19th ICCRTS – C2 Agility: Lessons Learned from Research and Operations

"Cyber-Argus: Modeling C2 Impacts of Cyber Attacks"

Topic 6: Cyberspace, Communications, and Information Networks

Topic 1: Concepts, Theory, and Policy

Topic 5: Modelling and Simulation

Dr. Alexandre de Barros Barreto
Instituto de Controle do Espaço Aéreo
São José dos Campos, SP
Brazil
+55-12-3945-9004
barretoabb@icea.gov.br
(Point of Contact)

Dr. Paulo Costa, Dr. Michael Hieb
Center of Excellence for C4I
George Mason University
4400 University Drive
Fairfax, VA 22030
USA
+001-703-993-3990
pcosta@c4i.gmu.edu
mhieb@c4i.gmu.edu

Cyber-ARGUS: Modeling C2 Impacts of Cyber Attacks

Abstract

Cyber security is often only seen as protecting networks. However, during critical operations, there is a desire to detect, assess and respond to cyber threats. Given the unknown vulnerabilities of large, complex Command and Control (C2) systems, organizations will protect the most critical assets essential for mission success. Cyber-ARGUS is a methodology that provides a mapping between the cyber and the operational domains, substantially improving the monitoring of information infrastructure (networks) supporting missions by correlating their status to mission goals. This enables a proactive, context-based response to ensure that cyber attacks will not affect ongoing operations.

Cyber-ARGUS relies upon a unique approach of modeling the network and the mission separately. After modeling the mission, the mission's tasks are mapped into services required for the mission, and these services are allocated to network nodes to form a Mission Network Graph. A vulnerability assessment and an enemy behavior analysis are conducted to determine which vulnerabilities the network is exposed to. This information is then used to adjust the node values in the Mission Network Graph, represented as a Bayesian Network, to calculate the impact assessment for each node. Finally, a simulation is run using both an Entity Level simulation and a Network emulator to determine the C2 impact of a cyber attack on the Mission.

We illustrate this methodology with a detailed use case. In Brazil, the Campos Basin is a petroleum rich area 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. A new technology – ADS-B (Automatic Dependent Surveillance – Broadcast) will supplement radar coverage in the restricted oceanic airspace supporting the oil platforms. Results from this use case are assessed and extrapolated to determine if this methodology can be used to improve the agility of operations.

Keywords: Cyber, Simulation, Command and Control, Impact Assessment, Networks

I. INTRODUCTION

In their quest for better, safer, and lower-cost services, designers of modern critical infrastructure has relied upon Information Technology (IT) and made it a key aspect of their systems. This phenomenon, which can be observed in various domains, has made modern society technologically dependent [1] and transformed the cyber domain into a key element for strategic decision planning.

This dependence has forced most governments to investigate how cyberspace would complement a conventional campaign in traditional warfare domains (land, sea, and air) [2-3]. However, using cyberspace in a military campaign requires managing and understanding its effects in these other domains. In other words, to judge whether a cyber task can achieve a particular goal or not, one must be able to assess how actions performed in cyberspace affect behaviours in the traditional domains (land, sea, and air).

Understanding cyber effects in physical domains is also an increasing concern from the viewpoint of International Humanitarian Law (IHL) [4]. Within this context, the Commander is responsible for managing his actions, aiming to optimize its desired effects while minimizing the risk of collateral damage[1].

From a defense perspective, it is necessary to determine the key events in space and time, to understand how cyber threats could cause damage to mission critical infrastructures, and to predict possible actions in cyberspace by the enemy [5-6].

A Commander’s understanding the about the effect of cyber attacks on an operation requires a correlated cyber and operational integrated visualization. However the technology to develop this is not trivial. A Commander must be able to access all relevant data pertaining to the network and to view this data in a way that exposes the real impact of cyber attacks on the network, network, as well as its significance to the overall mission. These challenges led us to research new techniques to provide cyber understanding [7].

This paper presents a new methodology for handling cyber impact assessment in a mission context - *Cyber-ARGUS* [8-10]. Cyber-ARGUS is a methodology that provides a mapping between the cyber and the operational domains, substantially improving the monitoring of information infrastructures (networks) supporting missions by correlating their status to

[1] There are other implications from operating in the cyber domain within an IHL context. One example is the use of civilian targets. However, this is outside the focus of this paper.

mission goals. This enables a proactive, context-based response to ensure that cyber attacks will not affect ongoing operations. The goal of this paper is present how a Commander can use Cyber-ARGUS to increase his cyber situation awareness.

The threat of cyber attacks is pervasive and the ability to predict the impact of an attack is a very desirable capability. This capability, as we describe in this paper, could contribute to agility in providing flexibility in how to respond to a cyber attack – flexibility being one of the key components of agility as described in Alberts [11].

This work is described in much greater detail in [12]. Please refer to this PhD Thesis for clarification on, and a much expanded description of, this work. There is also an extended treatment in [12] of the Air Traffic Control use case described here along with additional analysis.

This work is organized as follows. Chapter 2 presents the key concepts needed to understand the proposed framework, as well as a summary of the most relevant approaches in the literature. Chapter 3 describes the framework for evaluating the impact of a cyber attack on an operation occurring in the physical domain. Chapter 4 presents a case study in the Air Traffic Control (ATC) domain and an analysis of results. Finally, Chapter 5 presents conclusions, highlighting the main contributions as well as issues to be addressed in future research.

II. LITERATURE REVIEW

Situation Awareness (SA), as defined by Endsley [5], is the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status after some other variable has changed, such as time, or a predetermined event. The process to obtain SA is Situation Assessment [13].

A relevant discussion about SA is the difference between situation and impact assessment. An important contribution is provided by Salerno [14], which defines situation awareness as an estimate of the current object states while impact assessment is related to the prediction of future states.

A good explanation of a process that creates SA is provided by Tadda and Salerno [15]. Their approach is based on Endsley's SA process, which has four main phases: *Perception, Comprehension, Projectio*n and *Resolution*. *Perception* provides information about the status, attributes, and dynamics of relevant elements within the environment. *Comprehension* consists of understanding the context of data retrieval, using previous knowledge about entities, groups, and events to define a set of possible situations. *Projection* defines the estimation of future states. Finally, *Resolution* tries to identify the best path to achieve a desired state change to the current situation.

The cyber domain has complicated the SA process described above, and there are significant differences from developing SA in a more conventional domain [16]. In the general sense, researchers have ascertained that cyber threats and attacks could affect missions in many different ways. Thus we see the need to integrate cyber SA with the SA in mission space. However, the question is: *"How can this integrated SA be developed?"*

The most common approach to develop cyber SA uses an *enemy viewpoint approach* [16]. In this approach, an Analyst attempts to predict how vulnerabilities can be exploited by the enemy, usually through a database of an enemy’s preferences and capabilities [17-18] or an attack graph [19-30].

The weakness of this approach is when the enemy behaviour is not predictable, because of the lack of evidence or ignorance about the enemy’s capacity. Further, representing an enemy’s knowledge is computational complex and poses implementation problems [21,26].

An alternative approach was proposed by Musman et al. [30-32] for handling cyber impact assessment. The Computing the Impact of Cyber Attacks on Complex Missions (CMIA) framework tries to evaluate the mission impact through understanding what is important to accomplish mission goals.

CMIA's approaches have changed the traditional way for evaluating cyber impacts. Its focus is on the effect, allowing for the evaluation of impact in zero day attacks, as the attack model is not required. Another contribution is the mapping between the cyber and the mission domains, enabling an Analyst to understand what cyber events will impact a kinetic mission. In the current paper, we call the CMIA's approach as *mission viewpoint approach*.

The main benefits of using this approach are that the impact measures depend only on understanding the effects and how they impact the mission. This is different from the enemy viewpoint approach, as even if the enemy behaviour is not known or detected, an impact can be measured. Hence, the mission viewpoint approach does not fail when the enemy's behaviour cannot be predicted.

Cyber-ARGUS follows the general mission viewpoint approach for impact assessment. As opposed to Musman et al. and Jajodia et al., the proposed methodology shows how to map mission and infrastructure concepts, providing a practical model to be used in a real scenario. Additionally, it defines an index to evaluate the cyber impact and it extends Kim and Kang's MCDM (Multi-Criteria Decision-Making) approach [33], adapting it to a mission viewpoint perspective.

III. CYBER-ARGUS FRAMEWORK

Cyber-ARGUS framework is designed to determine the impact of a cyber threat on a mission [8-10]. To measure the cyber impact, Cyber-ARGUS requires the mapping of concepts between the cyber and operational domain and a determination of which concepts are dependent on one another. To model these dependencies, an adaptation of Jakobson's Impact Dependence Graph [23] was used. Jakobson's Impact Model defines five kinds of dependencies: a) Intra-Mission; b) Service to Mission; c) Intra-Service; d) Asset to Service and e) Intra-Asset. These levels of dependencies are presented in Figure 1.

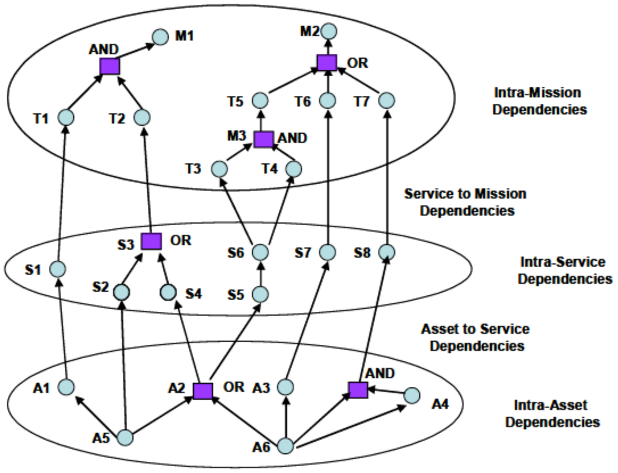
M1
AND
M2
OR
T1
T2
T5
T6
T7
M3
AND
T3
T4
Intra-Mission Dependencies
Service to Mission Dependencies
S3
OR
S1
S2
S4
S5
S6
S7
S8
Intra-Service Dependencies
Asset to Service Dependencies
A1
A2
OR
A3
AND
A4
A5
A6
Intra-Asset Dependencies

Figure 1 - Jakobson's Impact Model - from [23]

Using Jakobson's Impact Model to define a mission requires specifying tasks, services and assets. However, a clear definition of these concepts is required. Cyber-ARGUS uses the taxonomy of United States Department of Defense (DoD) Architectural Framework [34].

In our model, a *Mission* is composed of a task (or set of tasks), together with its associated purpose (that clearly indicates the action to be taken assigned to an individual or unit). A *Task* is performed by a performer and requires a set of resources. A *Performer* is any human entity, automated entity, or any aggregation of human and/or automated entities– that perform an activity and provides a capability. A *Service* is a mechanism that enables access to a set of one or more capabilities. In other words, availability of services defines which tasks can be performed. A *Cyber Node* is an element that hosts one or more services (abbreviated in this work to "node").

However, these elements do not define completely a mission, which requires a deeper level of detail. Additionally, Mission information usually comes from diverse sources, so Cyber-ARGUS ensures consistency of the integrated data representation by means of a mission ontology describing the relevant concepts (tasks, services, cyber nodes, etc.). Semantic technologies also facilitate code reuse, which allow us to avoid developing the mission ontology from scratch. Instead, Cyber-ARGUS leverages previous related work by D'Amico et al. [35] and Matheus et al. [36].

The Cyber-ARGUS' Concept Model is presented in Figure 2, which identifies the relevant concepts used to model the mission and the information required for impact assessment. However, two of the concepts require a more detailed explanation. The first is the *Vulnerability*. Any resource has a set of vulnerabilities. Using the US DoD definition, a vulnerability is the characteristic of a system that cause it to suffer a degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in a hostile environment [37].

The other concept is the *Service Level Agreement – SLA*. Tasks require that services are provided with a minimum level of quality. To define service levels, a mission's Analyst needs to clarify a set of conditions and states (as specified in a Service Level Agreement - SLA). As an example, Internet service providers will commonly include SLAs within the terms of their contracts with customers to define the level(s) of service being sold. In this case the SLA will typically have a technical definition in terms of mean time between failures (MTBF), Mean Time To Repair or Mean Time To Recovery (MTTR), data rates, throughput, jitter or similar measurable details.

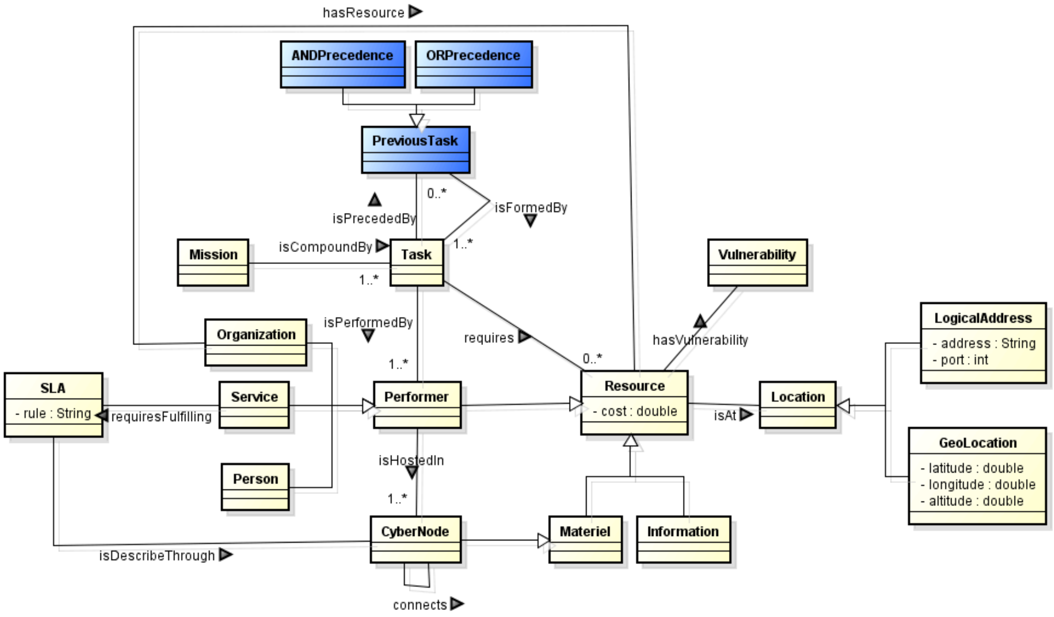

Figure 2 - Cyber-ARGUS' Concept Model

Within the Cyber-ARGUS concept model, the two domains are represented in an integrated and coherent view, so that Cyber-ARGUS [8-10] can measure the cyber impact on the mission. Cyber-ARGUS has four main phases: 1) *Mission Modeling*, 2) *Classification of Cyber and Mission Data*, 3) *Mission Impact Assessment,* and 4) *Hypothesis Definition*. Figure 3 depicts these phases.

During the first phase, *Mission Modeling*, an Analyst models a target mission, defining required tasks; services and associated nodes, as well as which vulnerabilities and possible attack-paths exist in the environment. This information is saved in a Semantic Knowledge Base (KB). Then, a set of data is collected from infrastructure through log servers (applications, network, security, etc.), during the *Classification of Cyber and Mission Data* phase. In the *Mission Impact Assessment* phase, using information from the previous phase to classify it and infers what is relevant to accomplish the mission and then builds an Impact Graph, which is used to calculate the cyber impact. The last phase, *Hypothesis Definition* allows the Analyst to test various actions (such as cyber attacks, or the response to them) to see what how the mission would be impacted – Cyber-ARGUS calculates the most plausible situations resulting from these actions.

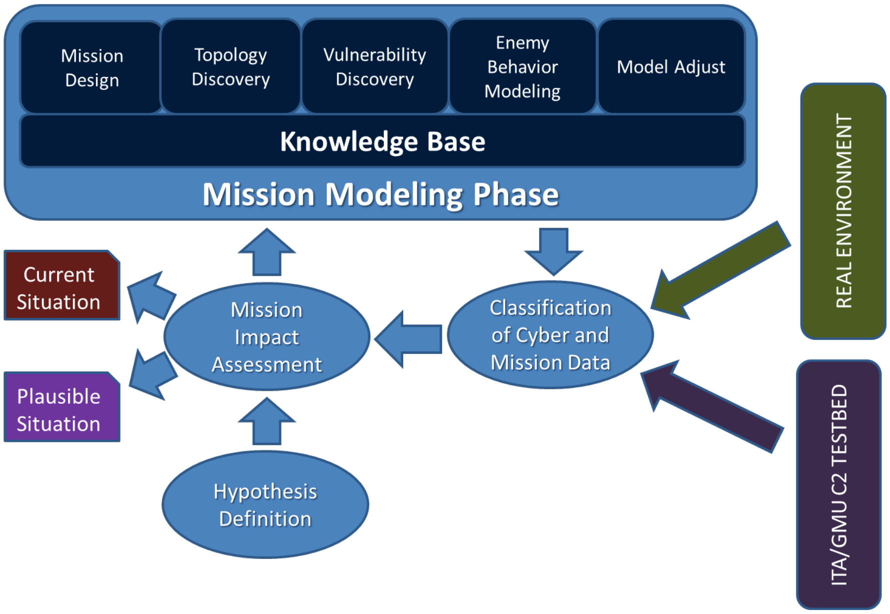

Figure 3 - Cyber-ARGUS Framework

3.1. Mission Modeling Phase

The DoD defines Mission Assurance as the process to protect or ensure the continued function and resilience of capabilities/assets critical to the execution of mission-essential functions [38]. A part of this process is Mission Modeling, as stated by Jabbour and Muccio [39]. The goal of the *Mission Modeling* phase is to describe critical tasks and their dependencies.

Within the Concept Model previous presented, a mission Analyst can design the mission using any process management modeling language. The process to retrieve this information is divided in five steps: 1) *Mission Design*; 2) *Topology Discovery*; 3) *Vulnerability Discovery*, 4) *Enemy Behaviour Modeling*; and 5) *Model Adjustment*. Each one of these steps is described below.

In the *Mission Design* step, an Analyst, using a process model language, captures the most relevant information of the mission within the Concept Model and stores it in a semantic Knowledge Base (KB). Relevant information includes tasks, relationships between tasks, resources required to develop the mission and, finally, the performer.

In the current research, we leveraged previous experience within our group and made the design decision of capturing these aspects using the Business Process Modeling Notation

(BPMN). However, any process modeling language with the ability to capture the information described above could have been used and, therefore, might be used with the framework in the future, as for example *Battle Language Management (BML)* [40-41].

After all tasks have been specified, and their dependencies are mapped, the second step is initiated – *Topology Discovery*. This step will discover where required services are hosted. To perform this task, Cyber-ARGUS queries a service repository and retrieves all information linking nodes to their hosted services, as well as the network topology depicting the required connectivity between nodes, saving the output in the KB.

Following the *Topology Discovery* step, the framework can proceed with the next step, *Vulnerability Discovery*. *Vulnerability Discovery* aims to map all vulnerabilities in the infrastructure and store them into the KB to be used in the *Mission Impact Assessment* phase. This is similar to the *Topology Discovery* step, where the framework, using a database - *National Vulnerability Database - NVD*[2], looks for node vulnerabilities that are part of the environment. After this activity, all vulnerabilities and their related impact factors (*Vulnerability Factor –* V_f) are collected, and Cyber-ARGUS stores this information into the KB. The classification is indexed by Cyber nodes, enabling an Analyst to perform specific queries relating nodes to vulnerabilities and vice-versa.

After the *Vulnerability Discovery* step is completed, an optional step can be performed – the *Enemy Behaviour Modeling* step, which will model known attack-paths using an attack graph. This task requires the existence of a database in which all known attack-paths are described and saved in an appropriate format. To reduce the amount of information that Cyber-ARGUS needs to use during the impact assessment phase, we have adopted the *Cauldron* approach developed at George Mason University - GMU [26]. The general idea of Cauldron is to eliminate implausible scenarios, through the analysis of firewalls and other entry-devices restriction rules and Access-Control-List (ACL). As cited above, Cyber-ARGUS uses the mission viewpoint approach [30-32] for cyber impact assessment so if enemy information does not exist, this step is simply not performed. The enemy information, if available, is used to adjust and increase the accuracy of model.

The last step is the *Model Adjustment*, when the Analyst complements the KB with additional information, which was not possible to do earlier - either because the modeling

[2] http://nvd.nist.gov/

language did not support this or because the Analyst decided to add this later. Cyber-ARGUS performs three adjustments in this step: a) it defines cyber attributes needed to be monitored by the framework, as well as the relative importance that each one of the attributes has compared to another; b) it adjusts the dependences between tasks-services, services-services, services-nodes and nodes-nodes dependencies in the KB; and c) it prioritizes tasks, services and nodes based on their importance in accomplishing the mission.

3.2. Classification of Cyber and Mission Data Phase

After the *Mission Modeling* phase, the Analyst has a comprehensive view of the mission and the factors that affect its success. That is, the Cyber-ARGUS model is ready to be used; it is now able to collect and correlate infrastructure information, to infer what is pertinent to the mission, and to provide relevant data in order to calculate the cyber impact.

To use this model, the mission Analyst needs to collect information from the relevant Cyber nodes. This will enable the Analyst to assess each node's current status, as well as to estimate, during the impact assessment phase, whether the node is able to perform the tasks it is expected to perform.

In addition to the node status information, Cyber-ARGUS must collect further data in order to calculate the cyber impact. An example is information about security, which includes attack events, system incidents, etc. This information can be collected from intrusion detection and prevention systems, firewall logs, anti-virus, and other security logs. One important source for this type of data is application and database logs, which can provide a view about how resources are used within the system (e.g., what users logged in, which resource types they used, etc.).

The data collection is one aspect of this phase. The other is correlating and inferring relevant information. To accomplish this, the mission Analyst needs to define a set of trigger events (situations), using a language such as the Semantic Web Rule Language (SWRL)[3]. SWRL extends a set of OWL[4] axioms to include Horn-like rules, which can be used in conjunction with the OWL knowledge base.

[3] http://www.w3.org/Submission/SWRL/.

[4] http://www.w3.org/TR/owl2-overview/.

3.3. Mission Impact Assessment Phase

The *Mission Impact Assessment* phase is defined by four sub-tasks, as can be seen in Figure 4. The first is to generate the impact graph, which is a dependence graph [42] that represents a mission, as well as the dependence (for the mission and IT domains) and the influence that each node has on the mission.

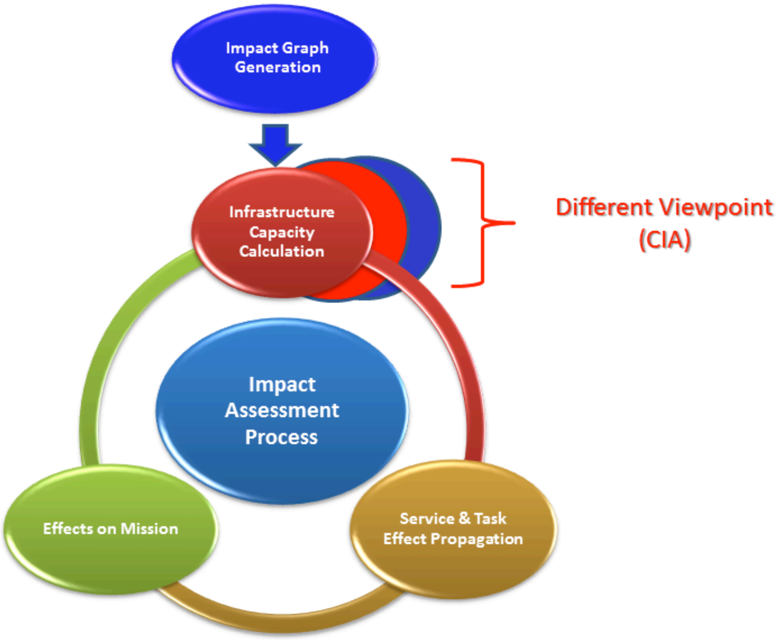
Impact Graph Generation
Infrastructure Capacity Calculation
Different Viewpoint (CIA)
Impact Assessment Process
Effects on Mission
Service & Task Effect Propagation

Figure 4 – Mission Impact Assessment Phase

To generate the impact graph, Cyber-ARGUS makes a set of semantic queries, using SPARQL[5], to the KB. This graph allows the measurement of the node's capacity to accomplish the mission.

Cyber-ARGUS uses a unique index to represent this important capacity, using different perspectives, using different security viewpoints for the mission (Confidentiality, Integrity, and Availability). The ***Infrastructure Capacity Index (IC)*** measures the ability of a node to provide the required resources and services with a certain level of quantity, quality, effectiveness, and cost.

[5] http://www.w3.org/TR/rdf-sparql-query/

The IC calculation is presented in Equation 1, where $IC_x(i)$ represents the infrastructure capacity of *node i*; $sec_x(i)$ represents its ***security index***, and $exp_x(i)$ represents its ***exploit index***. The letter *x* denotes the security situation of a node for a specific perspective (i.e., confidentiality, integrity, or availability).

$$IC_x(i) = \exp_x(i) \times \sec_x(i) \ [1]$$

Using the same approach of Kim and Kang [33], Cyber-ARGUS uses TOPSIS [43] to aggregate a set of node attributes to define an index. In Cyber-ARGUS, the attributes and the associated weights used to generate the security index are provided by the mission Analyst and collected by an event manager process.

The exploit index measures how vulnerable a node is, considering only plausible exploit scenarios, in other words, the vulnerabilities where there is a possible attack-path to explore it. To calculate it, Cyber-ARGUS retrieves all security information from the KB (consisting of vulnerability and exploit paths), and verifies the existence of active path attacks for the stored node's vulnerabilities. To compute the index, the possible exploit vulnerabilities are considered via their respective *Vulnerability Factor* (V_f).

IC measures the capacity of a Cyber-Node for providing its required service. However to understand how a node impacts the mission, this local index needs to be propagated to other mission components (services and tasks), to determine how the combination of them impacts the accomplishment of defined goals.

Cyber-ARGUS uses a Bayesian network [44] to propagate the IC's index through the mission components, measuring the success' belief of mission is accomplished, using the Impact Graph. To generate the Conditional Probability Tables (CPT), required to propagate the effects using a BN, Cyber-ARGUS uses an automated approach to build the CPTs based on parameterized distributions (that have semantic meaning) [45].

During the mission, ICs for the nodes are calculated and these values are propagated through the network. It is important to recognize that for each time-step, a round of measurements generates a particular view of mission levels, and includes the calculation of the likelihood that the goal is achieved given that each node's service level keeps its observed trend.

3.4. Flexibility in Cyber Argus

The previous section presented how to measure cyber impacts using the Cyber-ARGUS framework. Its main motivation was to develop a methodology for understanding how cyber components impact operational tasks during a mission, using real data in the environment. However, the framework cannot provide recommendations of what actions an Analyst needs to take to fix the current situation if responding to a cyber attack; the framework only identifies what is wrong and how each component contributes to the current situation.

The use of real data with Cyber-ARGUS is useful when a secure infrastructure is planned and tested exhaustively when planning cyber security strategies. But there is also a need for evaluating if actual infrastructure can support missions in a hostile environment. To address the analysis of potentially adverse situations, the *Hypothesis Definition* phase was developed, with the goal of simulating/emulating future environments, where the Analyst can manipulate variables (operational and infrastructure) and analyse the results.

The *Hypothesis Definition* phase enables the use of either real or simulated data to calculate the impact assessment. Simulated data is used to infer future plausible scenarios, showing what will happen based on actions specified by the Analyst (hypotheses). To enable the *Hypothesis Definition* phase, the *Classification of Cyber and Mission Data* phase requires collecting and correlating infrastructure information from simulated sensors (separately from real sensors), enabling the generation of future plausible scenarios.

The **Current Situation** calculation's process uses historical data collected in the real environment to generate the IC and the belief values of services and tasks. It is simple to understand, for example if a cyber-node has a transient failure (only in a specific slice of time), the belief of mission success in the *current situation* is completed influence by this event.

The process to calculate the **Plausible Situation** requires that the Analyst specify future actions that he plans to perform in the environment (Hypothesis Definition), for example, to fix a set of cyber-nodes issues. These actions are inserted in the Bayesian Network and future situations are inferred. The use of a Bayesian Network enables that the influence of a transient event decreases as new measurements collected indicate that the event is not repeated.

IV. CASE STUDY AND RESULT ANALYSIS

To provide simulated data to Cyber-ARGUS, the environment requires realistic simulation of both the operational and infrastructure environment. However, reproducing these behaviours in a real environment can be very complex, expensive, not repeatable, dangerous, or simply unfeasible. The approach adopted was to build a Simulation Testbed representing this environment. This approach has many advantages that are familiar to those who use such models, including the reproduction of real behaviours without unnecessary details and the ability to run various permutations of a scenario.

The ITA/GMU C2 Testbed [8] provides a rich simulation environment capable of generating approximately the same set of data as that of a real environment. In addition, there was a need for a cyber SA tool to implement the Cyber-ARGUS framework, to enable operational and cyber information to be fused and integrated in a coherent view.

The ITA/GMU C2 Testbed has two modules: the *Kinetic Operational Module* (*KOM*) and the *Testbed Emulation (TE)*. The first one, the *KOM*, is responsible for receiving physical behaviours from a *Computer Generated Forces Simulator* (CGF) and converting them into an appropriate format to be injected into the *TE*.

The second one, the *TE*, is responsible for generating all cyber-effects, whether caused by network, physical propagation, failures, or attacks. It receives operational information (such as aircraft tracks), calculates the effects, and injects the result inside the appropriate cyber-node. It is also responsible for injecting orders from specific-domain CGF simulators. In the Air Traffic Control (ATC) scenario, this module is responsible for receiving the aircraft's tracks from CGF and injecting them into the TE, to generate plans to be performed by CGF operational entities.

Using this environment, a case study was developed based on the ATC operations in the Campos Basin. The Campos Basin is a petroleum rich area located in the Rio de Janeiro state, and is responsible for 80% of Brazil's petroleum production. The oil exploration is made in oceanic fields, and the operational activities include heavy helicopter traffic between continental and oceanic fields during daytime, with an average of 50 minutes per flight.

The problem is that most oil platforms are located more than 60 Nautical Miles away from Macaé and the helicopters fly at low altitude. Most of the airspace is outside the range of land-based radar. The consequence is that the ATS provided on most of the oceanic area is based on non-radar procedures, which significantly reduces the efficiency of air operations, increasing the cost of operations and reducing its safety.

The oceanic area has a homogeneous airspace and a large concentration of low altitude air traffic. These reasons have motivated the Brazilian Air Traffic Department (DECEA) to evaluate the use of ADS-B technology [47] in a restricted airspace to supplement radar coverage to provide better air traffic service [48]. However, ADS-B, because of its broadcast and decrypted mode, became a strong candidate to be exploited by malicious users [49-51].

The use of Cyber-ARGUS to impact assessment in this scenario is presented in [12]. The current work uses the same environment to show the preliminary results of Cyber-ARGUS extended with the new *Mission Impact Assessment* algorithms.

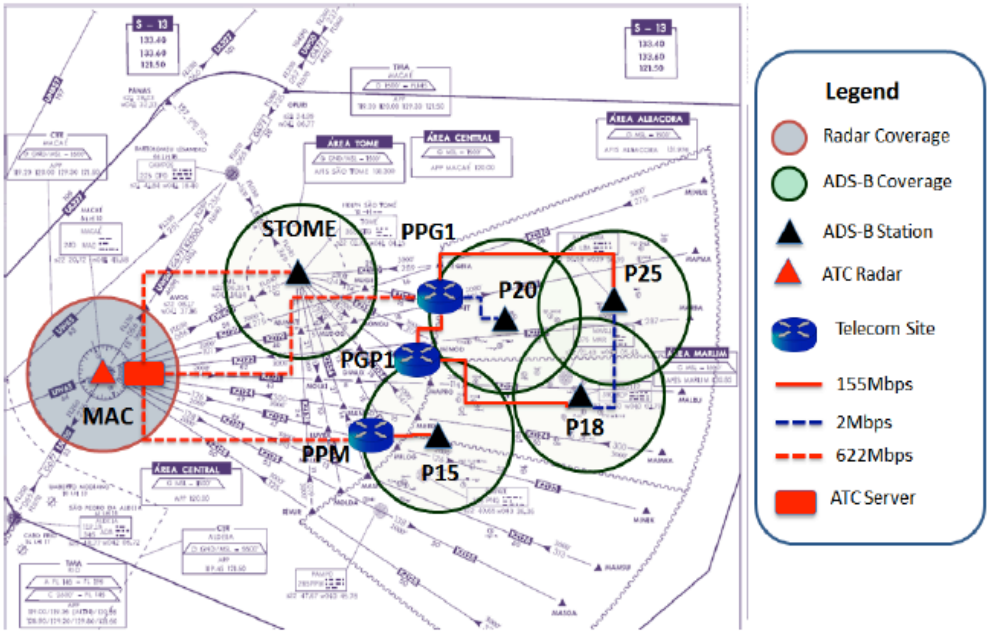

Figure 5 – Campos Basin and ATC Topology [12]

Figure 5 presents a map of the Campos Basin and the experiment topology implemented in the ITA/GMU C2 Testbed. To degrade this environment, two kinds of attacks are designed in the experiment. Initially, the scenario runs without any kind of attacks. The next step included a set of SMURF Attacks and UDP Flood Attacks that were performed against ATC-SIM (an emulated ATC console) during the final approach to platform heliports. In the last phase of experiment, a new set of attacks was performed during the final approach to the continental airfield. These are different than the previous work (which only used platform heliports) – this time aircraft flew towards the same place, making the separation task harder for air traffic controllers than in the previous phases. The selected sensor (MAC) was chosen because it is the most important sensor to the mission accomplishment. This happens because in the continental area, the MAC is the sensor that has the largest surveillance coverage. The Impact Graph related to this scenario is presented in Figure 6. In this graph, gray nodes are Cyber-Assets; green nodes are services; blue nodes are tasks; and the pink node is the goal of the mission. The arcs represent the dependencies (direct and temporal), and the number over the arcs defines time slices.

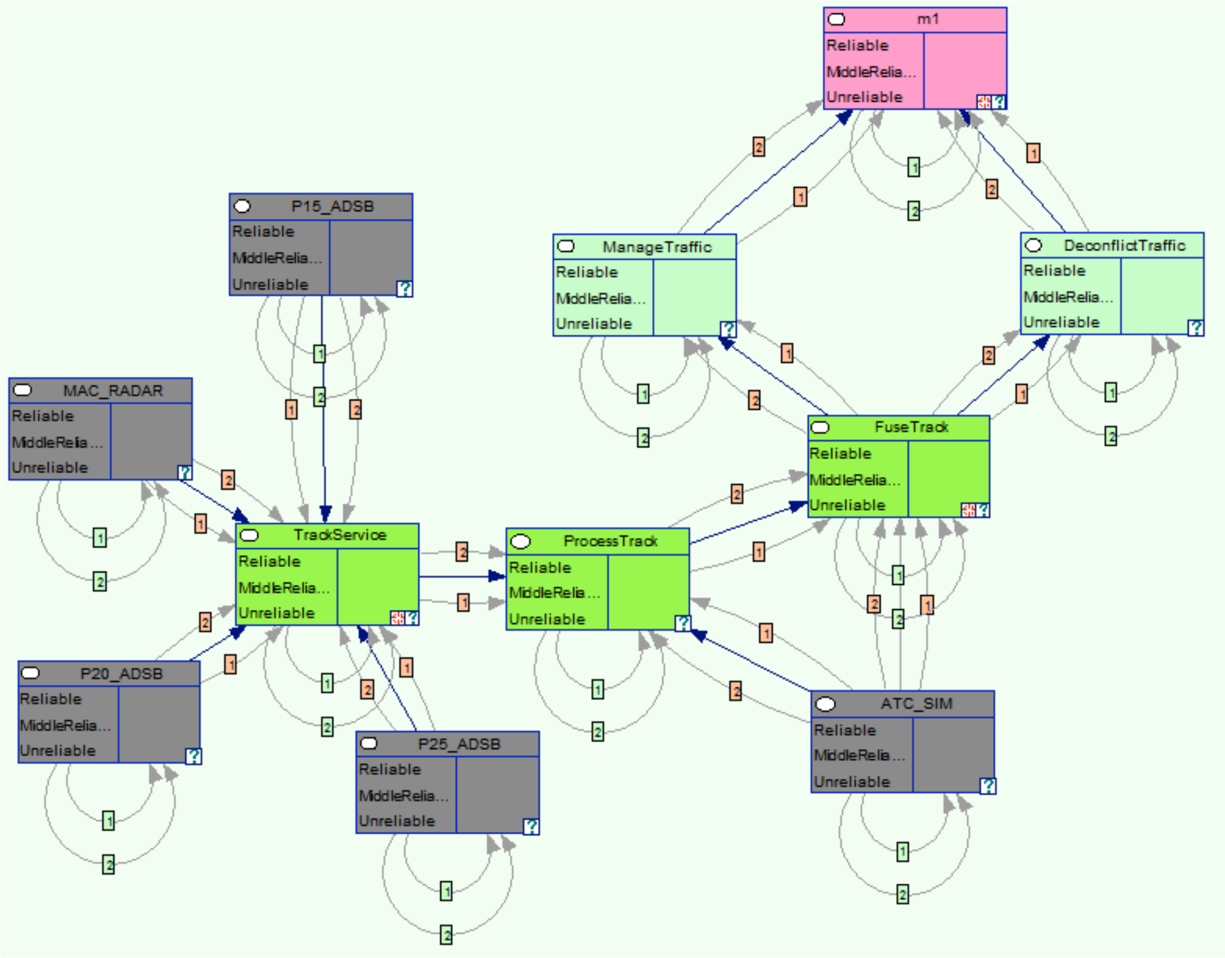

Figure 6 - Impact Graph for the ATC Scenario

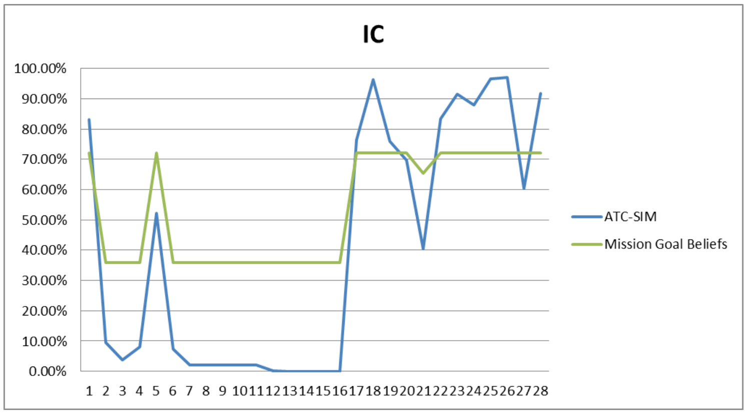

Figure 7 - Infrastructure Capacity Measurement for ATC Scenario

The graph in Figure 7 presents the mission goal belief and ATC-SIM infrastructure impact over time (time slices). Note that mission goal belief is calculated through the impact propagated by the Impact Graph, using a Bayesian Network [12]. Analyzing this graph, it is possible to see that the belief in the mission goal follows the ATC-SIM's IC trend.

Note that ATC-SIM infrastructure capacity decreases during UDP attacks against MAC-RADAR. The reason for this is simple. During the slot-time when the attacks happened, aircraft were returning to continental airfields, when only the MAC-RADAR provides track coverage. Thus, an attack against this sensor directly impacts the IC of the ATCSIM, since most of the information needed to perform its work is absent.

V. FINAL CONSIDERATIONS

This research presented the Cyber-ARGUS framework, which calculates the impact of cyber events have upon elements in the operational domain. This allows for a spectrum of analysis on complex C2 operations (military, civil, and others), where events that happen in one domain will be reflected in other domains. The framework also provides a better understanding of the critical events that affect the environment and have an impact on the mission. This capability can also be used to develop more accurate defense/offensive plans and scenarios in critical applications.

Cyber-ARGUS is a framework within an area where clear answers are usually not attainable, mostly due to the complexity of the problem as well as the level of subjectivity involved in continuous impact assessment. As such, the framework presented here should be seen as a first step. Yet, it is a very solid step, since after attempting various approaches we remain convinced that the solution to this problem relies on a combination of techniques where semantic technologies, multi-criteria analysis, probabilistic inference and simulation play a major role. Cyber-ARGUS enables the Analyst to have the ability to generate predictions about future situations through simulation and historical data.

The main contribution of this research in the scientific community is that it opens a new branch in cyber security, building on the new approach for handling security, a mission viewpoint approach, proposed by [7]. The Cyber-ARGUS framework enables cyber impact assessment for an ongoing mission using overall effects, making knowledge of enemy plans no longer required. This is different than similar works [30-32], in that this research not only further defines the problem, but also states how it can be solved and demonstrates, using a case study, that it can be implemented in a realistic scenario, enabling future studies to be based on solid experiments.

While this work has not been systematically assessed in terms of agility, we believe it is an important element in making more robust and flexible plans to address cyber attacks. By systematically assessing where the cyber vulnerabilities are in the mission, a Commander can then construct contingency plans for how to respond to the most likely threats, while not constraining the options available. Clearly, the ability to flexibly respond to cyber threats in general will greatly increase the agility of current operations.

ACKNOWLEDGEMENTS

The authors would like to thank the VT MÄK to provide all tools and support to develop the Testbed. They also thank the anonymous reviewers for their useful comments.

REFERENCES

[1] TAKAHASHI, T. **Sociedade da informação no Brasil: livro verde.** Brasília, Brazil: MCT, 2000. 153 p., il. p. ISBN 8588063018. Available from Internet: http://livroaberto.ibict.br/handle/1/774.

[2] BRAZIL. Portaria Normativa 3.389: **Política Cibernética de Defesa.** Brasília, Brazil: Ministério da Defesa (MD), December 2012.

[3] USA. **Cyber Command Fact Sheet.** Washington, USA: US Department of Defense (DoD), October 2010. Available from Internet: http://www.stratcom.mil/Cyber_Command.

[4] FLECK, D. **The Handbook of International Humanitarian Law.** 2nd. ed. Oxford, England: Oxford University Press, 2008. ISBN 0199573166.

[5] ENDSLEY, M. **The Application of Human Factors to the Development of Expert System For Advanced Cockpits.** In: HUMAN FACTORS SOCIETY. Annual Meeting of Human Factors and Ergonomics Society. New York, New York, USA: Human Factors and Ergonomics Society, 1987. p. 1388-1392.

[6] BOYD, J. R. **The Essence of Winning and Losing.** Unpublished. 1996.

[7] SAYDJARI, O. S. **Cyber Defense: Art To Science.** Communications of the ACM, ACM New York, v. 47, n.3, p. 52-57, 2004.

[8] BARRETO, A. B.; HIEB, M.; YANO, E. **Developing a Complex Simulation Environment for Evaluating Cyber Attacks.** In: Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2012. Orlando, USA: 2012. Paper 12248, p. 1-9.

[9] BARRETO, A. B.; COSTA, P.; YANO, E. **A Semantic Approach to Evaluate the Impact of Cyber Actions to the Physical Domain.** In: COSTA, P. C. G.; LASKEY, K. B. (Ed.). Semantic Technologies for Intelligence, Defense, and Security 2012. Fairfax, USA: CEUR-WS, 2012. v. 966, ISSN 1613-0073, p. 64-71.

[10] BARRETO, A. B.; COSTA, P. & YANO, E. **Using a Semantic Approach to Cyber Impact Assessment.** In: COSTA, P. C. G., EMMONS, I. & LASKEY, K. B. (Eds.). Semantic Technologies for Intelligence, Defense, and Security 2013. Fairfax, USA. CEUR-WS, 2013. v. 1097, ISSN 1613-0073, p. 101-108.

[11] ALBERTS, D.S. **The Agility Advantage: A Survival Guide For Complex Enterprises and Endeavors.** CCRPS Publications, 2011.

[12] BARRETO, A.B. **Cyber-ARGUS Framework - Measuring cyber-impact on the mission.** Thesis of doctor in science - Program of Electronic Engineering and Computer Science. Field of Computer Science - Instituto Tecnológico de Aeronáutica, Brazil, 2013.

[13] STEINBERG, A.; BOWMAN, C. **Rethinking the JDL Data Fusion Model.** In: National Symposium on Sensor and Data Fusion. San Diego, USA: International Society of Information Fusion, 2004.

[14] SALERNO, J. **Where's Level 2/3 Fusion: A Look Back Over the Past 10 Years.** In: Proceedings of the Tenth International Conference on Information Fusion. Quebec, Canada: International Society of Information Fusion (ISIF), 2007.

[15] TADDA, G. P.; SALERNO, J. S. **Cyber Situational Awareness - Issues and Research.** Springer, 2010. (Advances in Information Security), In: Overview of Cyber Situation Awareness, p. 15-35.

[16] BARFORD, P. et al. **Cyber Situational Awareness - Issues and Research.** New York, USA: Springer Publishing Company, Incorporated, 2009. In: Cyber SA: Situational Awareness for Cyber Defense, p. 3-14. ISBN 1441901396 9781441901392.

[17] AMOROSO, E. G. **Fundamentals of Computer Security Technology.** Upper Saddle River, USA: Prentice-Hall, Inc., 1994. ISBN 0-13-108929-3.

[18] SALTER, C.; SAYDJARI, O. S.; SCHNEIER, B. **Toward a Secure System Engineering Methodology.** In: NSPW'98, Proceedings of the 1998 Workshop on New Security Paradigms.

[19] PHILLIPS, C.; SWILER, L. P. **A Graph-Based System for Network-Vulnerability Analysis.** In: Proceedings of the 1998 Workshop on New Security Paradigms. New York, USA: ACM, 1998. (NSPW '98), p. 71-79. ISBN 1-58113-168-2. Available from Internet: http://doi.acm.org/10.1145/310889.310919.

[20] HOLSOPPLE, J.; YANG, S.; ARGAUER, B. **Virtual Terrain: a Security-Based Representation of a Computer Network.** In: DASARATHY, B. V. (Ed.). Proceedings of SPIE, Defense and Security Symposium 2008. San Diego, USA: 2008. v. 6973, p. 69730E-69730E-10. Available from Internet: http://dx.doi.org/10.1117/12.776980.

[21] HOLSOPPLE, J.; YANG, S. J.; SUDIT, M. **TANDI: Threat Assessment of Network Data and Information.** In: Proceedings of SPIE, Defense and Security Symposium 2006. San Diego, USA: 2006. v. 6242, p. 114-129. Available from Internet: http://dx.doi.org/10.1117/12.665288.

[22] JAKOBSON, G. **Extending Situation Modeling with Inference of Plausible Future Cyber Situations.** In: Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2011 IEEE First International Multi-Disciplinary Conference on. Miami Beach, USA: Institute of Electrical and Electronics Engineers (IEEE), 2011. p. 48-55.

[23] JAKOBSON, G. **Mission Cyber Security Situation Assessment Using Impact Dependency Graphs.** In: Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on. Chicago, USA: International Society of Information Fusion (ISIF), 2011. p. 1-8.

[24] LEWIS, L.; JAKOBSON, G.; BUFORD, J. **Enabling Cyber Situation Awareness, Impact Assessment, and Situation Projection.** In: Military Communications Conference, 2008. MILCOM 2008. IEEE. San Diego, USA: Institute of Electrical and Electronics Engineers (IEEE), 2008. p. 1-6.

[25] JAJODIA, S.; NOEL, S. **Topological Vulnerability Analysis.** In: Cyber Situational Awareness Advances in Information Security: Springer, 2005. Volume 46, 2010, pp 139-154.

[26] JAJODIA, S. et al. **Cauldron Mission-Centric Cyber Situational Awareness with Defense in Depth.** In: MILITARY COMMUNICATIONS CONFERENCE (MILCOM 2011). Baltimore, USA: Institute of Electrical and Electronics Engineers (IEEE), 2011. p. 1339-1344. ISSN 2155-7578.

[27] WHITEMAN, B. **Network Risk Assessment Tool (NRAT).** IA Newsletter, Cyber Security & Information Systems Information Analysis Center (CSIAC), v. 11, p. 4-8, 2008.

[28] BUCKSHAW, D. L. et al. **Mission Oriented Risk and Design Analysis of Critical Information Systems.** Military Operations Research, Military Operations Research Society, Alexandria, USA, v. 2, p. 19-38, 2005.

[29] LEMAY, E. et al. **Model-based Security Metrics Using Adversary View Security Evaluation (ADVISE).** In: Quantitative Evaluation of Systems (QEST), 2011 Eighth International Conference on. Aachen, Germany: IEEE Computer Society, 2011. p. 191-200.

[30] MUSMAN, S. et al. **Computing the Impact of Cyber Attacks on Complex Missions.** In: 2011 IEEE International Systems Conference (SysCon). 2011. p. 46-51.

[31] MUSMAN, S. **A Systems Engineering Approach for Crown Jewels Estimation and Mission Assurance Decision-Making.** In: IEEE Symposium on Computational Intelligence in Cyber Security (CICS). Paris, France: Institute of Electrical and Electronics Engineers (IEEE), 2011. p. 210-216.

[32] MUSMAN, S. **Evaluating the Impact of Cyber Attacks on Missions.** Washington, USA: MITRE Corp, 2010.

[33] KIM, A.; KANG, M. H**. Determining Asset Criticality for Cyber Defense.** Washington, USA: Naval Research Laboratory, 2011.

[34] DEPARTMENT OF DEFENSE (DOD). **DoD Architecture Framework – Volume 1: Introduction, Overview, and Concepts.** Washington, USA: Department of Defense (DoD), 2009.

[35] D'AMICO, A. et al. **Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships Between Cyber Assets, Missions and Users.** In: Proceedings of the 5th International Conference on Information Warfare and Security (ICIW). Ohio, USA: Academic Conferences International, 2010.

[36] MATHEUS, C. J. et al. **SAWA: an Assistant for Higher-Level Fusion and Situation Awareness.** Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, Orlando, USA, v. 5813, p. 75-85, 2005.

[37] DEPARTMENT OF DEFENSE (DOD). **Joint Publication JP 1-02 - Dictionary of Military and Associated Terms.** Washington, USA: Department of Defense (DoD), August 2012.

[38] DEPARTMENT OF DEFENSE (DOD). **DoD Directive, DoD Policy and Responsibilities for Critical Infrastructure.** Washington, USA: Department of Defense (DoD), July 2010.

[39] JABBOUR, K.; MUCCIO, S. **The Science of Mission Assurance.** Journal of Strategic Security, Henley-Putnam University, IV, p. 61-74, 2011.

[40] HIEB, M. R. et al. The SIMCI OIPT: **A Systematic Approach to Solving C4I/M&S Interoperability.** In: SISO Fall 2002 SIW. Orlando, USA: 2002.

[41] NATO SCIENCE AND TECHNOLOGY ORGANIZATION. **RTO-TR-MSG-048 - Coalition Battle Management Language (C-BML)**. February 2012.

[41] ALLWEYER, T. BPMN 2.0**: Introduction to the Standard for Business Process Modeling.** Norderstedr: Bod, 2010. 156 p. ISBN 978-3839149850.

[42] BALMAS, F. **Displaying Dependence Graphs: a Hierarchical Approach.** In: BURD, E.; AIKEN, P.; KOSCHKE, R. (Ed.). Proceedings of the Eighth Working Conference on Reverse Engineering (WCRE'01). Washington, USA: IEEE Computer Society, 2001. (WCRE '01), p. 261. ISBN 0-7695-1303-4.

[43] YOON, K.; HWANG, C. **Multiple Attribute Decision Making – An Introduction.** 1st. ed.: SAGE Publications, 1995.

[44] PEARL, J. **Markov and Bayes Networks: A Comparison of Two Graph Representations of Probabilistic Knowledge.** California, USA: University of California, 1986.

[45] FENTON, N.; NEIL, M.; CABALLERO, J. G. **Using Ranked Nodes to Model Qualitative Judgments in Bayesian Networks.** Knowledge and Data Engineering, IEEE Transactions on, v. 19, n. 10, p. 1420-1432, 2007. ISSN 1041-4347.

[46] MURPHY, K. **Dynamic Bayesian Networks: Representation, Inference and Learning.** Dissertation (PhD). UC Berkeley, Berkeley, USA, 2002.

[47] ICAO. **Global Air Navigation Plan for CNS/ATM Systems.** Montreal, Canada: International Civil Aviation Organization (ICAO), 2012.

[48] DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO (DECEA). **Use of ADS-B at the Macaé - Cuenca de Campos TMA.** Lima, Peru: International Civil Aviation Organization, 2010.

[49] MCCALLIE, D.; BUTTS, J.; MILLS, R. **Security Analysis of the ADS-B Implementation in the Next Generation Air Transportation System.** International Journal of Critical Infrastructure Protection, Elsevier, v. 4, p. 78-87, 2011.

[50] STROHMEIER, M.; LENDERS, V.; MARTINOVIC, I. **Cryptography and Security, Security of ADS-B: State of the Art and Beyond.** Ithaca, USA: Cornell University Library, Jul 2013. Available from Internet: http://arxiv.org/abs/1307.3664.

[51] COSTIN, A.; FRANCILLON, A. **Ghost in the Air (Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B devices.** In: Black Hat Conference. Las Vegas, USA: Black Hat, 2012.