# Serious Game for Cyber Threat Impact Assessment

# Air Traffic Controller Cyberattack Evaluation Serious Game (ACES)

April 9, 2014

OR / SYST 699 Capstone Project Proposal

Prepared by Group 3
Doran Cavett
Will Fontan
Imran Shah

Table of Contents

1. Introduction .......... 1
2. Overview .......... 1
3. Background .......... 1
4. Problem Statement .......... 3
    4.1 Problems With ADS-B Communication .......... 4
    4.2 ADS-B Threats .......... 4
        4.2.1 Interception Attacks .......... 5
        4.2.2 Jamming Attacks .......... 5
        4.2.3 Injection Attacks .......... 5
    4.3 Serious Game to Detect and Adequately Respond to ADS-B Cyber Attacks .......... 6
5. Stakeholders .......... 7
6. Project Scope .......... 7
7. Assumptions .......... 7
8. Deliverables .......... 7
9. Preliminary Requirements .......... 8
10. Technical Approach .......... 10
    10.1 Simulation Approach .......... 10
11. Expected Results .......... 12
12. Project Work Breakdown Structure .......... 12
13. References .......... 12

Table of Figures

Figure 1 – Overview of Campos Basin Oil Operations .......... 2
Figure 2 – Campos Basin Radar Coverage .......... 3
Figure 3 – ADS-B Communication .......... 4
Figure 4 – Simulation-Emulation Scenario .......... 11

## 1. Introduction

As computing systems have become more ubiquitous they play an integral role in the daily operation of critical infrastructure assets and operations critical to society. Automation of tasks and increased capabilities afforded by computing systems are intertwined into critical infrastructure operations.

The interconnectedness of systems and reliance upon technology has opened a new cyberspace front for warfare. To protect against technological attacks, events that may occur must be identified, threats and impact to critical infrastructure understood, and mitigating actions developed.

Gaming provides a means to evaluate various types of attacks against critical infrastructure without the need for large investments in real world test scenarios and harm or loss of life. We will leverage the use of a game, Air Traffic Controller Cyberattack Evaluation Serious Game (ACES), to simulate cyber attacks on the critical infrastructure scenario of helicopter operations in support of oil production off the Rio De Janeiro coast of Brazil.

ACES will provide a venue for training of air traffic controllers and understanding the impact of attacks on critical infrastructure and operations which will in turn help to identify and prepare mitigating actions.

## 2. Overview

Our team will support a cadre of George Mason University undergraduate Simulation and Gaming (SGI) design students in designing, developing, and evaluating a serious game prototype based on the system requirements specifications.

Section 3 provides details on the critical infrastructure scenario that will be captured in the serious game. Section 4 describes the critical infrastructure target and threats that will be the focus of the project. Our stakeholders and their roles are identified in section 5. Section 6 defines the project scope. Section 7 identifies the project-wide assumptions. Section 8 identifies the project deliverables. Section 9 includes the project preliminary requirements. Section 10 summarizes the technical approach. Section 11 lists the expected results. Section 12 provides the project Work Breakdown Structure (WBS). Section 13 lists the references used to prepare for this project and develop this proposal.

## 3. Background

The Campos Basin is a petroleum rich area located in the Rio de Janeiro state that is responsible for 1.3 million barrels a day of petroleum production. The Campos Basin accounts for 80% of Brazil's petroleum production.

Oil development operations in the Campos Basin include heavy helicopter traffic between the continent and oceanic fields during daytime, with an average of 50 minutes per flight. A map of Rio de Janeiro and the offshore islands and oceanic fields is shown in figure 1 below.

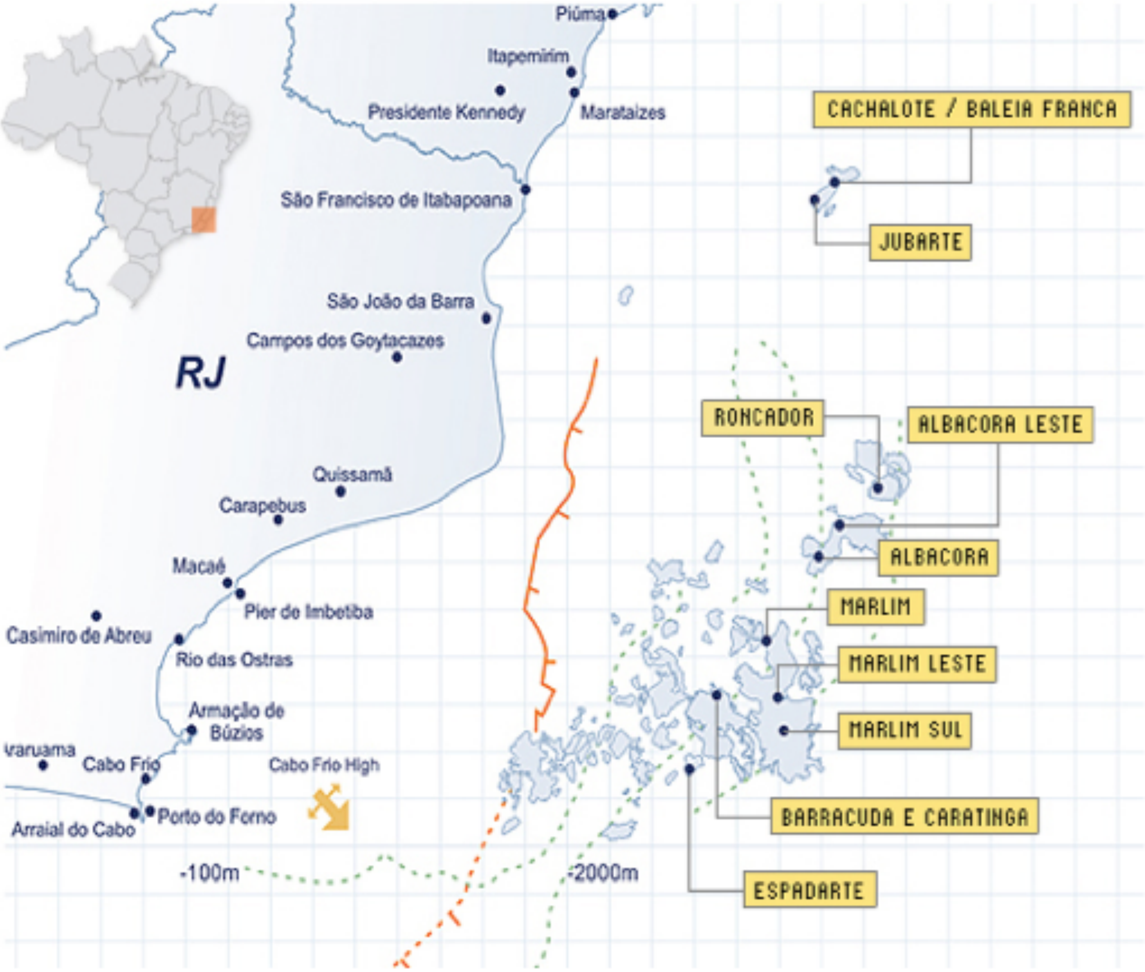


Figure 1 – Overview of Campos Basin Oil Operations

Helicopter flights are conducted at low altitudes and oil platforms are located more than 60 nautical miles from the region's main airport, Macaé. As a result, helicopter operations cannot be monitored by Air Traffic Service (ATS) from the Macaé airport, the region's main airport, which only supports air traffic within a 45 nautical mile radius and 9500 foot and above altitude.  ATS for these offshore helicopter operations is then provided through the Automatic Dependent Surveillance-Broadcast (ADS-B) system (see figure 2 below).

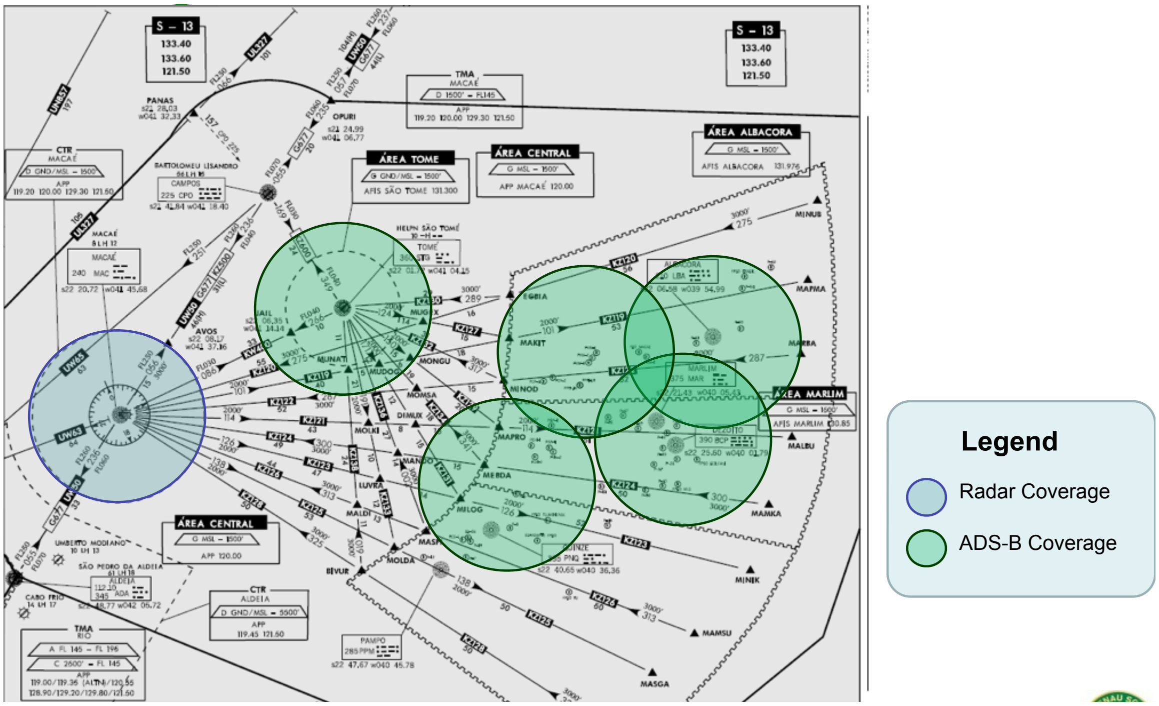


Figure 2 – Campos Basin Radar Coverage

## 4. Problem Statement

Disruption to the Campos Basin helicopter operations has the potential to severely disrupt and even bring production at the oceanic fields to a halt. Safe and continuous operation of helicopters supporting offshore oil production is critical to meet production capabilities and protect against loss of life or assets.

ATS personnel's reliance on ADS-B may allow for hostile individuals to disrupt helicopter operations through various cyber attacks. To better understand the potential mission impacts of cyber threats and to allow for the development of improved operational and risk management processes, gaming and simulation tools will be used to simulate the real-time scenario, cyber attacks, and their effects.

### 4.1 Problems With ADS-B Communication

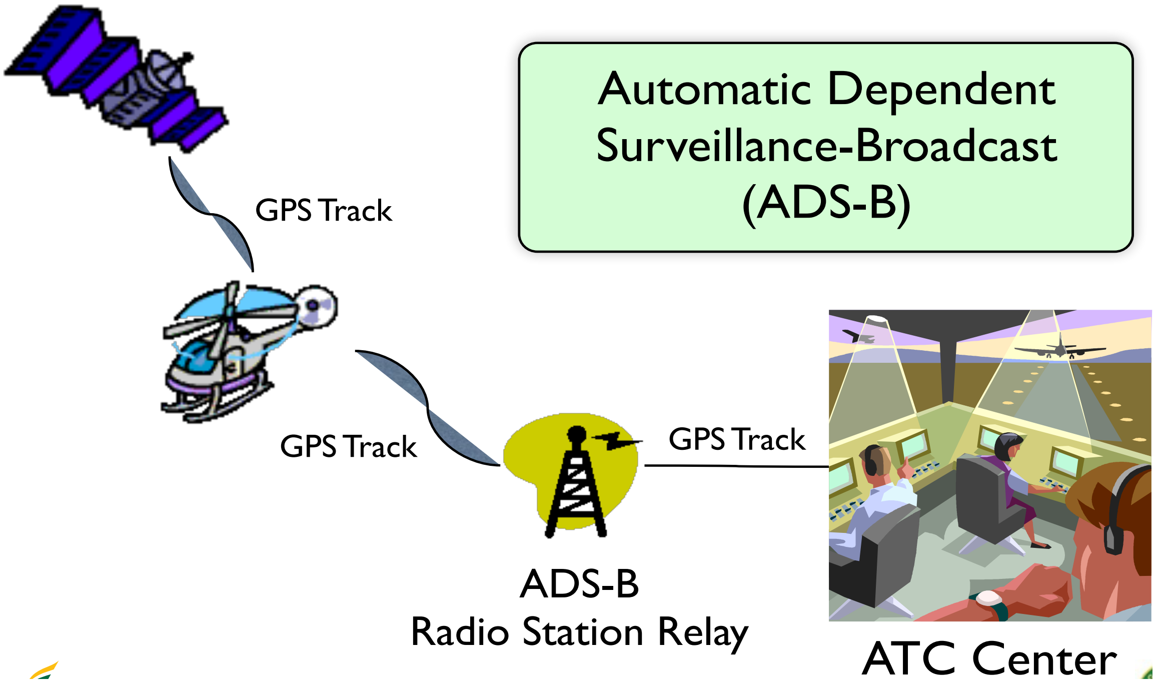


Figure 3 – ADS-B Communication

Helicopter operations in the Campos Basin depend on ADS-B communication to promulgate their current positions and thus manage flight paths and operations safely and effectively (see figure 3 above). Vulnerabilities and their possible exploitation are of interest to a wider audience due to mandatory use of ADS-B in the United States by 2020 and in Europe by 2030. ADS-B is already in use in parts of North America, Europe, China, and Australia.

ADS-B communication is unencrypted and unauthenticated; anyone can listen to it and decode the transmissions from aircraft in real time. ADS-B does not make use of data level authentication of data from aircrafts, only checksums are use to verify integrity of a submitted message.

ADS-B communication can be attacked through interception of messages, jamming of transmission, and injection of messages. The target of ADS-B attacks can be generally grouped into two categories: aircrafts, helicopters in our scenario, and ground stations.

### 4.2 ADS-B Threats

We will seek to determine the impacts of interception, jamming, and injection attacks and their direct effects to the Command and Control operations of critical infrastructure. The ADS-B attacks below are provided from a Graduate Research

Project by Donald McCallie in June of 2011 and will be used a reference source for this project.

### 4.2.1 Interception Attacks

Name: *Aircraft Reconnaissance*

Description: Intercepts and decodes ADS-B transmissions.

Purpose: Target specific aircraft, gain knowledge about movement of assets and build an air order of battle, often the first step of a more insidious attack.

Target: Aircraft

Attack Technique: Interception of ADS-B OUT signals

Difficulty: Low

### 4.2.2 Jamming Attacks

Name: *Ground Station Flood Denial*

Description: Disrupts the 1090MHz frequency at the ground station

Purpose: Blocks all ADS-B signals intended for the ground station. Impact is localized to a small area determined by the range and proximity of the jamming signal to the ground station.

Target: Aircraft and Air Traffic Controllers

Attack Technique: Jamming signal capable of disrupting the 1090MHz frequency range or GPS frequency

Difficulty: Low

Name: *Aircraft Flood Denial*

Description: Disrupts the 1090MHz frequency for an aircraft

Purpose: Blocks all ADS-B signals intended for an aircraft. Most significant impact involving this attack stems from gaining close proximity to an airport and affecting landing or taxi operations.

Target: Aircraft

Attack Technique: Jamming signal capable of disrupting 1090MHz

Difficulty: Medium

### 4.2.3 Injection Attacks

Name: *Ground Station Target Ghost Inject*

Description: Injects an ADS-B signal into a ground station

Purpose: Cause illegitimate (i.e., ghost) aircraft to appear on the ground controller's console.

Target: Ground Station

Attack Technique: Inject message that conforms to ADS-B message protocol and mirrors legitimate traffic.

Difficulty: Medium-High

Name: *Aircraft Target Ghost Inject*

Description: Injects an ADS-B signal into an aircraft

Purpose: Cause illegitimate (i.e., ghost) aircraft to appear on an aircraft's console.

Target: Aircraft

Attack Technique: Inject message that conforms to ADS-B message protocol and mirrors legitimate traffic

Difficulty: Medium-High

Name: *Ground Station Multiple Ghost Inject*

Description: Injects ADS-B signals into a ground station

Purpose: Overwhelm the surveillance system and create mass confusion for the ground controller

Target: Ground Station

Attack Technique: Inject multiple messages that conform to ADS-B message protocol and mirrors legitimate traffic

Difficulty: Medium-High

## 4.3 Serious Game to Detect and Adequately Respond to ADS-B Cyber Attacks

Unlike traditional games, serious games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. A serious game provides simulation of a real world situation and offers new experiences, insights, and knowledge to game players and observers, transforming learning into a more-engaging and dynamic process. Gameplay elements such as scoring, the possibility of winning or losing and embedded prizes may also be included to gauge a participant's progress with regards to established learning goals or objectives.

As described above, ADS-B attacks can focus on either aircrafts or ground stations. We will develop requirements and a Concept of Operations (CONOPS) for a serious game that simulates the effect of cyber attacks on helicopter operations in support of Maritime Oil Fields off the coast of Brazil. The scenario will model Air Traffic Control operations in the Campos Basin and serve as a training tool for Air Traffic Controllers to help detect and respond to ADS-B cyber attacks.

## 5. Stakeholders

The primary stakeholders for this project are listed below:

Dr. Paulo Costa, GMU C4I Center

pcosta@gmu.edu

(703) 993-9989

Dr. Chris Ondrus, GMU Simulation & Game Institute

condrus@gmu.edu

(703) 993-9423

## 6. Project Scope

To allow for completion of the project within a semester we will only focus on injection attacks listed in section 4.2.3. The effect of the attacks at varying intensities of injection will be evaluated against critical infrastructure and operations from the perspectives of helicopter pilot and crew and Air Traffic Controllers.

## 7. Assumptions

Attacks such as interception and passive monitoring are critical to the successful completion of more advanced attacks such as injection. We will assume that reconnaissance and monitoring has already occurred and will not simulate these prerequisite activities by malicious entities. We will also assume that helicopters will follow all directions provided by Air Traffic Controllers as long as they will not result in obvious harm to life or assets.

## 8. Deliverables

The five deliverables listed below will be completed by the end of the semester:

1. Requirements Documentation
    a. System requirements for the game including "gamification" piece implemented by SGI students.
2. CONOPS
    a. Frame the problem
    b. Define the solution for the game based on the existing simulation engine.
3. Proof of Concept Evaluation Plan (and evaluation report)

## 9. Preliminary Requirements

Functional Requirements

- The system shall integrate existing simulation software packages with Mak VR-Forces to generate a serious game for purposes of better preparing air traffic controllers to identify, assess, and mitigate cyber attacks.
- The system shall simulate injection attack types on air traffic control consoles.
- The system shall simulate injection attack types on ADS-B technology.
- The system shall be capable of handling at least fifty simultaneous air vehicle tracks.
- The system shall simulate at least five ADS-B broadcast towers.
- The system shall simulate at least one air traffic control tower.
- The system shall utilize the existing C2 Collaborative Research Testbed Integration to generate cyber attacks.
- The system shall utilize the existing C2 Collaborative Research Testbed Integration Engine to simulate the effects of cyber attacks on IT components.
- The system shall utilize the existing Exata/Cyber Emulation Environment to simulate cyber warfare.
- The system shall update aircraft tracks at least every second.
- The system shall generate ghost tracks for placement into the air traffic control view.

Scoring/Metrics

- The system shall provide output to the player that captures the time for flight patterns under their control measured by an expected performance.
- The system shall provide output to the player that captures the estimated degradation in helicopter flight operations due to a cyber attack, along with its duration.
- The system shall provide output to the player that captures the time and accuracy in responding to and recovering from a cyber attack.

Difficulty Levels

- The system shall have two levels of difficulty. Difficulty levels are determined by an increase in quantity of simultaneous or near-simultaneous attacks and/or severity in operational degradation caused by attack(s).
- The system shall allow the player to increase the difficulty to the highest threshold.

- The system shall allow the player to decrease the difficulty to the lowest threshold.

Gameplay History

- The system shall maintain records for at least 10 unique players.
- The system shall maintain a users performance metrics from at least their previous 10 games.
- Upon a user request the system shall display a users performance metrics for at least their previous 10 games.

# 10. Technical Approach

In using our knowledge of the Systems Engineering processes we have gained throughout the SEOR graduate program and by leveraging the experience we have from working in our respective fields, we have formulated a technical approach that provides our teammates and ourselves the best chance for success. Each deliverable listed in section 8 adds to the understanding and knowledge we expect to gain about the system as we research and further enhance its capabilities.

We plan to start working on the CONOPS and Requirements documentation as we perform our research and better refine the problem space. As we work the CONOPS documentation we will interact with the SGI group to create a Storyboard description of how the game will be interacted with, from the perspective of the trainee. As we work through the CONOPS, we will continue to discover requirements that will be applicable at both, the system and software level, and we will continue to refine those. The premise behind the Storyboards is to allow for parallel efforts between both teams. This approach provides the SGI group timely guidance to start their high-level design efforts and thus avoid being on a holding pattern.

While the SGI group is evaluating the high-level design guidelines provided, the SEOR team will start looking into the APIs for the respective components of the system and create content for the IRS document. This will aid in the integration of the different components of the system so when the time arrives we will have knowledge on what interfaces and operation calls are available.

During this time we also be working with the SGI group to determine what level of user interaction can be captured from the prototype in order to develop a meaningful Evaluation Plan/Report. One desirable related activity would be to capture data during users interaction with the game to better understand their performance and areas where they might be able to improve. Some initial thoughts on data they we would like to capture is (1) Rate of positive identification of threats, (2) Response time in identification, (3) Corrective action chosen, and (4) Increased C2 degradation due to improper actions taken. As we progress through our research, we intend to further refine and build upon the above-mentioned metrics.

## 10.1 Simulation Approach

In order to build the serious game we intend to leverage work previous completed in a joint effort between the GMU C4I Center and the Technological Institute of Aeronautics in Brazil, the C2 Collaborative Research Testbed. The Testbed is a set of Commercial Off-the-Shelf (COTS) tools that provide a realistic and complex simulation environment to conduct C2 research experiments for operational scenarios, which we will be utilizing for our air traffic controller scenario. The C2 Collaborative Research Testbed consists of a number of different components to simulate cyber attacks on a C2 environment. The main components that make up the Testbed are as follows: (1) A Core Simulation Manager that consists of Cyber

Attack and IT Effects Generators, (2) A selectable attack emulation environment (Exata Cyber), (3) MAK VR-Forces application, (4) and various interfaces to allow the components to communicate, see Figure 4 below for an overview of the architecture.

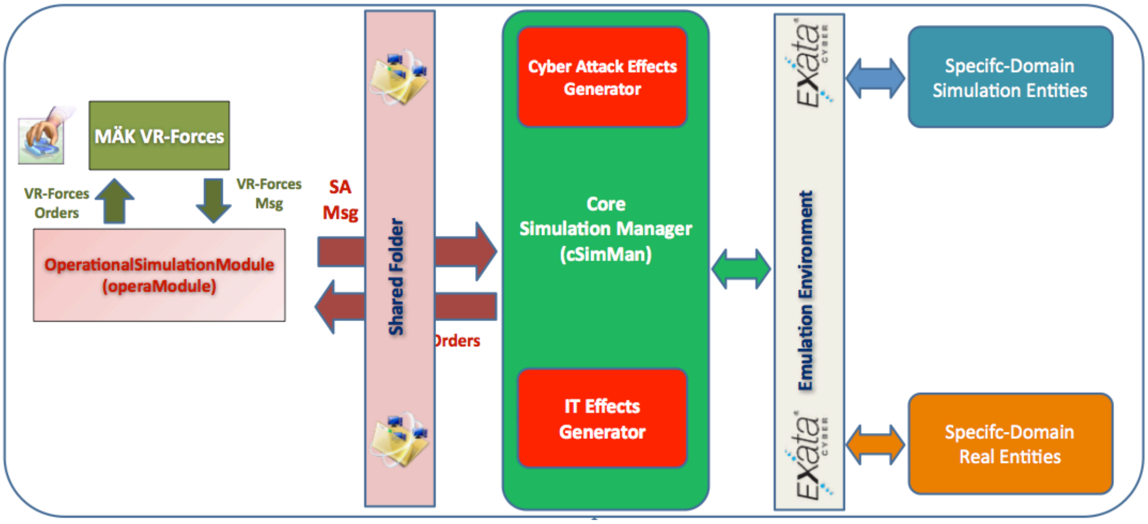

MÄK VR-Forces
VR-Forces Orders
VR-Forces Msg
OperationalSimulationModule (operaModule)
SA Msg
Shared Folder
Orders
Cyber Attack Effects Generator
Core Simulation Manager (cSimMan)
IT Effects Generator
Exata CYBER
Emulation Environment
Exata CYBER
Specifc-Domain Simulation Entities
Specifc-Domain Real Entities

Figure 4 – Simulation-Emulation Scenario

We plan to leverage this work by researching the Application Programming Interfaces (APIs) for the components, specifically the VR-Forces application and the Cyber Attack & IT Effects Generator. This is to understand which messages, operations, and classes will need to be utilized in order to make the simulated cyber attacks be represented properly inside of the VR-Forces implementation of the serious game.

Another piece of software that will be integrated with VR-Forces is the Unity Game Design Engine. Unity will be used by the SGI group in order to enhance the visual aspects, such as terrain and building structures, inside of the game. VR-Forces interfaces with Unity in order to accept 3-dimensional (3D) model updates to the Geographical Information System (GIS) data that comes preloaded with the tool. One of the skills that the SGI group will bring to the effort is to build these enhanced 3D models inside of Unity and then integrate them to VR-Forces and map them to object instances so that the visual aspects of the game are appealing to the user.

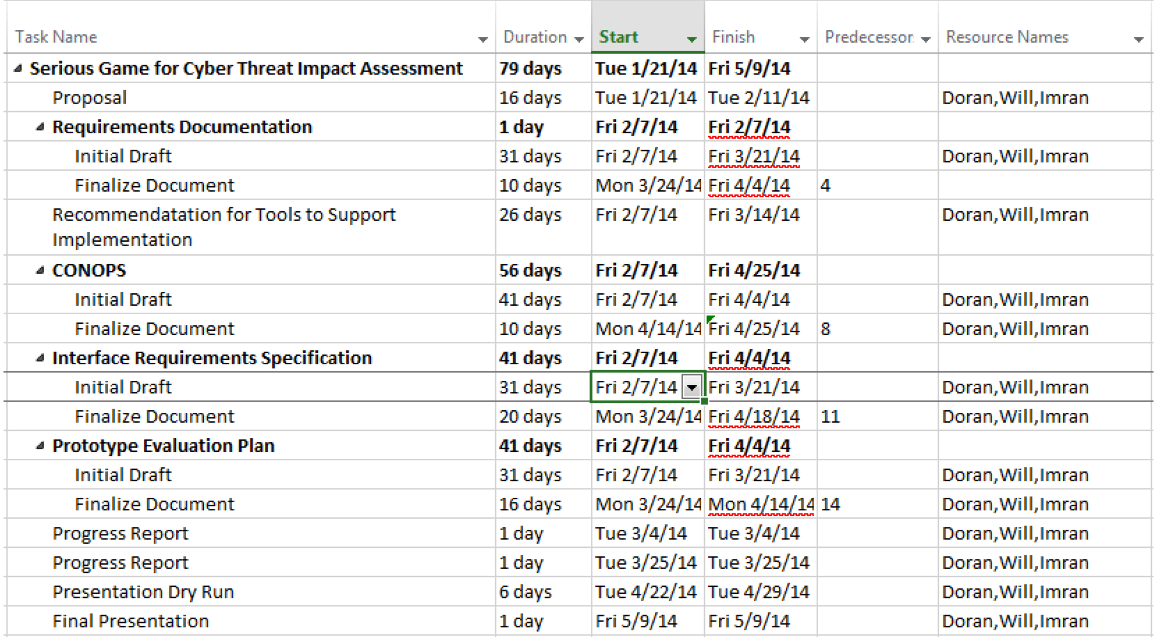
Another overall objective is build beyond the framework put in place by the C2 Collaborative Research Testbed by implementing additional tools in place that will allow this work to continue beyond our involvement.

Finally, there are many different types of cyber threats that can be used to attack operational C2 environments yet we are addressing only one type of threat during this compressed design and development timeline. With the proper architecture and tools in place the foundation that has been built can be expanded upon by teams in the future to build a more robust system that can incorporate threats that we do not touch upon and even new threat types that are discovered in the future.

## 11. Expected Results

The deliverables listed in section 8 will be completed by the end of the semester. A working prototype of the serious game in accordance with the CONOPS and requirements deliverables will also be completed and evaluated.

## 12. Project Work Breakdown Structure



| Task Name | Duration | Start | Finish | Predecessor | Resource Names |
|---|---|---|---|---|---|
| **Serious Game for Cyber Threat Impact Assessment** | **79 days** | **Tue 1/21/14** | **Fri 5/9/14** | | |
| Proposal | 16 days | Tue 1/21/14 | Tue 2/11/14 | | Doran,Will,Imran |
| **Requirements Documentation** | **1 day** | **Fri 2/7/14** | **Fri 2/7/14** | | |
| Initial Draft | 31 days | Fri 2/7/14 | Fri 3/21/14 | | Doran,Will,Imran |
| Finalize Document | 10 days | Mon 3/24/14 | Fri 4/4/14 | 4 | |
| Recommendatation for Tools to Support Implementation | 26 days | Fri 2/7/14 | Fri 3/14/14 | | Doran,Will,Imran |
| **CONOPS** | **56 days** | **Fri 2/7/14** | **Fri 4/25/14** | | |
| Initial Draft | 41 days | Fri 2/7/14 | Fri 4/4/14 | | Doran,Will,Imran |
| Finalize Document | 10 days | Mon 4/14/14 | Fri 4/25/14 | 8 | Doran,Will,Imran |
| **Interface Requirements Specification** | **41 days** | **Fri 2/7/14** | **Fri 4/4/14** | | |
| Initial Draft | 31 days | Fri 2/7/14 | Fri 3/21/14 | | Doran,Will,Imran |
| Finalize Document | 20 days | Mon 3/24/14 | Fri 4/18/14 | 11 | Doran,Will,Imran |
| **Prototype Evaluation Plan** | **41 days** | **Fri 2/7/14** | **Fri 4/4/14** | | |
| Initial Draft | 31 days | Fri 2/7/14 | Fri 3/21/14 | | Doran,Will,Imran |
| Finalize Document | 16 days | Mon 3/24/14 | Mon 4/14/14 | 14 | Doran,Will,Imran |
| Progress Report | 1 day | Tue 3/4/14 | Tue 3/4/14 | | Doran,Will,Imran |
| Progress Report | 1 day | Tue 3/25/14 | Tue 3/25/14 | | Doran,Will,Imran |
| Presentation Dry Run | 6 days | Tue 4/22/14 | Tue 4/29/14 | | Doran,Will,Imran |
| Final Presentation | 1 day | Fri 5/9/14 | Fri 5/9/14 | | Doran,Will,Imran |

## 13. References

"Simulation-based Evaluation of the Impact of Cyber Actions on the Operational C2 Domain", Paulo C.G. Costa, Ph.D., Associate Professor, Department of Systems Engineering and Operations Research / C4I Center/ Center for Air Transportation Systems Research

"Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service"; OMB Approval of Information Collection, https://federalregister.gov/a/2010-19809

"Exploring Potential ADS-B Vulnerabilities in the FAA's Nextgen Air Transportation System Graduate Research Project", Air Force Institute of Technology, Donald L. McCallie, BS, MS Major, USAF, http://www.hsdl.org/?abstract&did=697737

http://www.radartutorial.eu

http://www.oig.dot.gov/sites/dot/files/ADS-B_Oct%202010.pdf

"Hackers + Airplanes No Good Can Come Of This", Defcon 20, Brad "RenderMan" Haines, CISSP