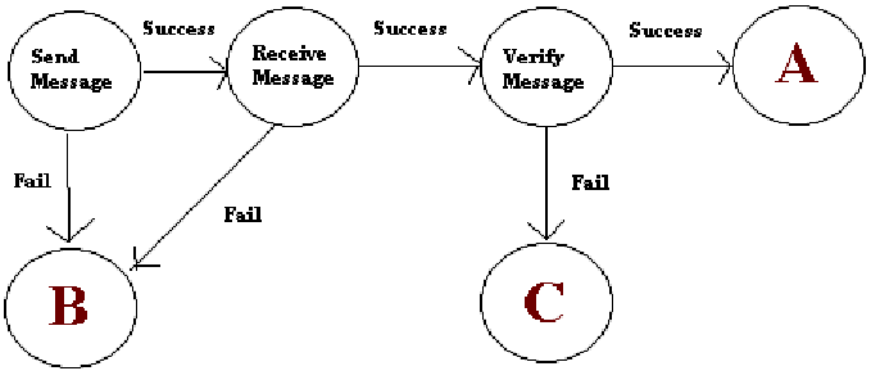

Figure 5. Tactical Communication Workflow

Figure 5 shows the tactical communication process. We used this process to simulate communications between a Joint Forces Air Component Commander (JFACC) and aircraft. Each KC-135 Stratotanker and E-3 Sentry in the MAP scenario had a tactical communication agent associated to it.

The agent connects to a chat server and joins a predefined channel. The agent then requests permission for a randomly generated activity from the JFACC. A simulated JFACC automatically responds to each request. The agent then verifies the response. This outcome is state A.

An example agent conversation:

```
*** tankerBravo has joined #aoc-east
<tankerBravo> request permission to pass some gas
<jfacc-east> tankerBravo: permission to pass some gas granted
<tankerBravo> acknowledged, proceeding
```

The agent could report failure when the chat server connection fails or the JFACC response times out. The agent could also report the corruption of the process when an unexpected response is received from the JFACC. These outcomes are captured by states B and C.

SECOT communicates events to the world model when states A, B, or C are encountered. These events represent the effects attached to the state in the cyber/kinetic inference model. The model translates the event into an XML message that communicates the effect to Modern Air Power. An effect is an asset, a capability, and the setting (enable, disable, or degrade).

Upon entering a state, an agent queries the damage level of each asset the state depends on. Acceptable damage level for an asset is random and changes at each check. The asset passes the damage check when `random(0 … 100) < damage(assetId)`. If an

asset dependency is not satisfied, the agent dissolves the process and takes away points from the owning team.

4.5 Level 2 and Level 3 Cyber Attacks

The CAAJED technology enables level 2 cyber attacks in an exercise setting. Cyber attacks cause disruptions. A disruption to a process results in a kinetic effect visible within Modern Air Power.

To enable ideal level 3 attacks, our processes would have to generate an information product utilized by Modern Air Power. This initial effort did not achieve this coupling.

We did motivate level 3 attacks through the use of point values. SECOT agents generate points based on the outcome of a process execution. The agents monitor themselves and look for corruptions within their information flow. For example, the kinetic effect of denying a logistics process versus changing the contents of an order are the same. The point values for changing the contents of an order are much greater than simple denial.

Each side also has an Air Tasking Order (ATO) process associated with it. This process represents the planning and dissemination of a master air attack plan to both sides. We reward capture of an adversary's ATO with many points. This was meant to reward the team that manages to achieve stealth, persistence, and communication within their adversary's network.

We also used point values to motivate student interest in level 2 attacks. Destroyed assets result in dissolved processes. Less active processes imply less opportunity to score positive points.

5. 2007 Cyber Defense Exercise

5.1 Advanced Course in Engineering

The Advanced Course in Engineering (ACE) Cyber Security Bootcamp develops next generation cyber security leaders from military officer candidates ***[9]***. The course immerses students in cyber security through coursework, internships, and competition.

The capstone to the ACE course is the Cyber Defense Exercise (CDE). This event has occurred over the past 4 years including 2007. The CDE evaluates participants on leadership skills, technical expertise in network defense, threat assessment, active response, host & network based monitoring, and vulnerability mitigation.

5.2 Event Setup

The two student teams constructed their own networks and had 10 weeks to test and harden them. Each team had to allow the SECOT agents to accomplish their mission. Beyond this requirement, they could do as they wished. SECOT agents operated both within and outside of the student networks.

The SECOT/CAAJED setup consisted of 3 hardened servers. Each server had two network interfaces. One interface acted as an out-of-band channel for agent migration, MAP network play communication, and CAAJED communication. The other interface was exposed to the exercise network. Figure 6 shows the network topology.

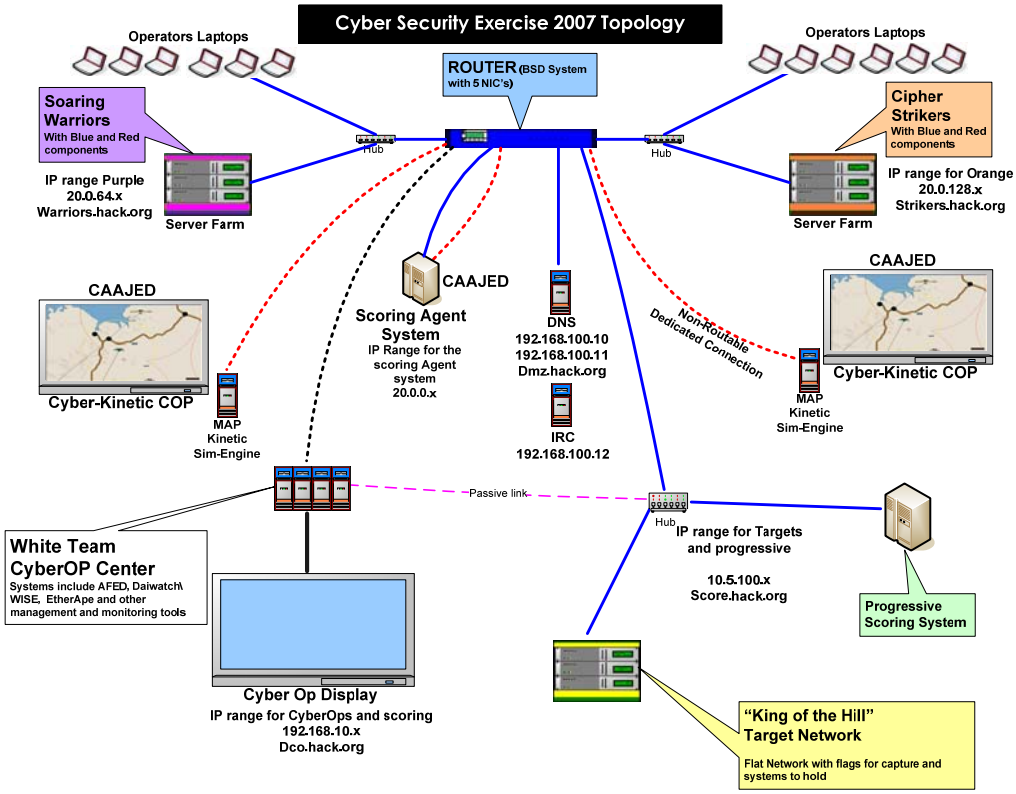

Figure 6. Cyber Security Exercise Topology

Each student team had one of these hardened servers within their network. We used another one on the outside. This enabled agents to assume roles within and outside of the networks. Students submitted configuration information to the agents via a website hosted on their hardened server. Each student area had two plasma displays. One showed the air battle as it unfolded. The other provided real time score information.

The two-day event was divided into separate heats consisting of half a day each. Modern Air Power play was driven by computer players. The exercise consisted of 71 SECOT agent instances. Each agent represented some active process coordinated amongst multiple systems that the students had to defend. There were over 900 events generated by SECOT per four-hour period.

5.3 Results

This year's CDE was the most successful yet. A number of interesting events, not seen in previous years, occurred.

Early in the summer, one team planted two insiders on the other team. They managed to maintain the insiders until the opportune time came to use them. The team with the

embedded spies was more technically superior with very weak operational security (OPSEC). The other team, aware of their ruse, maintained strong OPSEC throughout the course.

Figure 7. A team captain responds to an event from CAAJED

One student found a security flaw in the application used to submit configuration information to the SECOT agents. The victim team did not place their CAAJED server behind a firewall. The student exploited the flaw to delete all configuration information for their adversary's agents. This resulted in a near complete failure of all processes. This attack created intense confusion as the victim team struggled to understand what happened. Interestingly, they did not initially assume a cyber attack.

Students organized into teams with team captains on both sides maintaining military style control. Their whiteboards listed the defensive assets and offensive targets. The team captains appreciated physical signs of cyber attack. Many defensive actions were initiated in response to an event noticed within CAAJED first.

The kinetic to cyber inference frustrated both teams. Students did not like losing points through kinetic attacks they had no control over. This is exactly what we wanted them to feel.

Without taking credit from the students, we believe a number of catalysts allowed the success of the exercise. These are:

- The 10-week buildup to the CDE allowed students to form into teams, understand their networks, and prepare for the exercise.

- We provided source code to the SECOT and all agents to the students weeks prior to the exercise. This increased the students trust in the system and enabled them to focus on the exercise not the score system.

- CAAJED created scale, intensity, and a physical manifestation of the cyber warfare. Students had the opportunity to reason in terms of targets and effects, rather than network addresses and exploits only.

6. Recommendations

With CAAJED we developed the architecture, model, and preliminary tools to allow level-2 and level-3 cyber warfare in an exercise environment. We evaluated these tools in the 2007 ACE Cyber Defense Exercise. These concepts are ready for adoption to other exercises. Bulwark Defender and other exercises now have the option to include a kinetic component. Moving our training to the next level will help network operators reason about and develop war fighting techniques for integrated air, space, and cyberspace.

7. Acknowledgements

This work was funded by the Air Force Office of Scientific Research under the AFRL/RI Chief Scientist Minigrant Program. Mr. David Ross (AFRL/RISB) and Dr. John Tiller (John Tiller Games) contributed to the research for and implementation of CAAJED. Mr. Brian Kropa (AFRL/RIGA) and Mr. Thomas Vestal (AFRL/RIGA) contributed to the troubleshooting and administration of the SECOT.

8. References

[1] United States Department of the Air Force, Air Force Scientific Advisory Board. "Implications of Cyber Warfare: Vol. 1 Executive Summary and Annotated Brief." SAB-TR-07-02. August 2007.

[2] A. Hansen "BD06 confirms joint CND capability." *Spokesman Magazine*. April 2006.

[3] A. McBride, "Air Force Cyber Warfare Training." *DSP Journal*. April 2007

[4] L. Forston**, "**Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology" Air Force Institute of Technology Masters Thesis. March 2007

[5] J. Brown, D. Ross, A. Ford, S. Lingley "Cyber & Air Asset Joint Effects Demonstration (CAAJED) Technical Memo," AFRL/IFSB, September 2006.

[6] http://home.hiwaay.net/~tiller/modernairpower.htm.

[7] A. Carzaniga, GP Picco, G. Vigna, "Designing Distributed Applications with Mobile Code Paradigms," *Software Engineerin, Proceedings of the 1997 (19th) International Conference on.* 1997.

[8] http://sleep.hick.org/.

[9] K. Jabbour, S. Older, "The advanced course in engineering on cyber security: A learning community for developing cyber-security leaders," *Proceedings of the Sixth Workshop on Education in Computer Security*. July 2004.