Developing a Complex Simulation Environment for Evaluating Cyber Attacks

Alexandre B. Barreto, Michael Hieb
C4I Center at George Mason University
Fairfax, VA
adebarro@c4i.gmu.edu, mhieb@c4i.gmu.edu

Edgar Yano
Instituto Tecnológico de Aeronáutica
São José dos Campos, SP
yano@ita.br

ABSTRACT

The management of oil exploration is among the most important strategic tasks that a nation has. In Brazil, the Campos Basin is a petroleum rich area compassing oceanic fields that accounts for 80% of Brazil's oil production. Because the Campos Basin is offshore, there is a high volume of helicopter traffic in the area. Currently, the Department of Airspace Control, that manages the Brazilian Air Traffic System, is developing a plan to improve Air Traffic Control Operations in this area using ADS-B technology (Automatic Dependent Surveillance-Broadcast). ADS-B will be used in a restricted oceanic airspace to supplement radar coverage to provide better service. As ADS-B technology is new and has vulnerabilities (unencrypted messages in a broadcast transmission mode), understanding the impact of a cyber-attack on the safety and security of Air Traffic Control Operations is a major challenge. This paper provides a case study in the evaluation and assessment of cyber-attacks to critical infrastructure using Simulation Tools. An analysis of the Simulation Environment used and its suitability for its purpose will be presented as a key finding. This environment consists of: 1) a cyber-attack generator; 2) an entity-level simulation to provide the dynamic behaviors of entities (helicopters and ATS infrastructure); 3) a network simulation that will include modeling ADS-B; and 4) a 3D visualization tool. The HLA protocol will be used to integrate selected components of the testbed. To provide information about the impact to the Campos Basin Air Traffic System, an external tool will be used to export the information to a Log System, for analysis by a cyber-assessment tool. This testbed will be used for developing an impact assessment framework that is applicable to a wide range of military and civilian missions.

ABOUT THE AUTHORS

Alexandre B. Barreto is a Brazilian Air Force (BAF) Major and a PhD Candidate in Computer Engineering at the Instituto Tecnológico de Aeronáutica (ITA) in Brazil. He recently worked in Brazil's Department of Airspace Control, where he was responsible for managing Information Technology infrastructure in the Amazon Region and developing simulator specifications for training air traffic controllers. Maj. Barreto is currently a Research Associate at the C4I Center at George Mason University in Fairfax, Virginia, where is using the C2 Collaborative Research Testbed for his PhD Research.

Michael Hieb is a Research Associate Professor at George Mason University's Center for Excellence in Command, Control, Communications, Computers and Intelligence (C4I Center) and a Technical Director for the Army's Simulation to C4I Overarching IPT (SIMCI OIPT). Dr. Hieb's research has concentrated on formalizing Command Intent for C2 Systems and Simulations. This has involved starting NATO and IEEE working groups and has spanned the fields of Computer Science, Networking, Semantics, and Computational Linguistics. Dr. Hieb has over 100 Publications and has presented his research on Command Intent to many International C2 and M&S Forums, as well as tutorials at I/ITSEC and SISO.

Edgar Toshiro Yano is an Associate Professor at Instituto Tecnológico de Aeronáutica (ITA) in Brazil. Dr. Yano has coordinated several cyber-security related projects for the Brazilian government and private organizations. Currently, he conducts research projects in Cyber-Security Situational Awareness, Security Governance and Resilience of Systems. He received his PhD in Computer Engineering from ITA in 1998, a MS in System Analysis from INPE (Institute of Space Research in Brazil) and a BS in Mechanical Engineering from ITA.

Developing a Complex Simulation Environment for Evaluating Cyber Attacks

Alexandre B. Barreto, Michael Hieb
C4I Center at George Mason University
Fairfax, VA
adebarro@c4i.gmu.edu, mhieb@c4i.gmu.edu

Edgar Yano
Instituto Tecnológico de Aeronáutica
São José dos Campos, SP
yano@ita.br

INTRODUCTION

With the evolution of computing systems, many critical infrastructures (Command & Control, Air Traffic Management, Power Plants, Weapon Systems, etc.) use advance automation, making modern society, technologically dependent (Evans & Wurster, 2000). This dependence makes Cyberspace a new way to conduct wars, as in ground, air or sea combat. To protect Cyberspace during a war, it is necessary to identify the main events in space and time, understand how Cyber Threats could produce damage to critical infrastructure that is used for operations, and predict possible Courses of Action (Endsley, 1987) (Boyd, 1995).

Another important idea is mission assurance – the process of specifying and maintaining a reasonable degree of confidence in mission success (Musman, 2011b).

These Mission and Cyber Tasks in the real world are very difficult, because usually they are performed by several organizations, which exchange information and interact in different ways in their own timeframes. In the worst case, when an attack happens, a manager doesn't have time to remediate the problem. Because the recovery time is longer than task time, it is important to protect the main assets (including the critical infrastructure) and minimize the impact to operations, while assuring mission completion.

Due to the complexity of these Mission and Cyber Tasks, an IT Manager who supports critical infrastructures needs to have an environment which can obtain all relevant data pertaining to the network and translate it to a readable format so that the support team can understand the real impact of Cyber Threats in order to accomplish their mission. However, the existing tools and methodologies cannot answer these questions, and are not clear enough on how to apply a complex Cyber Threat assessment to real scenarios.

These types of studies will allow a continuous understanding of which mission assets are most important and which particular infrastructure components are required to avoid mission failure.

To reproduce these behaviors in a real environment can be very complex, expensive, not repeatable, dangerous or impossible. The approach adopted was to build a Simulation Testbed representing this environment. This approach has many advantages familiar to those who use such models, including the reproduction of real behaviors without unnecessary details and the ability to run various permutations of a scenario.

The scenario chosen was air traffic control in Campos Basin. It's the biggest oil field in Brazil, located more than 60 nautical miles from the continent with continual offshore traffic between the airports and the platforms. Because the Campos Airspace is homogeneous and has many low altitude flights, Brazil Air Traffic Department plans to replace the old radio technology with a new one, named ADS-B (Automatic Dependent Surveillance-Broadcast).

Like any new technology, ADS-B has the potential of serious security problems caused by its main feature (broadcast and decrypted transmissions). A cyber-attack can cause catastrophic accidents (including fatalities), such as stopping flow of flights in the Campos Basin, resulting in the decrease of Brazilian oil production.

This paper is organized as follows: **Section 2 – Related Work** presents the related work, showing other approaches and how they relate to the framework developed in this paper. In **Section 3 – Campos Basin Scenario**, the Campos Basin scenario is presented. **Section 4 – Simulation Testbed** describes the Impact Assessment approach. In **Section 5 – Discussion** the approach is used to analyze the Campos Basin scenario. Finally, **Section 6 – Concluding Remarks** presents some final considerations and issues using this approach for future researches.

RELATED WORK

Cyber Impact Assessment

The understanding of how cyber-attacks impacts physical environments is a difficult problem and many researchers are trying to solve this question. The main approach is to detect intrusions and system attack paths using a set of distributed sensors in the network. The main technique is to use a Specialist or Signature-based system (Denning, 1987) (Bass, 1999).

To provide situation awareness (SA), it is not enough to identify attacks, but also a need to understand what the attack impact is within the environment. This question is partially addressed by (Bass, 2000). However, only after the attack-tree approach began to be used (Schneier, 1999) could effects be measured. Multiple approaches used the attack identification premise to provide SA (Amman; Wijesekera; Kaushik, 2002), (Ingols; Lippmann; Piwowarski, 2006), (Jajodia; Noel; O'Berry, 2005).

However, these techniques usually fail in the same way. When an attack is new (zero-day attack), it's not possible to have an unknown signature available or its attack-tree known, making hard to identify the attack pattern while it occurs. This limitation requires a new approach to be adopted. This paper is based on identifying attacks, highlighting significant events and then understanding the importance of them in a system (Saydjari, 2004). To understand the importance of events, a person must understand how a mission is planned and implemented.

Under this auspices, frameworks were developed, such as: Topological Analysis of Network Attack Vulnerability (TVA) (Jajodia; Noel; O'Berry, 2005) (Jajodia; Noel, 2010) and Mission-Oriented Risk and Design Analysis - MORDA's (Evans et al., 2004). The first framework (TVA) is dependent on knowing the attack path knowledge while the second framework (MORDA) referenced was a non-real time application for security planning.

A practical methodology was developed called Cyber Mission Impact Assessment (CMIA) (Musman et al., 2011a; Musman et al., 2011b) and extended by (Jacobson, 2011). The CMIA concept models the mission using a Business Process Model notation (BPMN) and maps IT components responsible for parts of the Mission. Later in the process, CMIA defines security attributes to each device. This simulates the process and evaluates the impact using taxonomy of effects (degradation, interruption, modification, fabrication, interception and unauthorized use). Nevertheless, CMIA use does have its challenges with understanding the creation of the effects, which sometimes make it very difficult to produce the same results.

Simulation to Cyber Impact Assessment in a Physical Environment

As indicated earlier, using real infrastructure for assessing cyber-attacks is impractical. This has led researchers to look at how to use simulation to test security aspects in a network and evaluate the vulnerabilities of a system. However the models developed usually are simplistic (Cohen, 1999) or have the same limitation of the cyber impact assessment methodologies discussed above (Amoroso, 1999).

Other approaches have many details along with a strong focus on the cyber environment (Chi, at al., 2001) making it hard to define the effects in physical scenarios. Some models focus on infrastructure dependence (Pederson, at al., 2006), but not the network in detail.

An alternative approach was made by Musman, as cited above, but lacked the explanation of how to develop the environment.

CAMPOS BASIN SCENARIO

The scenario developed is related to Air Traffic Control operations in the Campos Basin. Campos Basin is a petroleum rich area in Rio de Janeiro state, and is responsible for 80% of Brazilian's petroleum production. Oil prospection and exploration is made in oceanic fields. The operation includes heavy helicopter traffic between continent and oceanic fields during daytime, with an average of 50 minutes per flight.

To support this operation, Brazil has a center in Macaé (Rio de Janeiro) which manages approach procedures. This center has a radar station that supports the surveillance service within the terminal.

As most oil platforms are located more than 60NM from Macaé and the helicopter flights are carried out at low altitude, the Air Traffic Service (ATS) provided on most of the oceanic area is based on non-radar procedures, which significantly reduces efficiency of air operations.

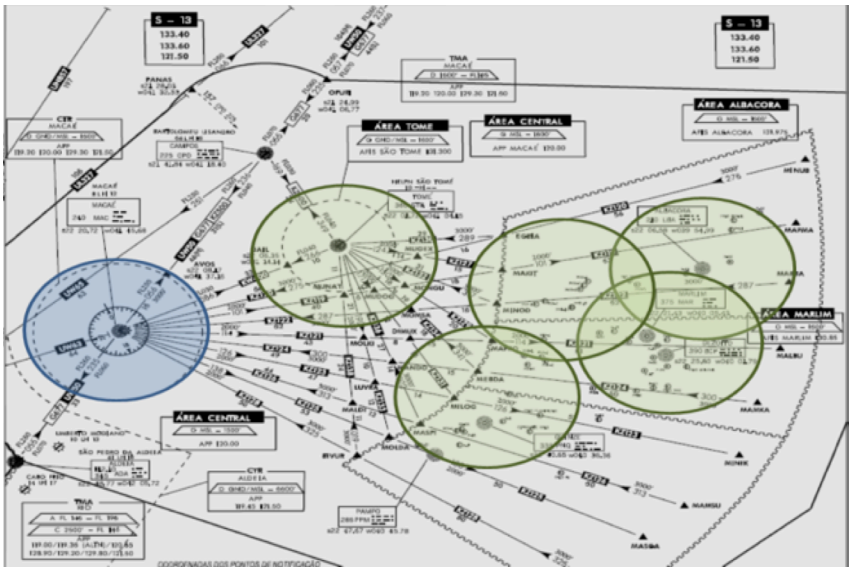

Figure 1. Campos Basin Coverage with radar and ADS-B radios (Brazilian Department of Airspace Control, 2010)

The above factors clearly indicate the need for restructuring the air navigation services in the Campos Basin. This effort must leverage new technologies to provide better support for navigation and surveillance of low-altitude flights in the oceanic area.

The Brazilian Government solution under study is the Automatic Dependent Surveillance-Broadcast (ADS-B) technology application. The strategy is to supplement radar coverage (blue circle in Figure 1) in the oceanic air space, as seen in Figure 1, where the green circles are the future coverage.

ADS-B is a new technology that is redefining the paradigm of COMMUNICATIONS - NAVIGATION - SURVEILLANCE in Air Traffic Management. Its main advantage is the cost when compared with conventional radar. It allows pilots and air traffic controllers to detect and control aircraft with more precision, and over a far larger percentage of the earth's surface, than has ever been possible before.

Its operation consists a radio that receives aircraft position information generated through the satellite linked GNSS GPS via a data link. This radio works as a relay agent, sending positional information to a central node. This data is integrated on an ADS-B Server, which is used by an air traffic controller to manage the air space (see Figure 2).

There are two different ADS-B configurations. In the first, an aircraft is able to send its own track information (ADS-B OUT). In the second mode, an aircraft is able to receive tracks by other aircraft (ADS-B IN) and by Air Traffic Service (ATS) (weather information, and etc.). In the first phase, Brazil is planning adopting the ADS-B IN Mode.

To implement this new service, Campos Basin needs a complex and optimized telecommunication infrastructure. In Figure 3 this infrastructure is shown in summary form. To connect oceanic platforms and Macaé, a submarine optical cable backbone (blue lines) is used. It provides a high speed connection 100Mbps plus connection. But on the same platforms, low-speed microwaves links (red dashed lines) also exist within the infrastructure.

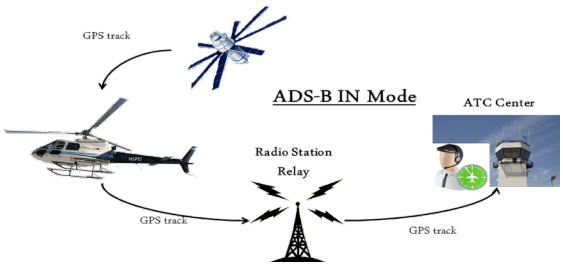

Figure 2. ADS-B IN Mode

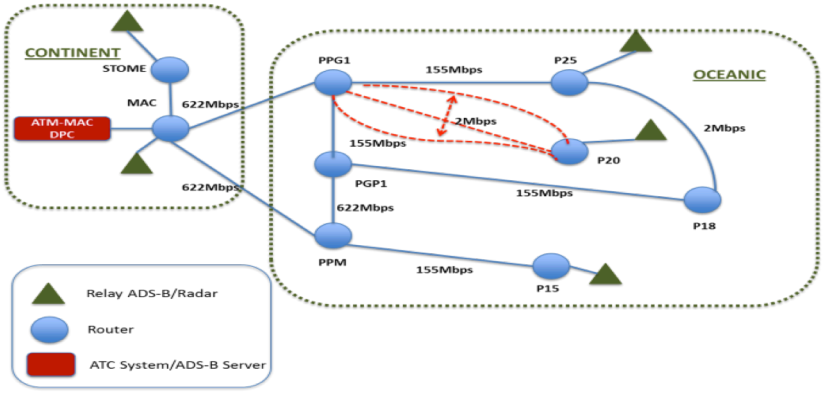

Figure 3. Campos Basin ADS-B Infrastructure

Since ADS-B is a new technology, many threats may exist and extensive analysis has not been performed. The main threat in ADS-B protocol is its transmission mode, which is based in broadcast and decrypted radio messages. It is possible that the radio packet data could be captured or inserted in the network.

Some studies are available on the main vulnerabilities within ADS-B network. In general they identify two vulnerabilities: data links and network backbone. In (McCallie at al., 2010) an attack taxonomy is described, where each attack was classified using three attributes: target, method and difficult to implement. This classification is presented in table 1.

Table 1. ADS-B Taxonomy - derived from (McCallie at al., 2010)

Attack Name	Target	Method	Difficulty
Aircraft Reconnaissance	Aircraft	Intercept ADS-B OUT signals	Low
Flood Denial	Ground Station	Create a jamming signal	Low
	Aircraft		Medium
Target Ghost Inject	Ground Station	Inject messages	Medium-High
	Aircraft		
Ground Station Multiple Ghost Inject	Ground Station	Inject multiple messages	Medium-High

There are other kinds of attacks that (McCallie at al., 2010) did not address. One of these attacks is track delay. In this attack, the target is a ground station or ATS system. This consists of the attacker sending a lot of packets in variable time-intervals.

This attack increases the network traffic and causes jitter problems. It's a major problem to ATS applications because of their extreme dependence on time accuracy. It is relatively easy to simulate this attack, because the existing Flood Denial technique will produce the same results.

SIMULATION TESTBED

In 2010, during the XII Symposium of Operational Applications in Defense Areas in Brazil, a partnership was established between George Mason University (GMU) and Aeronautics Institute of Technology – Brazil (ITA), which aimed to create an environment that supports C2 research by providing a Modeling and Simulation environment for C2 Planning, Security Issues and Cyber Warfare.

This environment, the C2 Collaborative Research Testbed, uses several COTS (commercial off-the-shelf) tools along with Open Standards that provide a rapid prototyping and modeling environment for C2 missions.

An overview of the C2 ITA/GMU Testbed is presented in Figure 4, where you can see the two COTS Simulation tools used. The first is MÄK VR-Forces (MAK, 2012), which is a powerful and flexible simulation environment for scenario generation. It has all the necessary features for use as a threat generator, behavior model testbed, or Computer Generated Forces (CGF) application.

The second is EXata Cyber (Scalable, 2012), that is a cyber-simulation platform which accurately emulates or simulates how complex communications will behave under battlefield conditions.

A main component in the testbed is an integrated bus, which is middleware responsible for integrating

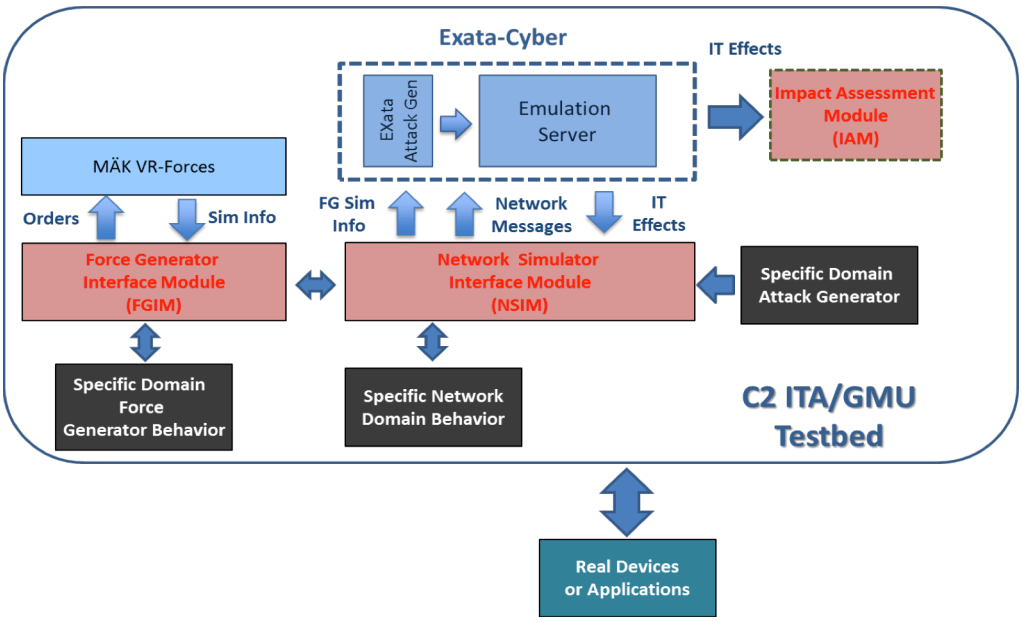

Figure 4. C2 ITA/GMU Testbed

physical environment behavior, provided by VR-Forces with IT behavior provided by Cyber EXata and real applications and devices.

The integrated bus is formed by three modules. The first is a Force Generator Interface Module (FGIM) that is responsible to obtain information about physical entities (forces) by VR-Forces and send this data using a network to Network Simulator Module (NSIM). The second function, which FGIM performs, is to send orders to VR-Forces for implementation in the physical simulation environment. These orders use a physical domain logic constraint, which are programmed by developers using a FGIM Testbed API.

The second module of the Integrating C2 Bus is the Network Simulator Interface (NSIM). This module implements an interface to connect real devices and specific network behavior in testbed. NSIM receives all force information passed through FGIM and inserts it in the environment. NSIM receives all physical entity information by FGIM and inserts it in the testbed. For example, when an aircraft generated by VR-Forces sends a message to another aircraft, it's the NSIM that transports this message to the emulator server (Cyber EXata) and, after the network effect is emulated, sends it to FGIM with the effect to be reinserted into the force simulator.

This same task happens when a real device sends a message or order to another entity (real or virtual). It's the NSIM that is responsible to insert this message in the emulator and (after the calculated effects) to send it to the correct recipient. As FGIM, NSIM has its own API that can be used by the developers in developing network domain-logic constraints.

To insert cyber-attacks in the testbed, there are two approaches. The first is to use the EXata library, which has many kinds of general attacks and attacker behaviors (Deny of Service (DoS), virus, jammer, etc.).

The second approach is to develop an Attack Generator outside and integrate it using the NSIM API.

The last module is Impact Assessment Module (IAM). This module receives messages from emulator entities through the existing interface. The IAM module has the responsibility to calculate the impact over physical mission in real time. This module is still under development.

The methodology to assess the impact of cyber-attacks on a physical environment consists of six steps:

1) Create mission physical environment using an entity level simulation (VR-Forces).
2) Create IT infrastructure environment using a network simulation (Cyber EXata).

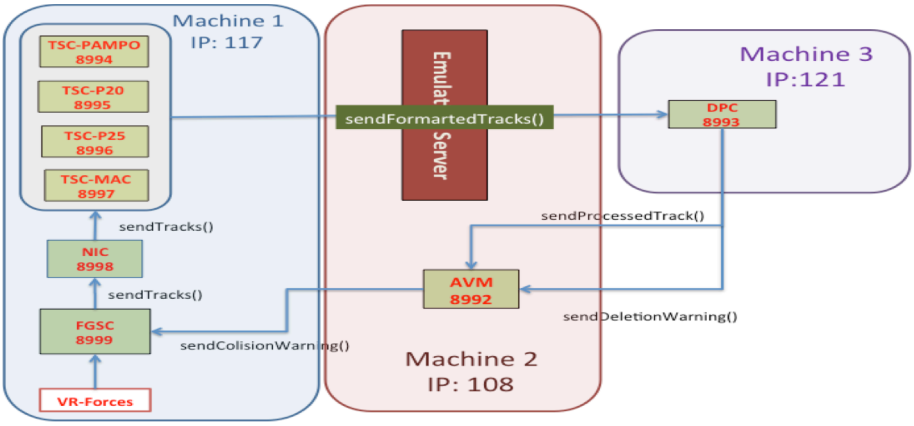

Figure 5. Campos Basin ADS-B Testbed Environment

3) Connect the two simulations using the C2 Collaborative Testbed Components (FGIM and NSIM Module).
4) Connect real applications, radios, and sensors in testbed using APIs (the NSIM Module).
5) Develop specific domain attacks using an external attack generator (or use pre-existent in Cyber EXata).
6) Collect information from the environment in real time, calculate the impact and display in an external dashboard.

DISCUSSION

The Campos Basin Scenario was used to evaluate if the testbed can reproduce the critical infrastructure impact of a cyber-attack over one mission.

To implement the Air Traffic Control Protocols a simple ADS-B relay (TSC) and an ADS-B Server Processor (DPC) were implemented using the NSIM API.

To allow the air traffic controllers to see and perceive delay tracks, ghost and suppressions attacks, a visualization interface (AVM) was built. This interface receives tracks sent by ADS-B Server processor through the EXata emulator server. The complete environment can be seen in Figure 5.

Voice pattern traffic (VHF and HF) was generated and introduced in the environment. This produces a more accurate model, as in real world conditions. Along with the tracks messages, the network now has the same throughput caused by the voice traffic sent by pilots to inform to air traffic controller of their conditions.

Figure 6. Tactical Map of Campos Basin Study Case

Three DoS attacks were develop during the simulation. The goal of these attacks was to generate delay tracks, jitter variances and crash in the ADS-B Server Processor. The delay track and jitter variance is a significant problem to controllers, because if a track doesn't advance at a constant rate, jumps happen in the visualization.

To provide mission domain warnings that can be used in an impact assessment module, two measures were developed. The first is collision warning – when two aircraft go to a vertical or horizontal distance below a minimum defined by International Civil Aviation Organization (ICAO) an alert is generated.

The second measure is the time it takes to update Aircraft tracks. This consists of the time between two tracks updating. If a track does not update often enough, it can mean a ghost track inject attack, an aeronautical accident or that the aircraft has landed.

To provide a realistic environment, 32 helicopters were created and each one of these receives a different plan – the plan consists of takeoff from an airfield, going to three or two different platforms and coming back to the continent, where it lands at the main airport. An overview can be seen in Figure 6.

In Figure 7, a 3D visualization of a landing operation is shown. To perform this operation all air traffic patterns need to be developed, inclusive of the new procedures, such RNAV/GNSS.

Figure 7. 3D View of Landing Operation

As commented previously, a visualization tool was developed to show what an operator would perceive. This interface is showed in Figure 8.

This tool represents aircraft through blue crosses, platforms through red crosses and waypoints through red circles.

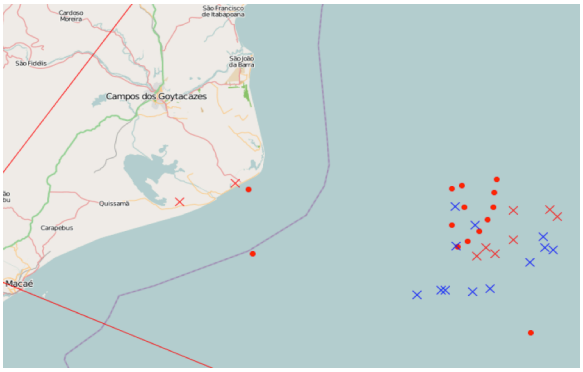

Figure 8. Air Traffic Visualization

Currently the impact evaluation module needs to be developed, however the simulation data has already been captured by the EXata interface through a COTS packet analyzer. This feature is important because during an attack, every change in the emulation environment can be perceived and retrieved through the use of an external tool. This allows the evaluation and analysis of multiple attack impacts.

CONCLUDING REMARKS

The C2 Collaborative Research Testbed is working to connect two important dimensions the Physical and Networked. This allows analysis of the complex Command and Control operations (Military, Civil, and other), where an event that happens in one dimension, is reflected in the other. It enables an understanding of the critical events that affect your environment and have mission impact. This capability will also be used to develop more accurately important defense/offensive plans and scenarios.

This research is built using COTS tools and open standards to validate a Simulation-Based Cyber-Attack Assessment Methodology. There are many other aspects of the Methodology to develop which would make it more usable by practitioners. Some of these developments could enhance the initialization of the Mission and Network data, create a better Representation of the Mission, and give the ability to validate the results of a network assessment.

ACKNOWLEDGEMENTS

The authors would like to thank the VT MÄK and Scalable Network Technologies to provide all tools and support to develop the Testbed. I thank too LatinMedia SA to support Testbed in Brazil site. They also thank the anonymous reviewers for their useful comments.

REFERENCES

Amoroso, E. (1999). *Intrusion Detection.*AT&T Laboratory, Intrusion Net Books.

Ammann, P., Wijesekera, D., & Kaushik, S. (2002). *Scalable, graph-based network vulnerability analysis.* 9th ACMConference on Computer and Communications Security.

Bass, T. (1999). *Multisensor data fusion for next generation distributed intrusion detection systems.* IRIS National Symposion. [S.l.: s.n.].

Bass, T. (2000). *Intrusion detection system & multisensor data fusion: Creating cyberspace situation awareness.* Communication of the ACM, v. 43.

Boyd, J. (1987). *A discourse on winning and losing*. Maxwell Air Force Base, AL: Air University Library Document No. M-U 43947 (Briefing slides).

Brazilian Department of Airspace Control. (2010). *Use of ADS-B at the Macaé – Cuenca De Campos TMA.* First Meeting of the Communications, Navigation, and Surveillance / Air Traffic Management Subgroup (CNS/ATM/SG/1) (Lima, Peru, 15-19 March 2010).

Chi, S., Park, J. S., Jung, K., & Lee, J. (2001). *Network Security Modeling and Cyber Attack Simulation Methodology.* ACISP 2001, LNCS 2119, pp. 320-333. Springer-Verlag Berlin Heidelberg.

Cohen, F. (1999).*Simulating Cyber Attacks, Defenses, and Consequences*. IEEE Symposium on Security and Privacy Special 20th Anniversary Program, Berkeley, CA.

Denning, D. E. (1987). *An intrusion-detection model.* IEEE Transactions on Software Engineering, v. 13, p. 222-232.

Endsley, M (1987). *The application of human factors to the development of expert system for advanced cockpits.* Human Factors Society. Annual Meeting of Human Factors and Ergonomics Society, p. 1388-1392.

Evans, P., & Wurster, T. S. (2000). Blow to bits: how the new economics of information transform strategy. *Harvard Business School Press*.

Evans, S., Heinbuch, D., Kyle, E., Piorkowski, J., & Wallner, J. (2004). *Risk-based systems security engineering: stopping attacks with intention.* IEEE Security and Privacy, v. 2, p. 59-62.

Ingols, K., Lippmann, R., & Piwowarski., K. (2006). *Practical attack graph generation for network defense.* 22nd Annual Computer Security Applications Conference (ACSAC).

Jacobson, G. (2011). *Mission Cyber Security Situation Assessment using Impact Dependency Graphs.* Proceedings of the 14th International Conference on Information Fusion. Ilinois, EUA.

Jajodia, S., & Noel, S. (2010). *Topological vulnerability analysis.* Cyber Situation Awareness - Issues and Research.

Jajodia, S., Noel, S., & O'Berry, B. (2005). *Topological analysis of network attack vulnerability.* Managing Cyber Threats, v. 5, p. 247-266.

MÄK VR-Forces (2012). Retrieved from http://www.mak.com. Accessed in June, 16 2012.

McCallie, D., Butts, J., & Mills, R. (2010). *Security analysis of the ADS-B implementation in the next generation air transportation system.* International Journal of Critical Infrastructure Protection N4 (78-87).

Musman, S., Tanner, M., Temin, A., Elsaesser, E., & Loren, L. (2011). *Computing the impact of cyber attacks on complex missions.* 2011 IEEE International Systems Conference (SysCon). [S.l.: s.n.], p. 46-51.

Musman, S., Tanner, M., Temin, A., Elsaesser, E., & Loren, L. (2011). *A systems engineering approach for crown jewels estimation and mission assurance decision making.* IEEE Symposium on Computational Intelligence in Cyber Security (CICS).

Pederson, P., Dudenhoefferb, D., Hartleyb, S., & Permannb, M. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research.* Idaho National Laboratory. Idaho Falls, Idaho 83415.

Saydjari, O. S. (2004). *Cyber defense: Art to science.* Magazine Communications of the ACM - Homeland Security, v. 47, n. 3.

Scalable Network (2012). Retrieved from http://www.scalable-networks.com. Accessed in June, 16 2012.

Schneier, B. (1999). *Attack trees: Modeling security threats*. Dr. Dobb's journal.