Air Traffic Controller
Cyber Attack Evaluation Serious Game (ACES)

Concept of Operations

Spring Semester 2014
OR/SYST 699 Capstone Project

George Mason University
Fairfax, Virginia

THIS PAGE INTENTIONALLY LEFT BLANK

SIGNATURE PAGE

Submitted by _____ Date: _____
Doran Cavett
MSSE Candidate, SEOR Team

Submitted by _____ Date: _____
Imran Shah
MSOR Candidate, SEOR Team

Submitted by _____ Date: _____
Wilbert C. Fontan, P.E.
MSSE Candidate, SEOR Team

Concurred by _____ Date: _____
Paulo CG Costa, PhD
Sponsor, GMU C4I Center

Concurred by _____ Date: _____
Christopher Ondrus, PhD
Sponsor, GMU Simulation & Game Institute

Approved by _____ Date: _____
Kathryn Blackmond Laskey, PhD
Professor, OR/SYST 699

Executive Summary

The security and economic prosperity of a nation depend on critical infrastructure that is increasingly at risk from a variety of hazards, including cyber-attacks. Increasing connectivity and automation of critical infrastructure components and processes results in vulnerability to attacks on the cyber-infrastructure supporting our automated processes. This creates an opening for hostile actors to disrupt society through cyber-attacks. Progressively more, the cyber domain is seen as a new dimension of warfare — one that is especially open to lightweight, agile actors who do not require resources for major hardware investments and can operate from remote locations to disrupt our critical infrastructure.

The security and resilience of these assets, systems, networks, and functions — whether physical or cyber — requires a partnership-layered approach that involves individuals and communities, businesses and non-profits, schools and universities, and governments at all levels, as well as a clear understanding of the risks we face. Only together, they can build a better understanding of the potential mission impacts of hostile cyber operations, better processes for planning for and rapidly responding to cyber threats, and better ways to assess both the impact of cyber operations and the effectiveness of their responses.

Serious games provide a means to evaluate cyber-attacks against critical infrastructure without the need for large investments in real world test scenarios and the potential harm or loss of life. A team of graduate students from the George Mason University (GMU) Systems Engineering and Operations Research Department (henceforth the SEOR Team) will guide and assist a cadre of GMU Simulation and Gaming Institute (SGI) students throughout the design, development, and prototyping phases of a serious game based on the contents of this document and subsequent requisite requirements documents. Phases or milestones not completed by the end of the Spring 2014 semester should be considered as potential themes for future collaborative efforts between both the organizations.

The Air Traffic Controller Cyber-attack Evaluation Serious (ACES) game will simulate cyber-attacks onto the air traffic management (ATM) system used to conduct off-shore helicopter operations in support of oil production off the Rio de Janeiro coast of Brazil. This document captures the operational concept of the ACES game to support ATM risk assessment and the development of strategies for mitigating the effects of attacks on its cyber infrastructure. ACES game will provide a venue for training air traffic management personnel and for understanding the impacts of cyber-attacks on ATM infrastructure and operations which will, in turn, help them identify and prepare effective mitigating actions.

The ACES game Concept of Operations (CONOPS) is a standalone document that describes at a high level how the ACES game will be employed to mitigate the impact of a cyber-attack to an Automatic Dependent Surveillance-Broadcast (ADS-B) based ATM system. Storyboards were used to assist in the developments of the ACES concept of operations due to the program's highly demanding schedule. They provided a timely iterative development process between the SEOR team, the SGI team, the Sponsors, and Professors. Ensuing requirement documents shall include the traditional use cases for the design and development teams to go by. Finally, this document is also intended to help codify future ADS-B based ATM cyber-security design and development decisions.

Revision History

Revision	Date	Summary of Changes
-	5/08/14	Original issue

Table of Contents

Table of Figures

List of Tables

1. GENERAL DESCRIPTION

The ACES game project is rapid design and development effort aimed at addressing the ATM risks encountered by air traffic controllers when challenged by a cyber-attack. It began as one of several potential GMU MSOR/MSSE capstone course research projects offered, focused on putting learned OR/SE skills into practice.

The initial description of the operational need to be addressed was provided by Dr. Paulo Costa, GMU Associate Professor and a faculty member of GMU's C4I Center. The operational needs established by his presentation, "Simulation-based Evaluation of the Impact of Cyber Actions on the Operational C2 Domain", set the foundation for the ACES game project.

The ACES game Concept of Operations (CONOPS) is a standalone document that describes at a high level how the ACES game will be employed to mitigate the impact of a cyber-attack to an ADS-B based ATM system. Storyboards were used to assist in the developments of the ACES concept of operations. They provided a timely iterative development process between the SEOR team, the SGI team, the Sponsors, and Professors. Finally, this document is also intended to help codify future ADS-B based ATM cyber-security design and development decisions.

2. MISSION

Unlike traditional games, serious games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. The ACES game will provide simulation of a real world situation and shall offer new experiences, insights, and knowledge to Air Traffic Controllers and observers, transforming learning into a more-engaging and dynamic process. Gameplay elements such as scoring, the possibility of winning or losing will be included to gauge a participant's progress with regards to established learning goals or objectives.

The operational concept described in this document is focused on cyber-attacks on helicopter operations in support of Maritime Oil Fields off the coast of Brazil. These off-shore flights are often conducted at low altitudes and at distances beyond the range of any available mainland radar (see figure 1).

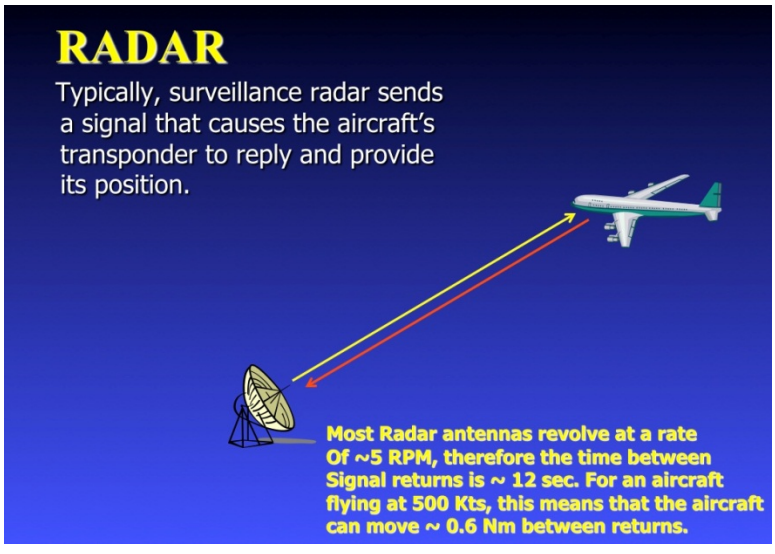

Figure 1 - How Radars Work?

As a result, the safe and effective management of these offshore helicopter operations is then provided through the Automatic Dependent Surveillance-Broadcast (ADS-B) system (see figure 2).

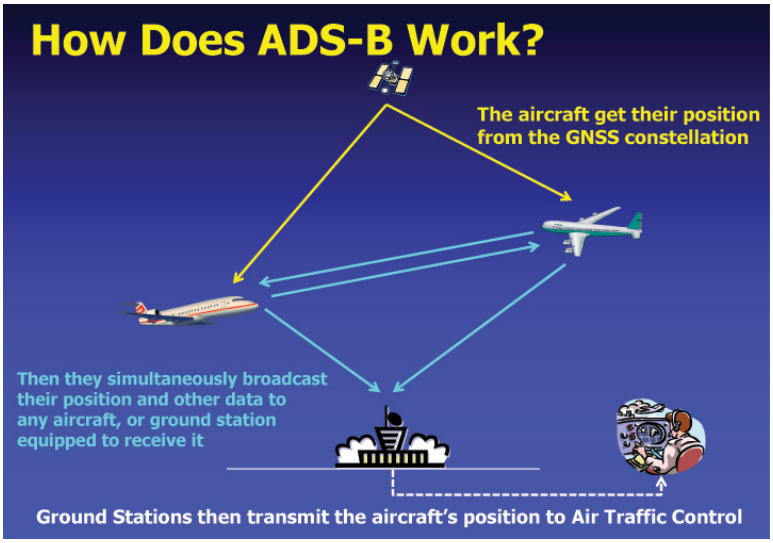

Figure 2 - How does ADS-B Work?

ADS-B communication is unencrypted and unauthenticated; anyone can listen to it and decode the transmissions from aircraft in real time. It does not make use of data level authentication of data from aircrafts, only checksums are used to verify integrity of a submitted message. ADS-B communication can be attacked through interception of messages, jamming of transmission, and injection of messages. A general description of these types of threats is shown below:

Type:	**Interception Attack**
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
Technique:	Interception of ADS-B OUT signals
Difficulty:	Low

Type:	**Jamming Attack**
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
Technique:	Jamming signal capable of disrupting the 1090MHz frequency range or GPS frequency
Difficulty:	Low

Type:	**Jamming Attack**
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
Technique:	Jamming signal capable of disrupting 1090MHz
Difficulty:	Medium

Type:	**Injection Attack**
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
Technique:	Inject message that conforms to ADS-B message protocol and mirrors legitimate traffic.
Difficulty:	Medium-High

Type:	**Injection Attack**
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
Technique:	Inject message that conforms to ADS-B message protocol and mirrors legitimate traffic
Difficulty:	Medium-High

Type:	**Injection Attack**
Name:	Ground Station Multiple Ghosts 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
Technique:	Inject multiple messages that conform to ADS-B message protocol and mirrors legitimate traffic
Difficulty:	Medium-High

Current ABS-B 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.

The effect of the attacks at varying intensities will be evaluated against critical infrastructures and operations from the perspective of an Air Traffic Controller (ATC).

3. OPERATIONS

This section is used to identify and explain the business needs, user groups, organizations, environment, interdependencies and other circumstances in which the solution must operate.

3.1. Missions (Primary/Secondary)

The primary mission of ACES is to offer a venue for training ATCs and for understanding the impacts of cyber-attacks on ATM infrastructure and operations which will in turn help them identify and prepare effective mitigating actions.

To better understand the potential mission impacts of cyber threats and to allow for the development of improved operational and risk management processes, the ACES game will be used to simulate the real-time scenario, cyber-attacks, and their effects.

3.2. Policies, Assumptions and Constraints

3.2.1. Policy Assumptions

GMU's SGI-promulgated standards, policies and best practices pertinent to serious game development will apply in this project. Best practices fostered by the U.S. Entertainment Software Association should also be taken into consideration while developing and refining ACES. Examples of policies and best practices to be adopted are those relating to Anti-piracy, intellectual property, and parental control.

The Entertainment Software Rating Board (ESRB) rating for ACES should be ADULT (content suitable only for adults ages 18 and above) as it is comparable to the typical demographics of an ATC plus, it might include prolonged scenes of violence and/or strong language.

3.2.2. Assumptions

This project shall be executed under a number of assumptions. These assumptions are designed to provide boundaries and guidance necessary for the development of ACES' CONOPS and to be able to scope out the level of effort required by the SEOR and SGI teams.

We shall assume the first version of ACES will be made available at the GMU C4I Center and SGI Development Center. Initially, the user (also known as the "player") will launch ACES game from a designated workstation.

We shall also assume the SGI team and members of the C4I Center will provide technical support, as needed. GMU's Department of Systems Engineering and Operations Research, along with its Simulation & Game Institute will provide logistical guidance and assistance, as required.

3.2.3. Constraints

Workstation processing power will be limited to what is available at the SGI Center. C4I Center and SGI's investment in hardware, servers, and video game development tools will determine ACES operational investment. System interface and interoperability requirements with applicable legacy systems shall then be determined and controlled by these two sponsors and not by the SEOR team.

The sharing of information between ACES and systems it operates and/or interfaces with shall be constrained by current C4I and SGI standard operating procedures and practices.

In addition, to build ACES's first prototype the SEOR-SGI team shall leverage work previously completed in a joint effort between the GMU C4I Center and the Technological Institute of Aeronautics in Brazil, the C2 Collaborative Research Testbed. It shall also use two COTS serious games development applications utilized during the aforementioned joint effort: Unity and MAK VR-Forces application.

The following are high-level constraint requirements for the ACES system:

- The system shall leverage from existing C4I Center and SGI's hardware, server, and development tools
- Interoperability and interface requirements shall be set by SGI development team
- The system shall leverage from the C4I Center's C2 Collaborative Testbed

3.3. Operational Description

3.3.1. Operational Concept

The major players of this serious game are the user (aka the player) and ACES. Although relevant, maintenance and support personnel are overlooked in this document. Being a serious game, the interactive nature between both, the player and the game is understandably the key design and development factor. The intended audience for ACES is the ATM personnel, particularly, the ATC.

Following traditional video games approaches, ACES' graphical user interface (GUI) will allow the user to interact with the game. In essence, every aspect of the game will involve the GUI in order for the user to progress or influence the gameplay.

The user will launch the application, create/delete/edit accounts, and play the ACES game.

Akin to a typical video game, the user will be visually challenged with two-dimensional and 3-dimentional entities mapped on the screen – representative of a cyber-attack scenario – he or she will be expected to react upon. The user's response will be achieved in traditional ways such the use of the mouse (right/left clicking) and/or clicking on keys on the keyboard.

The operational setting for the ACES game is Brazil's Campos Basin where over 30 oil fields (see figure 3) managed by large corporations such as, Petrobras, Esso, and Shell, are located at and accounts for over a million barrels a day of petroleum production (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.

Figure 3- 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 from the Macaé airport, which only supports air traffic within a 45 nautical mile radius and 9500 foot and above altitude. ATM for these offshore helicopter operations is then provided through the Automatic Dependent Surveillance-Broadcast (ADS-B) system (see figure 4).

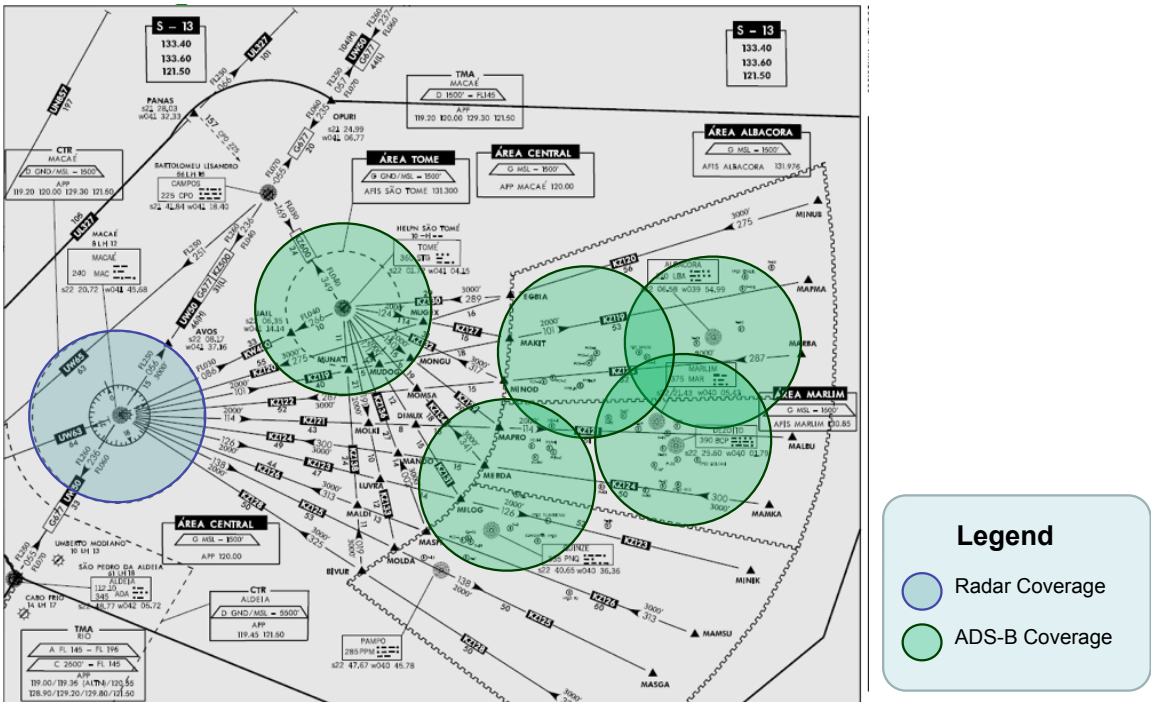

Figure 4 - Campos Basin Radar & ADS-B Coverage

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.

ATM 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, the ACES game will be used to simulate the real-time scenario, cyber-attacks, and their effects. As expected, an ATC operating (or about to operate) in an ADS-B environment would be the target player audience for the ACES game. Due to time constraints, the first prototype of ACES shall not take into consideration any radar contact feed.

Key parameters or capabilities ACES should take into consideration for scoring/metrics purpose are shown in table 1 below.

Capability	Attribute	Measure	Metric
Attack Detected and Positively Identified	Attack Characteristics and Pattern	Attack Type, Target, and Technique	Volume detected; % detected; % positively identified
Identified attacks quarantined(2)	Number of Affected Devices and Response Time	Number of consoles quarantined and recovered	% of ATC consoles recovered; Time of recovery(1)

Capability	Attribute	Measure	Metric
Recovery to Attack Event	Computer Terminal Down Time	Time to full recovery from attack	Time to recovery
Mission Assurance	Flight operations to and from Oil Platforms	Operations Tempo (OPTEMPO)	Sortie Generation Rate; Average mission fuel consumption; Average mission flight time
Mission Assurance	Flight operations to and from Oil Platforms	Mission Reliability (MR)	% of flight operations successfully completed
Schedule Adherence	Late Flight Departures and Arrivals	Schedule Slippage	% of late departures & arrivals; average late departure and arrival times

Table 1 - Key Metrics

NOTES:

(1) Recovery is defined as the threat has been detected, positively identified, and prescribed recovery procedures have been implemented.

(2) Quarantined is defined as the cyber threat has been removed from the ATC's console.

(3) Mission Reliability is defined as the probability of completing entire sortie without failure of any Mission Essential Function

3.3.2. Environmental Conditions

The ACES game will be used from a desktop or a laptop computer, located at either the C4I Center or the SGI facilities. The necessary software tools and programs will require traditional IT hardware and software components that prescribe a controlled temperature and humidity range.

Those specific environmental requirements shall be scoped out and complied with by the sponsors of this project at the C4I Center and the CGI team.

3.3.3. Interoperability with Other Elements

ACES will be integrated into the current hardware elements the SGI facilities currently possess. The tools to design and develop ACES are mostly COTS products, if not all. The SGI team will then be expected to identify and manage any identified interoperability demands with the support of the project sponsors at the SGI facilities and at the C4I Center.

3.4. Product Support Description

The support for the ACES game provided by the SEOR team will be minimum. Ensuing SEOR and SGI classes may or may not continue refining the ACES game.

Periodic hardware/software upgrades and modifications at the SGI facilities and C4I Center will be addressed by those currently assigned to such responsibilities.

3.5. Potential Impacts

The C2 Collaborative Research Testbed to be leveraged from is a set of tools that provide a realistic and complex simulation environment to conduct C2 research experiments for operational scenarios, which will be utilized to developed ATC scenarios.

The amount of leveraging possible is contingent upon researching the Application Programming Interfaces (APIs) for the components, specifically the VR-Forces application.

Integrating the Unity Game Design Engine with VR-Forces is a major effort of concern. Unity will be used by the SGI team to provide the gaming interface.

Finally, licensing limitations and organic technical expertise shall play a major factor on the level of effort required to accomplish these steps.

3.6. Storyboards

The SEOR team has developed a series of storyboard (SB) for SGI team to guide their design and development efforts by. The storyboards can be found in Appendix C.

3.7. Consideration of Alternatives

Although not part of this project, an analysis of alternatives for a solution aimed at training ATM personnel on how to handle cyber-attacks, along with a tool to aid in the development of improved cyber-attack tactics, techniques, and procedures might have led to two known activities: Wargames and Limited Objective Experiments. Although considered time consuming and perhaps more expensive solutions when compared to a serious game, they are indeed alternatives the sponsors might want to keep in mind. It is important to highlight these tools can later on assist in fine tuning and/or complement the ACES game.

A brief description of such efforts is provided below.

3.7.1. Limited Objective Experiment (LOE)

The limited objective experiment is a narrowly scoped, analytically focused concept assessment or prototype validation event. It provides final dress rehearsal of a concept or major component of a concept prior to its final validation in a full joint warfighting experiment.

3.7.2. Wargame

There are two categories of wargames: Exploratory and Scrubbing

Exploratory Wargame — the exploratory wargame is a critical examination of a concept under limited operational conditions to further concept development. It provides the first opportunity to explore a concept in a competitive environment, subject to opposing concepts, actions, and counter-actions to identify shortfalls and gaps and plan subsequent concept refinement.

Scrubbing Wargame — the scrubbing wargame is a robust test of a concept in a simulated operational environment to support quantitative analysis. It provides a rigorous examination of a maturing concept under conditions supporting structured analysis of outcomes to formulate final concept maturation strategy.

4. SECURITY

Security of air traffic operations and the oil operations will be evaluated according to compliance with Brazilian aircraft separation guidelines and avoidance of collisions with other aircrafts, oil platforms, or land.

According to Brazilian aircraft guidelines vertical separation of 1000 feet is required between aircraft and 500 feet for helicopters. In route lateral separation of 15 nautical miles is required for both aircraft and helicopters. Horizontal separation of 5 nautical miles is required when an aircraft is in route or 3 nautical miles when it is close to the airfield.

5. SAFETY

ACES shall place emphasis on preventing players from becoming desensitized to the significance of managing offshore flight operations, where lives, expensive equipment and critical operations are at stake. ACES shall remind its users to review national, state, and local laws, rules, and regulations regarding the safe management of air traffic services (please see Appendix D for Brazil's Rules of Air Traffic Services).

Prolonged exposure to 3-D video games may alter visual perception and might cause dizziness, nausea, cramps or involuntary movements. ACES shall remind its users to immediately stop playing the game should these symptoms appear and to avoid playing this game if in poor physical condition, sleep deprived, and/or are under the influence of drugs or alcohol.

6. FUTURE

The ACES game is intended to evolve into a more effective and comprehensive ATM – all cyber threat – risk management tool. There are many different types of cyber threats that can be used to attack operational C2 environments yet the SGI team is challenged with addressing only one or few types of threat at a time (the malicious injection of false ADS-B messages, the first).

An overall desire of the SEOR-SGI team is to build beyond the framework put in place by the C2 Collaborative Research Testbed by implementing additional tools, allowing this work to continue beyond our involvement. Future SEOR-SGI teams should then consider developing a more robust system that can incorporate threats we are unable to touch upon this semester and even new attack vectors that are discovered in the future.

The ultimate goal is to achieve some or all of the following desired technical and operational capabilities:

- **Technical**

An integrated ATM cyber network defense toolset complementing existing enterprise support environments providing improved visualization, management, and protection of computer networks installed and tested at Air Towers utilizing ADS-B technologies with capabilities consisting of

1. Behavior-based attack detection, counter-attack and inoculation of ATC workstations
2. Leak detection of both insider and outsider threats
3. Network attack data collection, data analyzed and future attack predictors
4. Network operational control at Airport Tower with visibility at higher Headquarters

- **Operational**
    1. Develop future Operational CONOPS and Tactics Techniques & Procedures (TTPs)
    2. Define and describe the ability of cyber network operations capabilities to support Regional and National ATM requirements.
    3. CONOPs and TTPs to foster relevant Research, Development, and Acquisition efforts.
    4. TTPs based actual integrated tools and lessons learned during technical and operational demonstration events.

APPENDICES

A Glossary of Terms (if necessary)

B Acronym List

C Storyboards

D References

Appendix A: GLOSSARY OF TERMS

- Shall – expresses a requirement that is mandatory.
- Should – expresses a requirement that is important but is somewhat flexible.
- Gameplay – plot or manner in which a video game is played

Appendix B: ACRONYM LIST

3D	Three Dimensional
ACES	Air Traffic Controller Cyber Attack Evaluation Serious (Game)
ATC	Air Traffic Controller
ATM	Air Traffic Management
C4I	Command, Control, Communications, Computer, and Information
ESA	U.S. Entertainment Software Association
ESRB	Entertainment Software Rating Board
GMU	George Mason University
HW	Hardware
HELO	Helicopter
IA	Information Assurance
OA	Operational Assessment
OILPLAT	Oil Platform
OR	Operations Research
SE	Systems Engineering
SME	Subject Matter Expert
SOP	Standard Operating Procedure
T&E	Test & Evaluation

Appendix C: STORYBOARDS

SB-1. Creating New Account and ACES Tutorial

SB-2. Launching ACES

SB-3. ACES Cyber-Attack Injects

SB-4. ACES General Description & Normal Operational Tempo Guidance

SB-5. ACES Scoring / Point / Rewards System

SB-6. Ghost Track Behavior

SB-7. ACES Levels of Difficulty

SB-8. Capturing Lessons Learned / Trend analysis

SB-9. ACES Graphical User Interface

SB 1: Creating New Account and ACES Tutorial

User launches ACES and is presented with a WELCOME screen. User wants to set up an account, so presses the LOGIN button. User is presented with a login page, with an option to register. User clicks on "REGISTER". A new page opens where the user registers and creates a username and a password. User is then redirected back to the login page where now logs in. Once logged in, ACES performs a check based on the basic profile information user filled out prior. Profile information will include a unique handle, first name, and last name.

If it is the first time user profile has been registered within the game a tutorial will automatically be launched. The purpose for the tutorial is to introduce the user to the different type of threats that could be encountered on an air traffic control display through attacking Automatic Dependent Surveillance-Broadcast (ADS-B) technology. Even though this project will focus solely on injection threats, the idea behind the layout of the game is that other threat types can be added to expand upon the serious game design and continue to make it more robust for continued training of real world scenarios and tactics. Through injection of ADS-B messages that conform to ADS-B protocol and mirror legitimate traffic attacks will cause either a single or multiple illegitimate (ghost) aircrafts to appear on an ATC console.

The tutorial will open and give an overview of the air traffic control display the user will be required to interact with. It will give examples of how aircraft detections are represented on the display and the typical information that will be associated with them. This tutorial will give a new user a basic overview of what they should be familiar with and how that information will be displayed in the serious game. The user will be able to view the movement of aircrafts on a screen. A click on an aircraft will allow for radio interaction with commands to respond or adjust course. The user will also be allowed to mark an aircraft as a “ghost” to be ignored. Options for interaction will be available through a dropdown list.

The next part of the tutorial will describe injection threats and how they differ from real aircraft detections. This will be a mixture of basic injection threat descriptions, their behaviors, and how the user can interact with the air traffic control console, within the game, to identify, assess, and ultimately classify aircraft detections as either actual aircraft or injected “ghost” tracks.

Upon the user login, if their credentials are detected as having logged into the system before than rather then automatically launching the tutorial a prompt will be displayed to allow the user to re-launch the tutorial to refresh their knowledge of the game and how to interact with it. The user will also be able to view the scores from the last 10 games played.

SB 2: Launching ACES

Upon completion of the tutorial, or rejecting ACES' prompt about re-launching it, the game will progress through the opening sequence. The opening sequence will demonstrate the capabilities of merging the Unity gaming engine with the VR-Forces software suite to showcase the different styles of gameplay that could be achieved through the integration of the two tools. The "in-game" operator will be shown progressing to their air traffic control console and eventually settle in for their days work, at which point the in-game camera will focus in on the air traffic control display and the game will commence.

The user will initiate the game by triggering a "start game" button. To reiterate, the main focus of ACES game will be the air traffic control display but the first person view camera will be movable so the user can look around their environment if they desire (fig. 6). This will be useful to view aircrafts that are landing and departing from the control tower, rather than from the control screen.

Figure 5 - Air Traffic Controller

Upon the game starting, the camera will be fixed on the air traffic control display so that the training experience can be controlled and the player does not miss any anomalies due to the camera being off-centered. As the game begins the air traffic control simulation engine will start to generate flight paths for aircraft and also, at this point, the tracks of these generate flight paths should be displays on the air traffic control display (fig. 7).

Figure 6 - Typical Radar Console Display

SB 3: ACES Cyber-Attack Injects

The type of cyber-attack chosen for the ACES project is one that injects false ADS-B tracks to the ground station which feeds air contacts to the Air Traffic Controller console/display. The amount of injects, the rate of injects, duration, proximity to actual flight operations are some factors ACES could use to modify the level of difficulty of each round/level of the game.

Upon starting the game and in parallel with the opening sequence, the cyber threat attack generation engine will start randomly generating <injection tracks>. As they are generated, these "ghost" tracks will be fed to the air traffic control console/display. Out of nowhere, these contacts will appear onto the ATC's display. Also, a well thought out cyber-attack may inject ghost contacts which would display common element values (e.g. call sign, speed, altitude; see fig. 10).

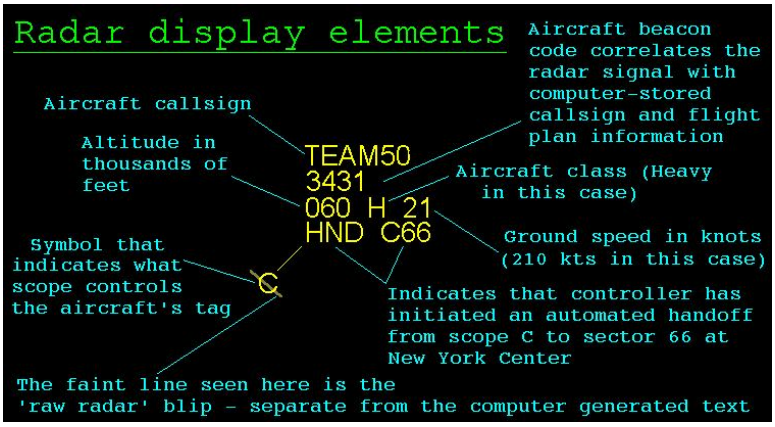

Figure 7 - Radar Display Elements

This is the point where the user has to utilize gained knowledge and techniques – or develop them – to distinguish between an actual track and a false one.

If the user suspects that a track is a threat they will be able to click on the suspicious aircraft and be provided a list of actions to perform in order to investigate the situation further. The options should be:

1. Request contact from the pilot
2. Request a modification to the flight path of the aircraft
3. Seek assistance from nearby pilots (Helicopter would not be under attack and can therefore, assist the ATC with figuring out what's real and what isn't).
    a. Lower levels of difficulty of the game to inject ghost contacts far enough from their landing or take off helipads the user has ample time to react accordingly (i.e. minutes vs. seconds).

Once the user is confident the track is not real, it will be designated as a "ghost" contact by clicking on the suspicious aircraft and designating it as such. ACES will offer additional corrective and follow up actions for the user to consider. Some examples are,

a. Inform immediate supervisor you have validated one (or several ghost contacts) and the ATM system appears to be under attack and/or malfunctioning.

b. Continue operations as normal while advising pilots to remain vigilant and continue discriminating contacts between real and fake ones.

c. Reduce operational tempo to "safe" levels (continue operations without jeopardizing people's lives and valuable equipment). For example, reduce cruise speed, increase time gap between helicopters, and implement loitering zones before landing at airport and OILPLATs.

Another possible scenario with ghost tracks is that of a possible mid-air collision or an imminent landing causing the user to redirect air traffic when it is unnecessary. This could prolong a flight, slow overall operations, or distract controller attention from other aircrafts.

Such decisions will degrade the existing operational tempo and will be captured by ACES and taken into account when figuring the user's final score and PASS or FAIL grade.

SB 4: ACES General Description & Normal Operational Tempo Guidance

The game will allow the player to speed up gameplay, i.e. speed of aircraft flight, up to 10 times real time speed. The ability to speed up the game will allow the player to expedite the flight path of aircraft from the Rio de Janeiro mainland to the oil platforms.

The game will have two levels of difficulty. The first level ("easy" level) will inject ghost tracks randomly. The second level of difficulty ("hard" level) will inject ghost tracks at specific locations to intentionally disrupt the flight patterns of airborne helicopters and confuse the player.

A run of the game will terminate after all aircrafts complete their track movement and land. A successful easy-level game should last no more than 5 - 10 minutes. A successful "hard" game should last no more than 30 minutes.

Only a handful of oil platforms (approximately 50 nautical miles, nm, apart), will be modeled and should be about 100 nm away from the mainland airport. Every OILPLAT will have an inbound and outbound air corridor (see fig. 9). Helicopter maximum speed will be about 150 knots (kts) and a maximum cruise speed of approximately 100 kt.

In reality, the airport and the oil platforms will have radars. These radars have a range of about 45 nm. These feeds also make it to the ATC console. The first iteration of ACES we will not take any radar feeds into account.

For the "easy" game level, helicopter operations will follow the default movement guidelines outlined below,

1. One helicopter about to land and one about to take off at OILPLATs and Airport; minutes apart
2. Airborne helicopters about 15 minutes apart; inbound and outbound from OILPLATs and Airport (see fig 7). All airborne helicopters at the start of the game are in their respective air corridors.

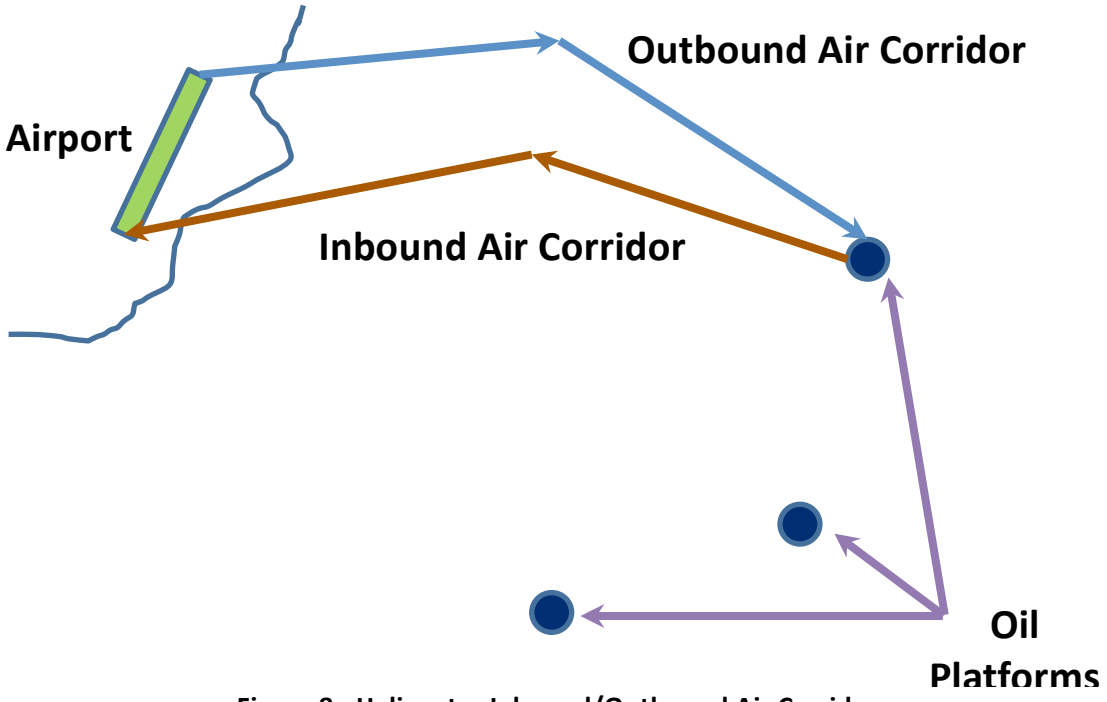

Figure 8 - Helicopter Inbound/Outbound Air Corridors

SB-5. ACES Scoring / Point / Rewards System

Success will be measured by correct identification and assessment of the situation by the player. In general, the game should add points for good decisions made and subtract for incorrect ones. The quicker the action (right or wrong), the larger the quantity of points gained or lost. Consecutive good/bad decisions should lead to a multiplying effect or a bonus / fine.

As threats are injected they will be logged so that a check can be performed to gauge the player's accuracy and the manner in which the attacks are dealt with. These actions will be calculated into a score, which will be displayed throughout the game and upon completion of the scenario.

A bad decision may or may not lead to a negative outcome (e.g. two helicopters colliding in midair; a helicopter running out of fuel at sea). The same will go for a good decision: e.g. bonus pay ($$), fuel saved for future runs or for the next level.

ACES players will either WIN (with the choice of advancing to the next level, play another game of similar difficulty, or exit the game) or LOSE. Winning the game may lead you to extend the playing time; losing to being mocked and/or fired.

Scoring will be provided for each run in the following categories:

1. Time – Difference between expected time to complete one run and actual time of run. Points are subtracted for helicopters that take longer to complete its mission.
2. Fuel Usage – Difference between expected fuel expended and actual fuel expended. Points are subtracted for helicopters that run out of fuel.
3. Cost Disruption to Operation – Calculated by attaching a dollar value to additional time required for a run and extrapolating over a day
4. Number of False Tracks Correctly Identified
5. Damage to Assets / Violation of Rules - subtraction of points for damage to any helicopters or assets as a result of helicopter accident or violation of Brazilian aircraft guidelines:
    - Vertical separation of 1000 feet is required between aircraft and 500 feet for helicopters
    - In route lateral separation of 15 nautical miles is required for both aircraft and helicopters
    - Horizontal separation of 5 nautical miles is required when an aircraft is in route or 3 nautical miles when it is close to the airfield

Scoring will be based on a scale from 0-100. A score of 75 or higher is required to WIN and transition from the "easy" difficulty to "hard". Scoring will be calculated as follows:

1. Time – Max score: 25, Min score: 0.A point is subtracted for every 2 minutes in excess of the expected completion time.
2. Fuel Usage – A player receives an overall score of zero if one or more helicopters run out of fuel.
3. Cost Disruption to Operation – Max score: 25, Min score: 0.A point is subtracted for every $1000 of lost revenue.
4. Number of False Tracks Correctly Identified – Max score: 25, Min score: 0.A point is subtracted for every false track not identified.

5. Damage to Assets / Violation of Rules – Max score: 25, Min score: 0. A player receives an overall score of zero if one or more assets are damaged. A point is subtracted for every 10 minutes an aircraft guideline is violated.

Before and after a game, or whenever queried, ACES will provide a list of the top-10 scorers of the game (by difficulty level).

SB-6. Ghost Track Behavior

Ghost track will behavior in different degrees of "abnormal" behavior the user could use to recognize the ATM system is under a cyber-attack. Subtle anomalies will tend to be harder to identify and therefore will be seen more as the level of difficulty is increased.

The following are a list of abnormal behavior a ghost target will exhibit:

1. A ghost aircraft appearing and updating at a longer rate than normal aircrafts
2. A ghost aircraft appearing with incorrect identifier information that makes no sense.
3. A ghost aircraft appearing in the simulation at a location then appearing at a significantly different position in the next update.
4. A ghost aircraft appearing as a duplicate of an existing legitimate aircraft that encroaches on the safe flying distance of a legitimate aircraft (500 feet vertical separation 15 NM in route horizontal separation and 5 NM in route horizontal separation).

SB-7. ACES Levels of Difficulty

The game will have two levels of difficulty. The first level (also known as the “easy” level) will inject ghost tracks randomly. The rate of injects will be minimum and will evenly spread throughout the ATC display/console.

The second level of difficulty (also known as the “hard” level) will inject ghost tracks at specific locations to intentionally disrupt the flight patterns of airborne helicopters and confuse the player. As the level of difficulty increases, the more elusive the cyber-attack is: ghost tracks will behave closer to a normal contact. The operational tempo of all air operations will increase as ACES’ level of difficulty increase, requiring the player to react sooner and make tougher decisions.

Inclement weather should be consider to make the game more difficult, as well as, having some aircrafts that would have actual mishaps, helicopter problems that might give the player the impression that it could be a cyber attack.

SB-8. Capturing Lessons Learned / Trend analysis

The ACES game shall include a means to capture lessons learned and assess mission/operational effectiveness trend analysis. This may not occur in the first prototype versions of ACES but it is crucial it does eventually to facilitate building and evaluating future CONOPS and TTPs.

First, ACES shall automatically save certain data at a fix rate of time throughout the entire duration of a game. This should be a default setting and the user (and the ACES systems administrator, to a greater extent,) should be allowed to tailor these variables as deemed necessary.

Second, attempts by the player (or even ACES itself through a scheme of automatic triggers) to take snapshots of the game while significant events and/or situations occur, might be an easy tool to implement. Memory capacity permitting, the option of recording parts of or even the entire game should also be considered.

Finally, the parameters, capabilities, and metrics depicted in table 1 would be a good source of the data to be gathered and linked to what is being shown on the ACES screen at that particular time. This data could, in turn, be displayed via charts and tables for ease of interpretation and understanding.

SB-9. ACES Graphical User Interface

The ACES Graphical User Interface (GUI) will be responsible for providing a means for users to interact with the serious game. In essence, it is a major factor in determining the success of ACES. Every aspect of the game will need a GUI in order to progress or influence the gameplay. The SGI team, along with our sponsors at the C4I Center, is the major stakeholder of this subsystem.

The user will interact with ACES to create, manage, import, export, and delete an account in a user friendly manner. Similarly, the user will interact with ACES through its GUI to pause and resume a game, as well as, to export and import any relevant gathered data from a player (e.g. best scores, historical average, trends and games played).

The system shall utilize traditional controls and widgets (e.g. windows, buttons, drop-down lists/menus) and interaction elements (i.e. cursor and pointer) to allow the user to interact with ACES games elements.

Equally relevant, the ACES GUI will need to allow the user to customize the gameplay parameters to their liking and, as a side note, ACES will need to provide tutorials on how to accomplish all of the abovementioned evolutions.

Throughout a game and in an inconspicuous way, ACES will need to display how is the game progressing (e.g. current scores, milestones achieved, threats captured, and threats missed) and shall offer easy ways to access quick reference guides on how to detect and deal with cyber-threats, as well as, how to play the game. Pausing and resuming the game should be achieved in a one-click / one-button mode.

The system shall utilize quick and easy interaction techniques to resemble real-time Air Traffic Management (ATM) evolutions. The system shall utilize the mouse and one-key strokes to allow user interact with ACES games elements in an elapsed time comparable to actual ATM voice and ATC console commands.

Finally, ACES shall offer multiple user views (e.g. Air Traffic Controller console view, airport tower view) to allow users to interact with ACES games elements in a visual manner comparable to actual Air Tower evolutions.

Appendix D: 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.euhttp://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

Cisco 2014 Annual Security Report

U.S. National Security Alliance, http://staysafeonline.org/

U.S. Multi-State Sharing and Analysis Center, http://msisac.cisecurity.org/

BRAZIL. ICA 100-12: Regras do Ar e Servi¸cos de Tr´afego A´ereo. Rio de Janeiro, Brazil, April 2009.

U.S. Entertainment Software Association, http://www.theesa.com/

U.S. Entertainment Software Rating Board, http://www.esrb.org/index-js.jsp