Using a Semantic Approach to Cyber Impact Assessment

Alexandre de Barros Barreto
Instituto Tecnológico de Aeronáutica
São José dos Campos SP Brasil
Email: kabart@ita.br

Paulo Cesar G Costa
George Mason University
Fairfax, VA, USA
Email: pcosta@gmu.edu

Edgar Toshiro Yano
Instituto Tecnológico de Aeronáutica
São José dos Campos SP Brasil
Email: yano@ita.br

***Abstract*—The use of cyberspace as a platform for military operations presents many new research challenges. This paper focuses on the specific problem of assessing the impact of an event in the cyber domain (e.g. a cyber attack) on the missions it supports. The approach involves the use of Cyber-ARGUS, a C2 simulation framework, along with semantic technologies to provide consistent mapping between domains. Relevant information is stored in a semantic knowledge base about the nodes in the cyber domain, and then used to build a Bayesian network to provide impact assessment. The technique is illustrated through the simulation of an air transportation scenario in which the C2 infrastructure is subjected to various cyber attacks, and their associated impact to the operations is assessed.**

***Index Terms*—Impact assessment, cyber-security, Bayesian Networks, C2, semantic technologies.**

I. Introduction

With the increasing automation of processes and systems that are part of critical infrastructures supporting military and civilian operations, the cyber domain became one of most crucial aspects in strategic planning.

As a result, major military players in the world stage started to envision cyberspace as a medium to extend their capabilities, in addition to their existing competencies in the traditional domains (land, air and sea) [1]. However, understanding how cyber operations affect operations and leveraging their effects on the mission are no trivial tasks [2].

To understand the significance of a cyber event in a mission requires mapping physical tasks to their required infrastructure, in a way of creating an integrated view of cyber and physical behaviors. The inherent complexity of this requirement implies, among other things, that an experienced mission analyst must be able to access all relevant data pertaining to the infrastructure and translate it to the support team. Further, this must be done in a way that allows them to understand the real impact of cyber threats not only on the network, but also on the mission it supports.

Many approaches exist to assess cyber impact. However, most are not suitable for supporting complex cyber impact assessment in real situations, where the correlation between kinetic tasks and cyber events needs to be assessed continuously, and with a high temporal resolution. This is a considerable gap that has not been successfully filled, in spite of the relatively large body of research focused on the subject.

This paper presents the Cyber-ARGUS Framework, which leverages semantic technologies to fuse data collected from sensors within the physical and the cyber domains, as well as to retrieve information relevant to the assessment of cyber impact.

The main contribution of Cyber-ARGUS is to provide a mapping of how cyber-events impact tasks in operational level as the mission unfolds. The framework does not create complete maps of vulnerabilities and attacks, or a comprehensive view of how these vulnerabilities and attacks can affect the overall mission. Instead, the framework is meant to provide analysts who need real-time decision support with a simplified situational awareness, which includes understanding what assets are more critical in accomplishing the most important tasks and how these assets are impacted during a cyber attack. As an example from the case study developed for this research, consider the problem of an Air Traffic Security Analyst, who needs to define which elements need to be prioritized to ensure mission success. This analyst must consider data from a large set of different sensors and components, and perform his analysis within very tight time constraints. In his situation, a complete understanding of the current attacks and fault-trees is neither feasible nor necessary, and his task can be accomplished with the simplified mapping and associated impact analysis provided by Cyber-ARGUS.

This paper extends previous work from [3] by addressing how Cyber-ARGUS evaluates the cyber impact on the mission. Among other additions, this paper provides a more detailed explanation on how data from sensors is aggregated, how node-statuses are calculated, and how impact is propagated throughout the network.

To evaluate the Cyber-ARGUS capabilities, we have independently designed a specific air traffic service (ATS) scenario that relies on a new protocol to perform air traffic control in a critical area located at the Campos basin, Brazil. The scenario provides a rich environment to understand how such capabilities can be employed in real life critical operation. The basin, located in the littoral of the Rio de Janeiro state, is a petroleum rich area responsible for 80% of Brazil's petroleum production. ATS missions are critical, happen in real time, and attacks can result not only in considerable economic loss but also in risk of human lives.

This paper is organized as follows. Section II describes the

main concepts of the framework being proposed, as well as a brief survey of the most relevant approaches developed so far to address the problem. Section III conveys a short summary of the Cyber-ARGUS framework, discussing its core ideas. Section IV explains in detail the impact assessment process. Section V presents the study case developed independently for this research, showing the application of Cyber-ARGUS in a specific situation. Section VI presents the results and provides a brief analysis of their significance. Finally, Section VII brings a few considerations and raises issues that must be addressed in future research.

II. Background and Related Research

As implied above, understanding how cyber events affect the missions happening outside the cyber domain is a major requirement for military operations. A common approach for detecting intrusions and system attacks is to use a set of distributed sensors in the network. Preliminary work on this subject focused on specialist or signature-based systems [4], [5].

However, understanding the significance of a cyber-event to a supported mission requires more than identifying attacks and suspect events. It is also necessary to assess their impact on the mission.

Cyber Impact Assessment can be understood as the estimation and prediction of effects on planned or estimated/predicted actions by participants; including interactions between action plans of several players (e.g. Assessing susceptibilities and vulnerabilities to estimated/predicted threat actions given one's own planned actions) [6].

Most approaches attempt to predict how vulnerabilities can be exploited by the enemy (enemy's focus) [7]. Usually, an attack graph [8] that includes vulnerabilities and exploit strategies is generated. Then, an analyst leverages information contained in the graph to calculate impact assessment.

There are a number of issues with this approach. As an example, there are situations in which it is not possible to predict the enemy's behavior, due to the lack of evidence (e.g. on attacks or its detection) resulting in ignorance of self-vulnerabilities or of enemy capabilities. Another issue is the computational problem involved in creating and evaluating the graphs [9].

A recent approach is based on the belief that it is not necessary to identify the enemy's plan or to recognize its actions against one's system. Instead, it is only necessary to know the impact that any plan (ours and enemy's) can have on one's system (mission) [10]. In other words, it is easier to understand the enemy's capabilities and restrictions than it is to predict his behavior. This approach focuses on effects; and does not require one to detect attacks or attackers, but to understand the spectrum of potential effects on the mission. To measure the impact, a model of the mission must be built that includes all critical components that must be identified and monitored. However, [9]–[11] do not describe how to accomplish the mapping between cyber and non-cyber components in detail, as well how to assess the impact of cyber events using real infrastructure data.

An approach to cyber impact assessment was proposed by Holsopple et al. [12]. They define a normalized compromising score, which represents the level of compromise that a node has caused by a specific threat. This method requires defining the threat severity level. One potential approach is to use the Common Vulnerability Scoring System (CVSS). CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

Even if an analyst knows which attributes are critical to the mission; a second question needs to be answered: how to combine these attributes and generate an index to support coherent and consistent decisions? One strategy is to employ multi-criteria decision making methods (MCDM), a sub-discipline of operations research that explicitly considers multiple criteria in decision-making environments. MCDM provides a set of different approaches that can potentially be used in this cyber-impact assessment. One example is provided in [13], which uses the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) for threat assessment. TOPSIS is a multi-criteria decision analysis method based on the concept that the chosen alternative should have the shortest geometric distance from the positive ideal solution, and the longest geometric distance from the negative ideal solution [14].

Another applicable technique from the MCDM toolbox is presented by [15], which combines Analytic Hierarchy Process (AHP) and TOPSIS for quantifying the degree of security. AHP can be seen as a weight elicitation method based on pairwise comparisons between attributes, and can thus be employed to produce a consistent multi-attribute value structure from experts' input.

Kim and Kang [16] present another MCDM technique to evaluate the critical assets needed to accomplish a mission. Their approach is extremely attractive because it allows for calculating the asset value during a mission using local and global classification. Since the approach involves working in a real-time environment, the authors modified the TOPSIS process to calculate the worst (A-) alternative and the best alternative (A+). Also, a set of maximum and minimum acceptable levels is defined as a means to ensure acceptable performance.

However, this approach has two interrelated limitations. Initially, it was not designed to handle tasks, which are key aspects in defining time sensitive aspects of the mission. As a result of this limitation, the technique becomes less suitable for evaluating distinct phases of a mission. For example, during deployment of a laser-guided bomb by an aircraft, both the soldier illuminating the target (e.g. from a nearby location) as well as the aircraft launching the bomb play equally critical tasks. However, after the ordnance release the aircraft loses its relative importance, since the bomb now relies only on the soldier's laser device in its flight to the target. Such time-sensitive situations cannot be modeled using the approach stated in [16].

In addition to the impact assessment calculations, a key

aspect is to propagate the impact assessed locally in a way of ensuring a coherent understanding of its consequences from a global perspective. A Markov approach approach to model security risk was developed by [17]. However, using Markov processes to propagate impact assessment brings the weakness of the technique's inability to represent non-monotonic dependencies. For instance, in this technique two independent variables must be directly connected by an edge, merely because there are some other variable that depends on both [18].

An alternative for modeling risk propagation is Bayesian Networks (BN). Examples of its use for solving real impact assessment problems can be found in [19], [20]. Li et al. [21] combine CVSS and Attack Graphs in a consistent representation using BNs - which are used to represent the uncertain aspects between exploitation attack paths and the required vulnerabilities. However, we were not able to find a formal description on how to build and elicit the probability tables, which is essential for implementing the technique in a real situation.

Similar the aforementioned work, Singhal and Ou [22] show how to propagate the risk, which is calculated using CVSS metrics, through an enterprise environment using probabilistic attack graph. The latter can be understood as an attack graph that has the associated uncertainty handled by BNs. One problem that is common to all the aforementioned approaches that use BNs to represent uncertainty in attack graphs is that they require complete knowledge of the enemy, a precondition that renders these modeling techniques unrealistic for practical problems.

A different use of BNs is presented by Duan and Babu [23], which periodically collects performance data at three levels: applications, database server, and operating system. The collected data is used to construct probabilistic models for predicting service-level violations. This approach is extremely similar to that of [10], [11], where the impact is calculated by identifying the critical components of mission, their dependences, as well as the effects of their respective failure, and then using a BN to propagate the beliefs to the overall mission.

III. Cyber-ARGUS Framework Review

The goal of this research is to design a framework that enables the understanding of cyber impact within a mission context. This chapter introduces the Cyber-ARGUS framework, which is meant to support this goal. Unlike most approaches cited in Section II, the framework is based on a mission viewpoint approach [10], [11]. From this perspective, the focus is on measuring how the effect generated by a cyber-event intervenes on the results of tasks performed in a mission.

Mapping from the cyber domain to the mission domain requires a few concepts to be defined (e.g. mission, service, and cyber node). The DoD Architectural Framework [24] defines a *mission* as composed by 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 *service* is a mechanism that enables access to a set of one or more capabilities. In other words, availability of services define which tasks can be performed. The last concept is *cyber node*, which is the element that hosts one or more services.

To understand how an event can produce effects in a mission, Cyber-ARGUS uses an adaptation of the impact dependence graph presented in [7]. The adapted graph includes all relations between tasks; tasks and services; as well as between services and cyber nodes, resulting in a structure that makes it easier to assess the consequences that follow when a node is compromised. Cyber-ARGUS flow of activities is comprised of three main phases [3], [25]: 1) Mission Modeling, 2) Collection Cyber and Mission Situation Awareness, and 3) Cyber Impact Assessment. The first two are treated in parts A and B of this Section, while the latter is explained in more detail in Section IV.

A. Mission Modeling

During the first phase, the core idea is to capture all information about the tasks required to accomplish the mission and consolidate these in an integrated data representation. This allows for a comprehensive analysis to be performed. In our framework, the importance of any given element is measured with respect to its relevance to impact assessment, and includes the associated tasks, the relationships between tasks, objectives, resources required to develop the mission and, finally, the task performer (i.e., entity or set of entities that have the responsibility to execute the mission).

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, nodes, etc.). Semantic technologies also facilitate code reuse, which allow us to avoid having to develop the mission ontology from scratch. Instead, Cyber-ARGUS leverages previous related work by D'Amico et al. [26] and Matheus et al. [27] in its own architecture.

Within this phase of the Cyber-ARGUS activity flow, a mission analyst can design the mission model using any business process language. The goal is to capture the most relevant information of the mission within the model and store it in a semantic Knowledge Base (KB). 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) [28]. However, as already mentioned, any business 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.

BPMN was not only convenient as a development tool for the framework, but also proved to be rather suitable for capturing the main aspects of a mission. This is especially true in civilian environments such as air traffic management, nuclear power plants, and others. Its business-oriented notation made it easier to accommodate air traffic domain concepts used in the evaluation part of the research, while also providing a relatively straightforward mapping to the associated concepts in the mission ontology.

The outcome of this first phase includes the mapping of tasks, sequences, and dependencies between them and the required services. Yet, there is no information on where these services are hosted, so the framework queries a service repository and retrieves all information linking IT nodes to their respective hosted services, as well as the network topology depicting the required connectivity.

Once this is accomplished, the framework has all critical information about mission (tasks; service dependencies; and cyber nodes) and can proceed with the next task, vulnerability discovery. The goal now is to locate all vulnerabilities in the infrastructure and store it into the KB to be used in the mission impact assessment phase. This is similar to an infrastructure discovery process, where the framework, using a database, looks for node vulnerabilities that are part of the environment. After this activity, all vulnerabilities and their related impact factors are collected, and Cyber-ARGUS stores this information into the KB. The classification is conducted by nodes, enabling an analyst to perform specific queries relating nodes to vulnerabilities and vice-versa.

The last activity within the Mission Modeling phase to model enemy behavior. Here, the goal is to 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 number of information that Cyber-ARGUS will use during impact assessment phase, we adopted the Cauldron approach developed at GMU [9]. Cauldron uses firewalls and others entrance devices' rules to eliminate implausible scenarios. This strategy reduces the number of nodes and the overall complexity of the original graph, generating a much simpler version that is stored into the Cyber-ARGUS KB as well.

B. Collection Cyber and Mission Situation Awareness

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 to calculate cyber impact.

To use this model, the mission analyst needs to collect information from cyber nodes. This will enable him to assess each node's current status, as well as to estimate, during the impact assessment phase, whether the node is able or not to perform the tasks it is expected to perform.

In addition to he node status information, Cyber-ARGUS must collect further data in order to calculate the cyber impact. An example is information about security, which includes attacks events, systems' abuses, etc. This information can be collected from intrusion detection and prevention systems, firewall logs, anti-virus, and other security log system. One important source for this type of data are 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 the need for 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). SWRL extends a set of OWL axioms to include Horn-like rules, which can be used in conjunction with the OWL knowledge base. The expressiveness achieved by this rule scheme is a key point ensuring the framework's ability to capture aspects that cannot be easily captured using OWL, such as utilization of resources, mission requirements, and others. Furthermore, using the aforementioned rules Cyber-ARGUS can classify from large data sets what elements are relevant, and store it to be used in the next phase, when the cyber impact is assessed.

IV. Cyber Impact Assessment

The cyber impact assessment is defined by four sub-tasks. The first is to generate the Impact Graph, which is a dependence graph [29] that represents mission, as well as the dependence (mission and IT domain) and the influence that each node has on the mission.

The framework will generate three impact graphs, each one representing a security viewpoint (Confidentiality, Integrity, and Availability - CIA). To generate these graphs, the mission analyst needs to inform which tasks he would like to assess and how deep the analysis should be. Using this information, the tasks and assets will be mapped using SPARQL queries [30]. Another key aspect of the framework is its ability to perform plausible reasoning with incomplete data, which enables principled handling of uncertainty. This is achieved by the creation of a Bayesian network (BN) [18] from the impact graph, which we explain later in this Section.

The most critical step in impact assessment is how to measure health node - the ability of the node to provide the services it is responsible for. Our framework measures it through the **operational capacity (OC)**, which is the ability to provide the required resources and services with a certain level of quantity, quality, effectiveness, and cost. In Cyber-ARGUS, this is calculated separately for each of the security views (CIA), enabling the generation of different perspectives.

The OC calculation is presented in Equation 1 below, where $\boldsymbol{OC_x(i)}$ represents the operational capacity of node i; $\boldsymbol{sec_x(i)}$ represents its security index, and $\boldsymbol{exp_x(i)}$ represents its exploit index. The security index x denotes the security situation of a node for a specific perspective (i.e., confidentiality, integrity, or availability).

$$OC_x(i) = cost \times sec_x(i) \times expl_x(i) \tag{1}$$

Using the same approach of Kim and Kang [16], Cyber-ARGUS uses TOPSIS 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 the event manager.

TOPSIS provides a choice between the shortest geometric distance from the positive ideal solution and the longest

geometric distance from the negative ideal solution. It is crucial because in most network attributes the highest and lowest values convey little or no useful meaning for calculating the security index. An example is the interface's load, in which the highest load value means that interface cannot answer new packets; and the lowest value simply indicates that the interface is not working.

The security index generation starts with creation of a **decision matrix** $(x_{ij})_{m_x n}$, where each of the m nodes (i) and their n associated attributes (j) are stored. The next step is the normalization of sensor data (Equation 2), which is required for ensuring consistency in additive aggregation techniques. In Cyber-Argus, all attributes are normalized using vector normalization [31], where x_{ij} is the value of the j^{th} attribute of the i^{th} node ($1 \leq i \leq m, 1 \leq j \leq n$).

$$z_{ij} = \frac{x_{ij}}{\sqrt{\sum_{j=1}^{n} x_{ij}^2}} \tag{2}$$

Using normalization matrix, the attributes weights are applied. In the Equation 3, w_j is the weight of the j^{th} attribute.

$$v_{ij} = w_j \times z_{ij} \tag{3}$$

The next step is the calculation of ***zenith*** (A^*) and ***nadir*** (A^-) values, using the equations Equation 4 and Equation 5, where I' is associated with benefit criteria, and I'' is associated with cost criteria [31]. As presented in [16], *max* and *min* values (for performance reasons) are defined by the analyst, based on the maximum and minimum values accepted to accomplish target mission.

$$A^* = v_1^*, ..., v_n^* = (max_j v_{ij} | i \in I'), (min_j v_{ij} | i \in I'') \tag{4}$$

$$A^- = v_1^-, ..., v_n^- = (min_j v_{ij} | i \in I'), (max_j v_{ij} | i \in I'') \tag{5}$$

In the sequence, the Euclidean distances are calculated using Equations 6 and 7.

$$D_j^+ = \sqrt{(\sum_{i=1}^{m} (v_{ij} - v_i^*)^2)}, j = 1, ..., n \tag{6}$$

$$D_j^- = \sqrt{\sum_{i=1}^{m} (v_{ij} - v_i^-)^2)}, j = 1, ..., n \tag{7}$$

Finally, the last step is the calculation of relative closeness to ideal solution (T_j^*). In our framework, this metric represents the security index of a node, $sec_x(i)$, and is calculated using Equation 8. An alternative w is better than y, when $T_w^* > T_y^*$.

$$sec_x(j) = T_j^* = \frac{D_j^-}{D_j^- + D_j^+} \tag{8}$$

The second component of OC is the **exploit index**, $expl(i)$. To calculate it, Cyber-ARGUS retrieves all security information from KB (vulnerability and exploit paths), and verifies the existence of active path attacks to the stored node's vulnerabilities. To compute the index, the possible exploit vulnerabilities are considered via their respective **vulnerability impact factor (V)**, as presented in Equation 9.

$$expl(i) = [\prod_{k=0}^{n} (1 - V_{[k]}(i))] \tag{9}$$

In Equation 9, *i* represents the cyber-node and *n*, the number of vulnerabilities that have a known exploit path that can be explored. This index has the same principles of metrics defined in [32], where the more high score vulnerabilities a node has, the smaller its OC will be and, consequently, the worst will be its ability to provide contracted services reliably.

OC's definition is an essential step in Cyber-ARGUS, as it reflects the model's beliefs. That is, a higher OC means a higher likelihood of accomplishing the mission's goals. The propagation of these beliefs is performed using a BN. In our model, cyber-asset is a deterministic rank node and its values are based on the calculated OC. To simplify the composition of a BN, the OCs will be discretized in three parametric states: high, medium, and low operational capacity. Belief on the reliability of services and tasks are also represented as probabilistic nodes, which states are: unreliable, medium reliability, and reliable. The range of each one of aforementioned states is calculated as defined in [33].

The values of cyber-nodes (i.e. their state variables) are used to assess the beliefs on the reliability of service and tasks. A main issue is how to generate the conditional probability tables (CPT) for the service and task nodes, since it requires time-consuming work from analysts [33]. For example, considering a node that has five parent nodes and each node has two different states, its associated CPT will have 63 values to be elicited (2^5-1, since the last value can be calculated). Cyber-ARGUS addresses this issue by using an automated approach to generate CPTs, as defined in Fenton and Neil [33]. A TNORMAL distribution is used to define the weighted rank node functions, and to calculate the CPTs. Equation 10 illustrates this approach, where **X** is the target variable and **Y** is the conditional evidence.

$$p(X|Y) = \left[FUNC, \quad \frac{1}{\sum_{i=1}^{n}(w_i)}, \quad 0, \quad 1\right] \tag{10}$$

A TNORMAL is similar to a NORMAL distribution, but with its values enclosed within a finite range. In the aforementioned equation, the first parameter is the mean of distribution, which is calculated using **WMIN** (Equation 11) and **WMAX** (Equation 12). The second parameter is the variance, which is calculated using the weight of influence that each parent-node has over the target variable. The last two parameters (values 0 and 1) are the boundary defined for $p(X|Y)$.

$$WMIN = min_{\forall_{i=1,...,n}} \left[\frac{w_i X_i + \sum_{i \neq j}(X_j)}{w_i + (n-1)}\right] \tag{11}$$

$$WMIN = max_{\forall_{i=1,...,n}} \left[\frac{w_i X_i + \sum_{i \neq j}(X_j)}{w_i + (n-1)}\right] \tag{12}$$

In Cyber-ARGUS, weights can be collected during Mission Modeling, using service-level information from the mission analyst. However, they can also be set manually by the analyst, so to reflect his level of uncertain about the fact. In general, the network weight is proportionally inverse to node's distance. For example, if node A hosts a service, its **weight** (w_k) is set to 1 (one). However, if node B is a neighbor of node A and does not host the target service, the framework applies Equation 13, where *r* is the distance of hosted node.

$$w_k = \frac{1}{r} \tag{13}$$

Further, when a dependent node (service or task) connects parent nodes using **OR** relationship, the **WMAX** function is used. Conversely, if it has an **AND** relationship, the framework uses the **WMIN** function.

The cyber impact on the mission is calculated after the belief propagation process, which occurs step-by-step from cyber-assets to services and from services to tasks. A more formal representation of impact on the mission beliefs, $imp(x)$, is presented in Equation 14, where its values are calculated from a joint probability distribution. In the equation, *X* is the mission result node and *Y* is the set of parents of this node.

$$imp(X) = p(X|Y) = p(Y|X) \times \prod_{i=1}^{n} p(X_i) \tag{14}$$

V. Study Case - Air Traffic Scenario

To evaluate the framework, we have independently developed an air traffic scenario representing the Air Traffic Control operations in the Campos Basin. This is a petroleum rich area in the Rio de Janeiro state that is responsible for 80% of Brazil's petroleum production, which is prospected and explored from oceanic fields. The operation relies on heavy helicopter traffic between the continent and oceanic fields during daytime, with an average of 50 minutes per flight.

To support this operation, Brazil has an Air Control Center (ACC) in Macaé (Rio de Janeiro). This center has a radar station that supports the surveillance service within the terminal. However, the oil platforms are located at sites that are more than 60NM from Macaé. Helicopter flights are carried out at low altitude, so there is no radar coverage close to the oil platforms and thus the Air Traffic Service (ATS) has to be based on non-radar procedures. This significantly reduces efficiency of air operations.

The Brazilian Government solution currently under study includes adopting the Automatic Dependent Surveillance-Broadcast (ADS-B) technology. The strategy is to supplement radar coverage in the oceanic air space. The ADS-B operation is based on using radios to transmit and receive aircraft position information generated through the satellite GNSS GPS via a data link. The radios work as relay agents, sending positional information to a central node. This data is then integrated to an ADS-B Server, which supports air traffic controllers in managing the air traffic.

This new technology has a set of security issues. A complete survey of ADS-B's vulnerabilities, different ways to exploit it, and the importance in protecting it is presented in [34].

Due to its criticality and vulnerability, the Campos Basin's scenario is a good candidate to validate the Cyber-ARGUS framework. The scenario was implemented using a complex, distributed simulation/emulation environment, the C2 Collaborative Research Testbed [25].

The C2 Collaborative Research Testbed scenario includes all ADS-B radio-stations existing in the area, a set of simulated helicopters. It provides a realistic environment, suitable for evaluating all phases of the Cyber-ARGUS framework. In the experiments, Cyber-ARGUS was used to build the Impact Dependence Graph, which has all tasks, services and nodes required to asses the cyber-impact on the typical mission with that scenario. As an example, to accomplish goal "M1" it is required to perform tasks "Manage Traffic" and "Deconflict Traffic," which were part of the experiments. The resulting graph was used to build the BN, and the services and tasks beliefs were calculated using WMIN and WMAX function, enabling that impact on the mission can be calculated. The preliminary results of these experiments are discussed in Section VI below.

VI. Preliminary Results and Discussion

In the Cyber-ARGUS evaluation experiments, each round consumed approximately two hours. During this time, a set of attributes of the cyber nodes were collected and their associated OCs were calculated. The OCs were then used to feed the BN and calculate the impact.

In this initial evaluation, the focus was in measuring the availability attributes in response to a campaign of Deny-of-Service attack (DoS). A DoS is an attempt to make a machine or network resource unavailable to its intended users. This attack aims to interrupt the service that is required to be performed for achieving a given mission task. The campaign was performed during three times, and in each iteration the required values were collected and the final impact assessed using the full Cyber-ARGUS process. In the first attack, the target included the ADS-B radios P20 and MAC. These two radios are important to the mission because they cover most of the oil platforms. When they fail, some platforms lose their ADS-B coverage, which results in the ATC reverting back to a lesser operation mode with increased separation between aircraft. The second attack aimed to deny all network, and all radio's nodes and servers were attacked. In the last campaign, the attack was specifically against the ATC-SIM. This is a server responsible for processing all tracks, fusing them and displaying on the ATC's visualization. It provides all information needed for the controllers' situational awareness.

The results of the first and second attacks are shown in the Figure 1. In the graphic, the beliefs for nodes OC, service and goal are represented. All values were normalized, and the most important information is the trend of attributes. Note that Mission Goal (M1) is completely insensitive to variations in the P15 radio. However, attacks on nodes MAC and P20

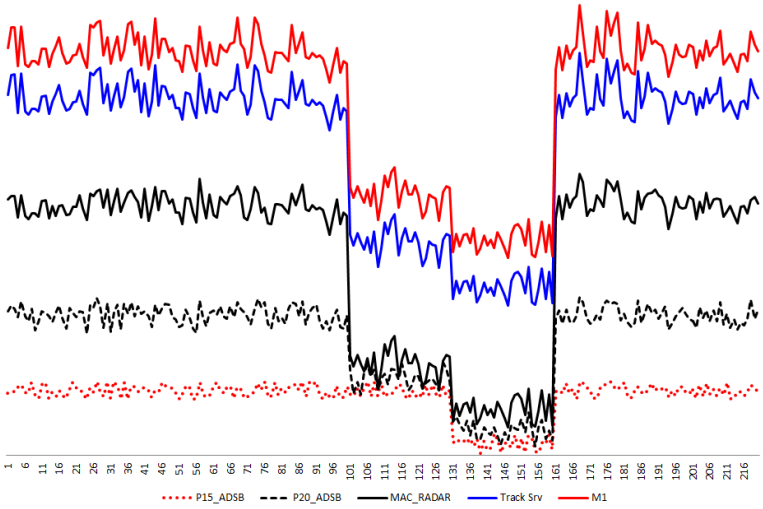

Fig. 1. Attack on P20 and MAC

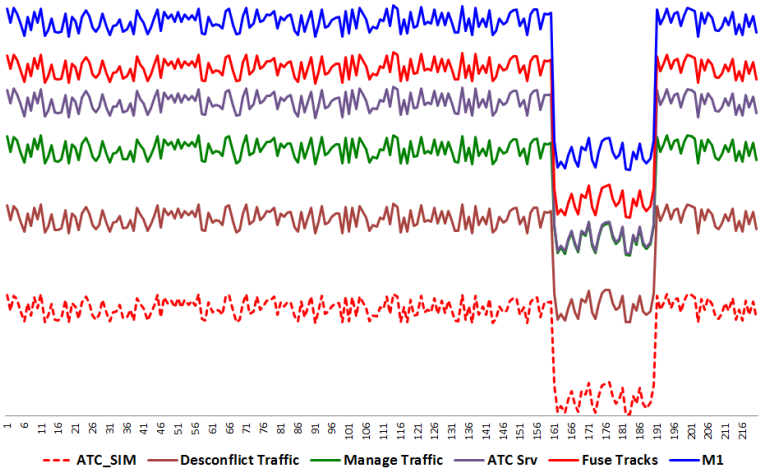

Fig. 2. Attack on ATC Server

(between 100 and 150 slot-time) resulted in a decrease in the track service and the goal beliefs. This shows that OC is a good estimator of mission assurance [11].

The last attack was more critical, as it happens on the main server that supports the mission. The results clearly show that all process automation was denied, decreasing the belief that mission can be performed with the same level of success than in a normal situation. Figure 2 shows that when the server is down, controllers revert back to conventional operation. This results in a great decrease of operational performance, although the mission still continues to happen. As in the early example, during the ATC attack the trend line is the same to the server, to the services it hosts, and to the mission goal.

VII. Final Remarks

Cyber-ARGUS is a framework that enables the calculation of the impact that actions within the cyber domain have over elements in the operational domain. This allows for a large spectrum of analysis on complex Command and Control operations (Military, Civil, and others), where events that happen in one dimension will be reflected in other dimensions. The framework also enables a better understanding of the critical events that affect the environment and have impact on the mission. This capability can also be used to develop more accurate defense/offensive plans and scenarios in critical applications.

In this paper, we showed the use of a knowledge base to generate the impact graph, which is then used to propagate

the nodes effects beliefs to services and tasks.

This is a research in progress in an area where clear answers are usually not attainable, mostly due to the complexity but also to the subjectivity involved in assessing impact in an ongoing operation. Currently the framework is being extended to provide new capabilities and allow its use in increasingly richer and more complex scenarios. One of the limitations of the current implementation is its inability to change the network topology and reflect the effect inside the BN, which is an important aspect given the constant network changes due to sensor reallocation, losses, and similar phenomena. Another limitation is the lack of a proper modeling of the enemy behavior (attack graph), which is needed to calculate the exploit index, and generate accurate information to represent the OC index. Finally, it's necessary more complex and different scenarios, providing confidence to apply method in general Command and Control scenarios.

ACKNOWLEDGMENTS

The authors would like to thank VT MÄK for providing all tools and support to develop the Testbed. They would also express their gratitude to the anonymous reviewers for their careful work and insightful comments.

REFERENCES

[1] M. G. W. T. Lord, "Cyberspace operations: Air force space command takes the lead," *High Frontier - The Journal for Space & Missile Professionals*, vol. 5, pp. 3–5, 2009.

[2] V. N. E. Brown, "Difficulties encountered as we evolve the cyber landscape for the military," *High Frontier - The Journal for Space & Missile Professionals*, vol. 5, pp. 6–8, 2009.

[3] A. B. Barreto, P. Costa, and E. Yano, "A semantic approach to evaluate the impact of cyber actions to the physical domain," in *Semantic Technologies for Intelligence, Defense, and Security 2012.*, P. C. G. Costa and K. B. Laskey, Eds., vol. 966, no. ISSN 1613-0073. CEUR-WS, October 2012, pp. 64–71. [Online]. Available: http://ceur-ws.org/Vol-966/STIDS2012_T08_BarretoEtAl_EvaluateImpactOfCyberActions.pdf

[4] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, vol. 13, pp. 222–232, 1987.

[5] T. Bass, "Multisensor data fusion for next generation distributed intrusion detection systems," in *IRIS National Symposion*, 1999.

[6] É. Bossé, J. Roy, and S. Wark, *Concepts, models, and tools for information fusion*. Artech House ˆ eBoston Boston, 2007.

[7] G. Jakobson, "Mission cyber security situation assessment using impact dependency graphs," in *Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on*, 2011, pp. 1–8.

[8] B. Schneier, "Attack trees: Modeling security threats," Dr. Dobb's journal, December 1999.

[9] S. Jajodia, S. Noel, P. Kalapa, M. Albanese, and J. Williams, "Cauldron mission-centric cyber situational awareness with defense in depth," in *MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011*, 2011, pp. 1339–1344.

[10] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, "Computing the impact of cyber attacks on complex missions." in *2011 IEEE International Systems Conference (SysCon)*, 2011, pp. 46–51.

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

[12] J. Holsopple, S. J. Yang, and M. Sudit, "Tandi: threat assessment of network data and information," in *Proceedings of SPIE, Defense and Security Symposium*, vol. 6242, April 2006, pp. 114–129. [Online]. Available: http://dx.doi.org/10.1117/12.665288

[13] Q. Changwen and H. You, "A method of threat assessment using multiple attribute decision making," in *Signal Processing, 2002 6th International Conference on*, vol. 2, 2002, pp. 1091–1095 vol.2.

[14] C. L. Hwang, *Multiple Attribute Decision Making: Methods and Applications*, ser. Lecture Notes in Economics & Mathematical Systems. Springer-Verlag, 1981.

[15] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and mcdm," *Power Delivery, IEEE Transactions on*, vol. 25, no. 3, pp. 1492–1500, 2010.

[16] A. Kim and M. H. Kang, "Determining asset criticality for cyber defense," ONR, Memorandum Report 55-6334, 2011.

[17] Y.-G. Kim, D. Jeong, S.-H. Park, J. Lim, and D.-K. Baik, *Modeling and Simulation for Security Risk Propagation in Critical Information Systems*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, vol. 4456, ch. Computational Intelligence and Security, pp. 858–868.

[18] J. Pearl, "Markov and bayes networks: A comparison of two grapgraph representations of probabilistic knowledge," University pf california, Tech. Rep., 1986.

[19] J. Wu, L. Yin, and Y. Guo, "Cyber attacks prediction model based on bayesian network," in *Parallel and Distributed Systems (ICPADS), 2012 IEEE 18th International Conference on*, 2012, pp. 730–731.

[20] S. van Gosliga, R. van Katwijk, and P. van Koningsbruggen, "Real-time traffic monitoring with bayesian belief networks," in *11th World Congress on Intelligent Transport Systems (ITS-2005)*, 2005.

[21] J. Li, X. Ou, and R. Rajagopalan, "Uncertainty and risk management in cyber situational awareness," in *Cyber Situational Awareness*, ser. Advances in Information Security, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Springer US, 2010, vol. 46, pp. 51–68. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-0140-8_4

[22] A. Singhal and X. Ou, "Security risk analysis of enterprise networks using probabilistic attack graphs," National Institute of Standards and Technology, Tech. Rep., 2001.

[23] S. Duan and S. Babu, "Proactive identification of performance problems," in *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*, ser. SIGMOD '06. New York, NY, USA: ACM, 2006, pp. 766–768. [Online]. Available: http://doi.acm.org/10.1145/1142473.1142582

[24] DoD, *DODAF. DoD Architecture Framework Version 2.0 - Volume 1: Introduction, Overview, and Concepts.*, DoD Std., 2009.

[25] A. B. Barreto, M. Hieb, and E. Yano, "Developing a complex simulation environment for evaluating cyber attacks," in *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2012.*, vol. 12248, December 2012, pp. 1–9.

[26] A. DAmico, L. Buchanan, J. Goodall, and P. Walczak, "Mission impact of cyber events: Scenarios and ontology to express the relationships between cyber assets, missions, and users." AFRL/RIEF, Tech. Rep. OMB No. 0704-0188, December 2009.

[27] C. J. Matheus, M. M. Kokar, K. Baclawski, J. A. Letkowski, C. Call, M. Hinman, J. Salerno, and D. Boulware, "SAWA: An assistant for higher-level fusion and situation awareness," *Proceedings of SPIE*, vol. 5813, no. 1, pp. 75–85, 2006. [Online]. Available: http://link.aip.org/link/?PSI/5813/75/1\&Agg=doi

[28] OMG, *Business Process Model and Notation (BPMN) 2.0*, http://www.omg.org/spec/BPMN/2.0, OMG Std., 2011.

[29] F. Balmas, "Displaying dependence graphs: a hierarchical approach," in *Proceedings of the Eighth Working Conference on Reverse Engineering (WCRE'01)*, ser. WCRE '01. Washington, DC, USA: IEEE Computer Society, 2001, pp. 261–. [Online]. Available: http://dl.acm.org/citation.cfm?id=832308.837144

[30] E. Prud and A. Seaborne, *SPARQL 1.1 Overview*, W3C Std., 2008. [Online]. Available: http://www.w3.org/TR/rdf-sparql-query/

[31] K. Yoon and C. Hwang, *Multiple Attribute Decision Making An Introduction*. SAGE, 1995.

[32] B. J. Argauer and S. J. Yang, "Vtac: virtual terrain assisted impact assessment for cyber attacks," in *Proc. SPIE 6973, Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security*, B. V. Dasarathy, Ed., vol. 6973, 2008.

[33] N. Fenton and M. Neil, *Risk Assessment and Decision Analysis with Bayesian Network*. CRC Press, 2013.

[34] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ads-b implementation in the next generation air transportation system." *International Journal of Critical Infrastructure Protection*, vol. 4, pp. 78–87, 2011.