18th ICCRTS

Title of Paper

Architecture for Cyber Defense Simulator in Military Applications

Topics:
Modeling and Simulation (primary topic)
Cyberspace Management (alternative topic)
Collaboration, Shared Awareness, and Decision Making (alternative topic)

Name of Authors

André F. A. Machado - Major
(STUDENT)
Instituto Tecnológico de Aeronáutica
São José dos Campos
SP, Brazil
majandre@ita.br
majafam97@gmail.com

Alexandre B. Barreto
Major
Instituto Tecnológico de Aeronáutica
São José dos Campos
SP, Brazil

Edgar Toshiro Yano
Professor
Instituto Tecnológico de Aeronáutica
São José dos Campos
SP, Brazil

Abstract

Currently, military actions are orchestrated within cyberspace and thus degradation or denial of service to cyberspace assets can have major consequences in combat. Based on general military strategies, with a focus on Command and Control, this paper proposes an architecture, for cyber defense simulation, which aims to unite kinetic environments with cyber environments. This architecture supports the creation of a flexible environment where different attack and disaster scenarios can be quickly developed and evaluated. A tactical scenario is used to evaluate the architecture. With a cyber-defense simulator, a commander can evaluate the current situation of the battlefield cyberspace, discern and correct potential vulnerabilities and design future actions.

1. Introduction

The modern battlefield is increasingly reliant on digital technology based networks and systems. Intentional or non-intentional disturbances on a single node of a network can result in a full or partial loss of a mission. This has led to the cyber domain being perceived as a new way to perform a war and increasing the effects in the other domains (land, air and sea). The knowledge and the measure of cyber effects in other domains are crucial to discover how an event in the cyber domain can affect a process executed in a physical domain.

Cyber-defense requires a constant surveillance lifecycle [1] to be effective. The elements that make up a security lifecycle are categorized into the following three areas: Prevention, Detection and Response.

- Prevention performs a risk management effort in which assets that requires support for confidentiality, integrity and availability are identified. For each protection requirement, the analyst verifies the risk; the probability of vulnerabilities that can be exploited and their impacts. The result is the identification and implementation of a set of controls.
- Detection involves the monitoring of the status of the implemented controls. For the detection, it is necessary to collect and analyze events and identify incidents.
- Response comprises actions to deal with incidents. The examples of tasks performed during this phase are: impact measuring and corrective actions. Forensic investigations can also be executed.

The implementation of a complete and effective security lifecycle for a complex network is extremely difficult, expensive and frequently ineffective. The following are some causes for the difficulties:

- Risk management uses, during its conduct, static and general models. It performs the identification of key threats, and recommends and describes controls; using, mainly, written texts. This approach cannot deal with the complexities of a real large network, where a large number of nodes, with many different alternative connection paths.
- New vulnerabilities are discovered frequently and detailed analyzes are not properly executed. The developed controls are not updated and don`t deal with unknown attacks that explore the new vulnerabilities.
- Monitoring of the status of the many different elements of a complex network is a hard effort since it is difficult to understand and evaluate the importance of the events and their combinations.

One option, to develop a cyber-defense evaluation capability, is the use of simulation technology [2]; however, the current simulation models are not effective and realistic. Some restrictions are related the complexity of networks [3], behavior models (attackers and defenses) [4] and the conduct of impact assessment in the operational domain (domain where the mission happens).

In this paper, we propose an architectural model for a cyber-defense simulator that integrates the kinetic (operational) with the cyber environment. With this integration, we expect to improve the reality of the simulations and thus the assessment of the operational domain impacts of cyber-attacks. To make this proposal, it is necessary to achieve realistic scenarios, which depict the characteristics of the battlefield.

With the impossibility of covering all the possible scenarios, this paper will give general scenarios, which aims to cover many of the possibilities for integration between Command and Control Centers (C2C).

For the development of a global scenario, we consider that a particular region is divided into spheres of power (or command), depicted in Figure 1.

The level called Political includes the entire physical region and includes the other levels (operation-strategic and tactical). Although each level has its well-defined scope, they are strongly connected and the flow of information permeates all spheres.

In this article, we will analyze the tactical level because it has specific military characteristics that are not well modeled at the level of Information Technology (IT) [5]. The idea is to provide a minimum environment for the proposed study.

Figure 1 - Levels of Power

Five main topics are presented. The first topic presents related works. The following one presents the tactical scenario that we use to verify the simulation architecture. The third topic presents the infrastructure of IT. The fourth topic presents an architectural model for a cyber-defense simulator, and finally, in the last topic, an evaluation of the architecture, based on the cyber-attacks developed in the scenarios, will be presented, followed by concluding remarks.

2. Related Works

The defense of the cyberspace used to conduct military operations requires the knowledge about how an event in cyberspace affects other domains. The first related work uses an expert signature-base system approach [6]. In this work, when a system detects an event (using a signature system), a set of expert`s rules provide an answer.

However, Denning's work only tries to detect an intrusion event; but to understand the event significance in other domains it is necessary to assess its impact. This issue is partially answered by an attack-graph approach [7]. Attack-graphs model how exploiting multiple vulnerabilities may be combined for an attack, enabling the identification of weak points in the infrastructure and the evaluation of the cascading impacts.

However, the attack-graph technique has a serious weakness when the vulnerability or the attack-path cannot be identified. In this situation, the graph cannot be built, and any analysis, as it did not use this information, usually fails. Due to these limitations, Saydjari [8] asserts the need to find a different approach that works in this situation. The approach should reduce the effort required in the identification of the attacker's behavior and increase awareness about the meaning of an event with respect to the mission (or task) performance.

In this context, two series of frameworks / methodologies were developed. The first set has the focus on the risk planning, while the other, focuses on the mission real-time analysis. The risk planning approach is the *Mission Oriented Risk and Design Analysis (MORDA)* [9] developed from 1998 to 2005 and successfully applied on many Department of Defense (DoD) risk assessment studies [9]. MORDA joins different techniques (attack tree; information assurance models; and multiple objective decision analysis) and produces a consistent analysis about the mission restrictions and weakness. To perform its work, it uses another model, *Security Optimization Countermeasure Risk and Threat Evaluation System (SOCRATES)*. SOCRATES, in turn, uses a variety of domain experts (mission, attackers, system) to define a collection of data that characterize the mission restrictions and environment, the attacker behaviors (motivations, skills, and possible paths), and the system functionalities, vulnerabilities and restrictions. Based on these inputs, and through the use of multi-criteria analysis technics, SOCRATES classifies the elements required and calculates the risk to develop the mission.

An alternative approach used to risk planning is *Computing the Impact of Cyber Attacks on Complex Missions (CMIA) [10,11]* whose purpose is to identify which are the assets most relevant to the accomplishment of the mission. CMIA determines the impact of a cyber-attack by modeling the effect of the attack through a simulation of a mission expressed in *BPMN (Business Process Model Notation). The BPMN provides* a workflow of activities that are dependent upon information technology resources and Musman's method [10] calculates the reduction in measures of effectiveness due to the attack. Using an offline analysis, each IT asset is subject to the same set of possible cyber effects, for the same potential durations. CMIA's approach has two main limitations. The biggest one is that it is not able to assess cascading effects (when multiple attacks leverage their individual effects). The other weakness is its offline mode, which makes it difficult to be used to prioritize resources during the execution of the mission. An important contribution of CMIA is that it shows the need to map IT resources and the mission tasks; nevertheless, Musman does not describe how to do it.

The second set of frameworks / methodologies have their focus on performing real-time mission analysis. A consistent framework is the *Topological Vulnerability Analysis (TVA)* [12]. TVA uses the graph attack method to model vulnerabilities, and how they can be explored, and presents it in a strong visualization. This enables an analyst to use it to evaluate the cyber impact in real-time scenarios. An implementation of this framework is given by *Cauldron* [13]. Cauldron uses a set of different data sources; correlates their information in an attack path and builds a rich visualization. One of the contributions in this approach is the group of techniques that he uses to reduce the graph complexity to enable its use in real-time analysis [13, 14]. Usually a small set of vulnerabilities generates large complex graphs that make it extremely hard to develop any analysis. In his last work [13],

Cauldron contextualizes the attack graph and the mission tasks, using a workflow to perform this task. The TVA's main limitation is its attack graph orientation. If the analyst does not map attack paths or any other failure situations, the model does not provide an answer.

The output of TVA is a graph that represents the current situation and the possible attack paths that can be performed. In general, the approach cannot provide any probabilistic prediction. However, this approach can be complemented by the *Future Situation and Impact Awareness (FuSIA)* [15] method. FuSIA generates future situations in a given environment using ontology. This ontology models the relationships between objects and activities.

Other approach that incorporates concepts related to uncertainty to assess the impact of cyber-attacks in real time scenario is the *Impact-Oriented Cyber Attack Model* [16]. An important contribution in this methodology is that it uses a workflow to model missions and integrates the infrastructure with it through a service concept; this starts to answer, in a general way, the mapping between mission and IT, complementing other studies were developed [10,11].

Jacobson [17] makes a general comment about the IT x mission map, but does not show any method or directions to realize a solution to this task. However, his model defines mission, and its relation with IT environment, simplifying the understanding how the mapping between these two components are realized.

In other work, *CAMUS: Automatically Mapping Cyber Assets to Missions and Users* [18], presents a specific and detailed approach to make this mapping from mission to IT infrastructure. CAMUS provides situation management through developing an automated mapping of Cyber Assets to Missions and Users, which increases the accuracy and efficiency of cyber incident mission impact assessment. The problem in this approach is his mission concept, which is based on the high level organization behaviors, so it is not possible to apply CAMUS in real-time tactical missions.

The related works presented are a representative subset of current research related to evaluation of the impact of cyber threats, and can thus support the claim that the research problem remains unsolved. In summary, each approach suffers from at least one of the two issues that can be singled out as the main causes for this situation. The first is the lack of a correlation between the required components to the impact assessment, the mission and its supporting infrastructure. The second cause for failures is the inability to provide continuous analysis of these two components and their interactions. The proposed architecture addresses both, with a unique combination of technologies and simulation, which we explain in this paper.

3. Scenario

In an operational environment, the need of information at all levels is a critical issue and should be exchanged quickly between all levels in a Command and Control Centers (C2C)

(Figure 2), enabling Commanders to practice their responsibilities. This work uses two distinct streams: horizontal and vertical information flows.

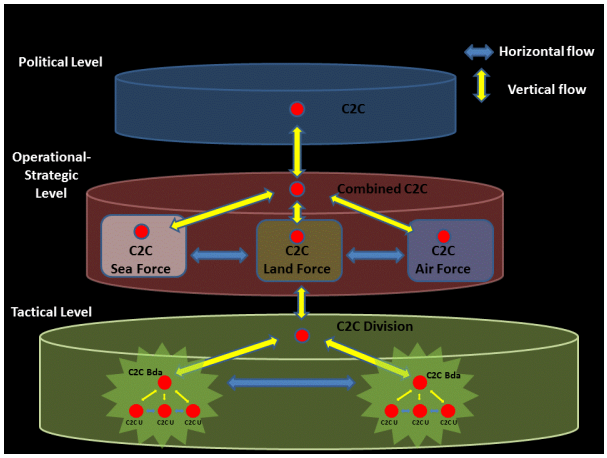

Figure 2 - Flow of Information

The horizontal flow is the data exchange between elements of the same level of command. The vertical flow is performed by communication of elements at different levels.

The Land Battle Scenario, that we will present, depicts ordinary situations of data exchange, designed based on the experience of the authors. The goal is to generalize the situations and not focus on military strategies of a particular country. Note also, that the emphasis will be given to the land force.

In this paper to illustrate the method we present only the following tactical level scenario:

The *Recognition Soldier* (***R Sd***) moves 20 miles in front of the platoon and verifies the presence of enemy troops (Figure 3). To provide information to his Commander, he uses a *Personal Digital Assistant (PDAs)* device to take photos, makes notes about the enemy platoon, their equipment, firepower and copies all the information gathered as well as the geographical location of his GPS device. The soldier finishes the message requesting guidance from his immediate commander. PDA transmits the information by Bluetooth to the soldier portable radio, using pulses (data packets), VHF modulation, to the vehicular radio of the squadron commander (vertical flow of information).

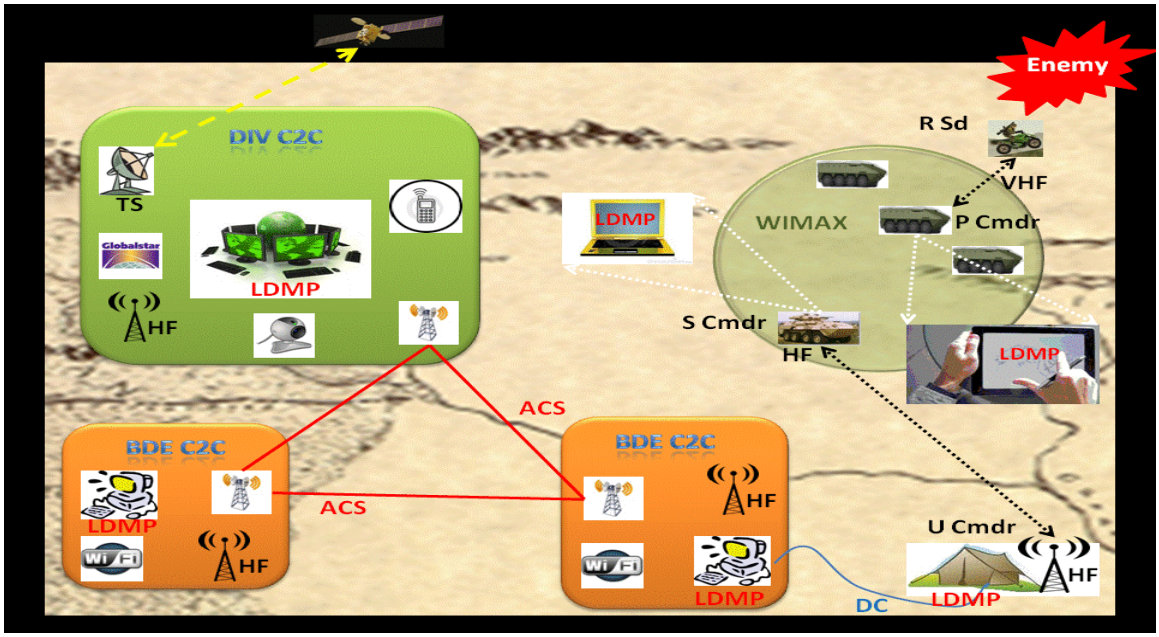

Figure 3 - Tactical Level Scenario

The *Platoon Commander* (***P Cmdr***) receives the message from the soldier in his *Land Data Management Program (LDMP)*, installed in his tablet, which has a Bluetooth connection with the armored vehicle radio. He answers the soldiers` questions by text message and warns the other members of the platoon about enemy presence. After that, the *Platoon Commander* uses the WIMAX network of the armored vehicle to transmit its information about the enemy to the *Squadron Commander* (vertical flow of information).

The *Squadron Commander* (***S Cmdr***), receives information in LDMP installed in his laptop (Command and Control Center Advanced), analyzes the situation (OODA cycle), responds to the ***P Cmdr*** and transmits his guidelines, using an IP telephone and an WIMAX network for the entire platoon, sending photos taken by the soldier, the enemy's data and location. He uses the same infrastructure to transmit a text message (enemy position) to all squadron commanders who are in the first echelon (horizontal flow data). And, through an HF Crypto connection (broadcast of encrypted data); the squadron commander contacts the regiment commander (dataflow vertical) transmitting the information of the enemy, informing his decisions and requesting immediate orientation (figure 3).

The ***Unit Commander*** (*U Cmdr*), receives all information, processes the data (filtering key information) in LDMP, that exists on the whole regiment network, and via data cable (DC) communicates with the *Brigade General Commander*, informing the enemy presence and actions to be taken (figure 3).

The Operations Officer, who is the Generals Assistant, receives all the information (text, photos and location), traces the possible courses of action in LDMP and transmits the possible actions via internal data network (Wi-Fi), from the ***Brigade Command and Control Center*** (*Bde C2C*). The *Brigade Commander (Bde Cmdr)* analyzes the situation, querys intelligence data, and identifies the necessity of more information about the terrain and the enemy. To accomplish this task, a recognition flight mission is requested to the echelon immediately above. The Operation Officer prepares the order in the LDMP and sends the current situation and calls for air support, via ***Area Communications System*** (*ACS*) or HF crypto-radio equipment as an alternative way, to the echelon immediately above his (Figure 3).

The upper echelon commander at the Division Command and Control Center (Div C2C), receives the order, gets situational awareness and studies the probability of action to create a diplomatic incident with the Neighbor Country.

Using the *ACS*, he reports the situation with other brigades and, by satellite links provided by Transportable Station (TS), requests a videoconference with the strategic level (Figure 3). For this connection, the Globalstar System can also be used (an alternative path).

In summary, the amount of data and connection possibilities are extremely large. It is essential that there exist alternative routes for data flow (vertical and horizontal). In a connection, what changes are the technology used and the means of data transmission. However, it is essential that the routing be as quick as possible and that priority messages reach the final address as soon as possible. The goal is to provide a quick and reliable flow of data to give feedback to commanders and avoid negative consequences.

In the next section we present the information technology infrastructure needed to support this scenario.

4. Infrastructure of Information Technology (IT)

To support the scenario discussed above, an infrastructure is required. This infrastructure should provide support for the flow of information between the members of the network and its systems.

To meet this need, a variety of IT assets, which include: hubs, switches, servers, firewalls, cables, computer equipment, and hosts, are composed to form distinct integrated networks. Figure 4 shows a basic infrastructure that supports the lower levels of this scenario.

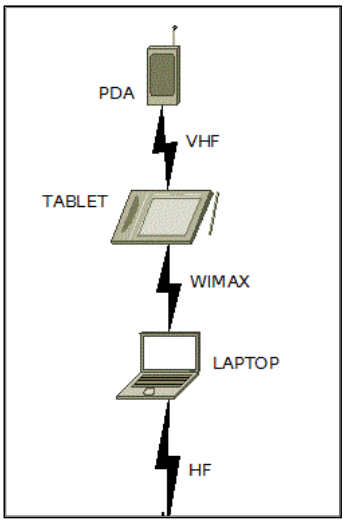

Figure 4 - IT infrastructure

To simplify the model, this work does not consider connections between the PDA and the Bluetooth's radio in the soldier's equipment. Similarly, equipment such as the P Cmdr (tablet) and S Cmdr (laptop) also do not have more details. The fact that we have simplified the assets of these actors will facilitate in future analysis, when we will discuss the architecture of the Cyber Defense Simulator. The HF radio communication in Figure 4 connects the infrastructure of the IT Unit in Figure 5.

Figure 5 shows an antenna, which enables connections between Units and Squadrons, connected to a modem. The modem is connected to the rectangle labeled with the acronym DMZ (DeMilitarized Zone). DMZ has military origins, meaning a space between two territories that are in conflict. Although, in our case, we do not have conflict areas but the DMZ and firewall is used to represent the concept of separation of the Military IT Units.

Therefore, the DMZ with firewall, and all other services, that have external access (vertical or horizontal information flow) are considered "separated" from the Unit's net. The goal is to limit or deny possible damage from a cyber-attack that has already occurred, for example, in the soldier's equipment.

The Unit's firewall connects a basic server (supporting the function of the LDMP); a Local area network (containing computers to perform some tasks such as artillery, logistics, engineering, and command; a cloud with other assets; and a connection via switch, with the Brigade (vertical information flow) using a physical medium (data cable).

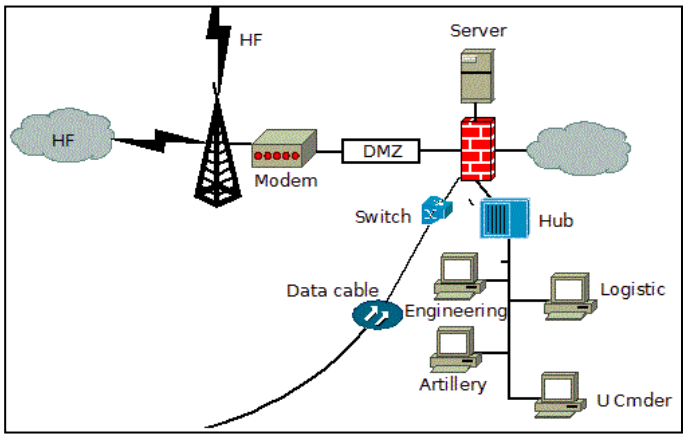

Figure 5 - IT Infrastructure at the Unit level

Finally, to provide mobility to the Unit, the topology shown above has considerable simplicity.

In the following text, we will analyze the infrastructure to the Brigade level. Figure 6 presents a light infrastructure for the Brigade level since, at this level we need to have conditions to receive and manage the large volume of information that flows from the levels below (Units, Squads, and Platoons).

The network topology at the Brigade level has a firewall and a server, which have goals similar the the Unit level; a router to manage the various existing assets; one or more databases for storage, management and retrieval of information; and some LANs required to coordinate logistics, operational tasks, and other activities.

Finally, this paper proposes two more possibilities for the network connection of the Brigade headquarters. Both are represented with radio links. The first, uses the Area Communications System (ACS) to connect the network under investigation with other Brigades (horizontal flow of information) or to link to the Divisional network (vertical flow of information). The second possibility is to use the HF radio link to make the same type of connections (horizontal and vertical). The importance of this redundancy will be more easily identified when submitting the entire infrastructure to cyber-attacks and analyzing the consequences of these attacks for the tactical scenario.

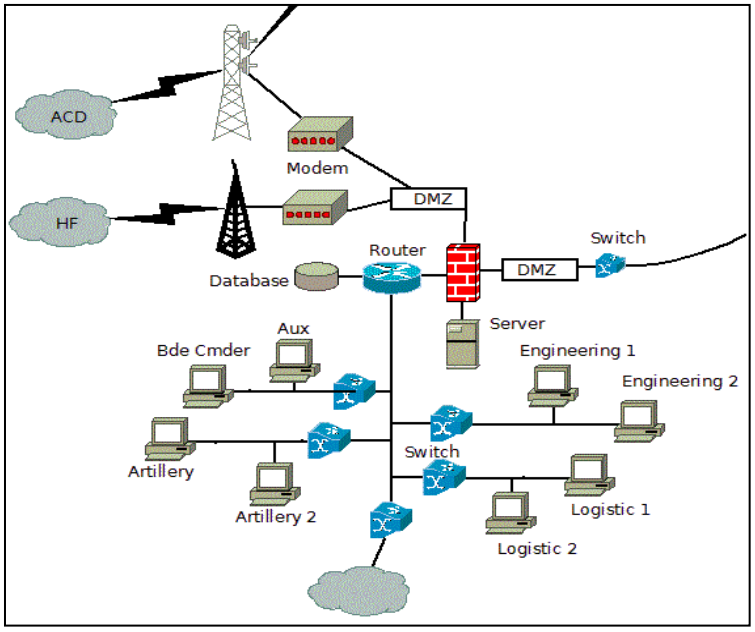

Figure 6 – IT Infrastructure at the Brigade level

Concluding this section, figure 7 presents the Divisional infrastructure. In this configuration, besides the assets already identified above, we have a greater amount of LANs and computers. As in the Brigade Network, there are a large number of computers and more than one device may be used to achieve the same operation (e.g. Logistics 1, 2, 3). The intention is to highlight the growth of information flows within each activity (artillery, logistics, and engineering).

The design of this network needs to support a large amount of data flows and the high relevance of authority in this level. To fulfill this requirement, the network has multiple redundant paths, represented by cell phone, Globalstar system, and satellite links (horizontal and vertical links).

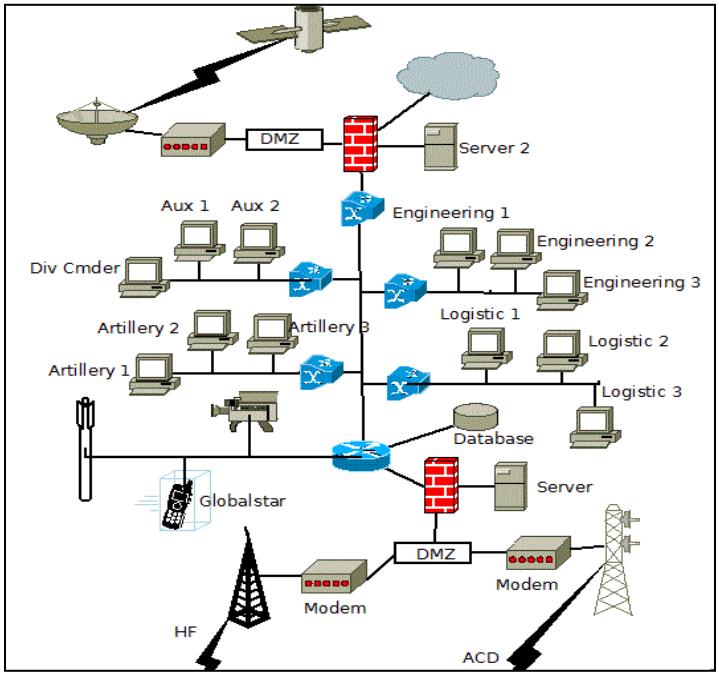

Figure 7 – Divisional IT Infrastructure

The assets and topology in this section serve only to illustrate and support the previous section. Like the scenario described in section 3, the infrastructure presented does not reflect the reality of a specific military force. The intention is to prepare environments that can be loaded into the kinetic and cybernetic simulators and thus allow the analysis of the architecture proposed in the next section.

5. Architecture of a Cyber Defense Simulator

The proposed architecture uses the framework presented in [19] to provide a new approach to the suggested work, which aims to unite kinetic environments with cyber environments to discover how an event in the cyber domain can affect a process executed in a physical domain.

In this section, we will propose an architecture for a Cyber Defense Simulator which combines kinetic and cyber simulated environments. The intention is to provide a way to identify how these two environments are related and how attacks in one may impact the other.

Figure 8 synthesizes the proposed architecture. The box located to the left of the figure, with the acronyms LDMP (Land Data Management Program), refers to the program used to coordinate tactical actions.

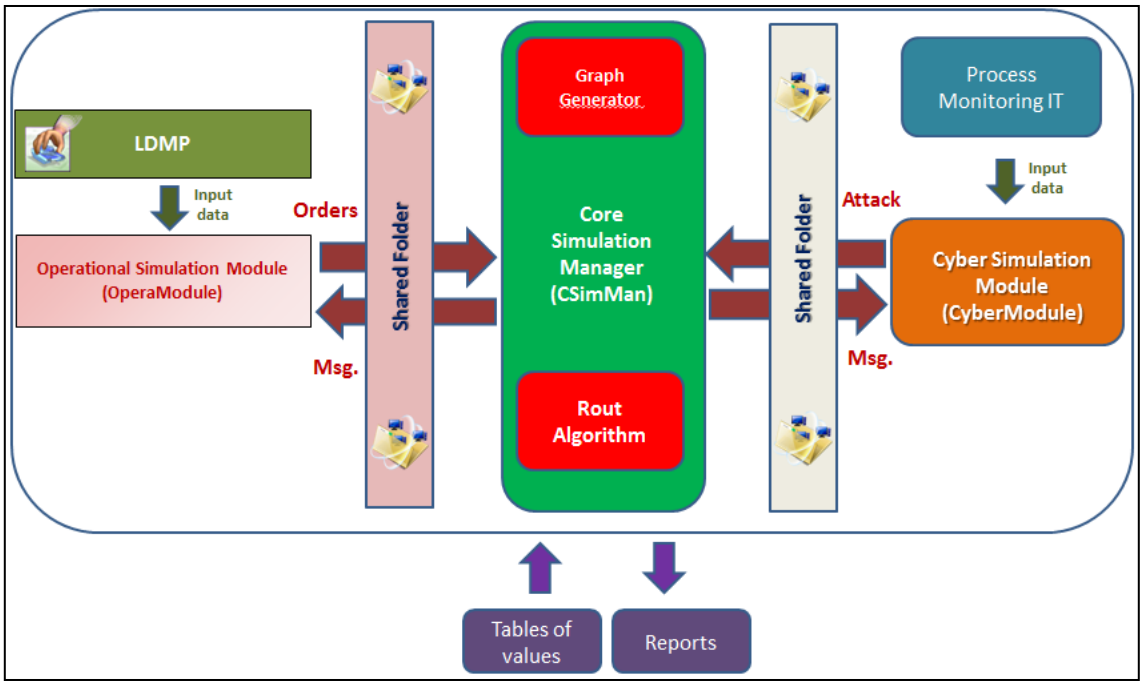

Figure 8 – Architecture

Thus, LDMP has the tactical information about the organization of the deployed troops in the field and will be used to load this data into the Operations Simulator Module (OperaModule).

The OperaModule receives data from LDMP, which contains the information about organization of tactical troops, and proceeds to identify the employed troops in the military action, their geographic positions, effectiveness, materials and vehicles. Consequently, the OperaModule provides the possibility of simulating missions and showing the consequences of actions or orders.

By further analysis of figure 8, we identify two Shared Folder boxes. The one on the left side carries the connection between the OperaModule and the Core Simulation Manager (CSimMan). The box on the right side has the purpose of enabling the integration between CSimMan and Cyber Simulation Module (CyberModule).

In this context, one may note that CSimMan is the core of the proposed architecture, within which interactions between the cyber and kinetic environments take place. However, in order to accomplish such interactions we still need to get data from the cyber environment, which is shown at the right side of the architecture in by Figure 8.

Still considering the right side of the Figure 8, one may find the box labeled Process Monitoring IT. Through this box, which has a real IT network, IT assets and a network

topology, are identified. This process becomes viable, as it is an accessible network and through sensors (hardware or software) the infrastructure can be monitored.

After scanning the network, the network status data is entered into the Cyber Simulation Module (CyberModule). This box is then able to simulate a cyber-environment. Depending on the simulator it is possible to identify vulnerabilities on IT assets and deliver cyber-attacks.

Thus, using kinetic data, simulated in OperaModule, and cyber data, simulated in CyberModule, we can unite both of these data in the CSimMan environment and identify possible consequences of both scenarios.

Essentially, the CSimMan builds a graph based on the data network from the CyberModule. The edges of the mentioned graph are the connection means between the assets (nodes). In this instance: data cables, wireless networks, wimax, wireless connections are the edges while computers, tablets and laptops, are nodes (vertices). In this graph, nodes are assets that can be attacked.

The graph's edges are parameterized by weights, which are proportional to the communication resources used to connect two assets (adjacent nodes). Thus, for example, if one edge is a data cable and the other one is a radio link, they will have different weights. This measure is intended to differentiate the traffic capacity of the different communication paths. Tables that link these weights to the transmission rates are kept in CSimMan. This input data is represented in Figure 8 by box "Tables of values", located below CSimMan.

Based on the considered scenario, the above mentioned table could be built according to the data given in Table 1.

The weight of the edge will enable, or not, the flow of information depending on the capacity of the communication resources. Thus, the table 2 lists the type of information flow and minimum requirements.

Communications resources	Weight (capacity) of the edge
VHF radio	1
Wimax	3
HF radio	2
Data cable	6
ACS	4
Satellite	5

Table 1 - Weights (capacity) of Edges

Type of Information	Minimum weight edge
Chat (text)	1
Document (text)	2
Images (low resolution)	1
Images (high resolution)	3
IP Voice	2
Video	4

Table 2 - Minimum Weight Edge

Besides the links, the assets can also influence the amount and kind of information processing carried out. However, for study purposes, we consider that all analyzed assets support any sort of information. For example, the soldier's PDA supports communication flows from basic transmission of text up to video conference, but the link (edge weight) must be present to support this service.

From the built graph, we get the logical paths in which the information is forced to flow. These logical paths are built from the information of the two simulators (kinetic and cybernetic). The OperaModule identifies who sent and who should receive certain information. The CyberModule identifies the infrastructure that may be used to connect the transmitter to the receiver.

Thus, an information lifecycle can be defined for each communication stream (Figure 9) consisting of the stream's start (request or task order), a path-way, the recipient (who is performing the work or service), and the information's return.

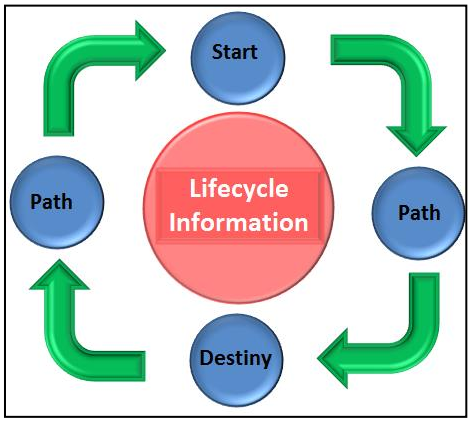

Figure 9 – Lifecycle of Information in a Communication Stream

In order to complete the communication task, it is necessary to pass through the entire lifecycle. If, by chance, the information arrives at the destination and does not return to the requestor, the logical path is not completed, and the information is not processed.

The information path is determined by the junction of the kinetic and cybernetic environments. Briefly, the kinetic environment identifies the START and the DESTINATION while the cyber environment indicates the PATH.

When there is more than one possible path (with consistent nodes and edges), the searching algorithm used in CSimMan will choose the shortest path, reducing the path information and thus, decreasing the possibility of cyber-attacks. For this statement, we are assuming that every node have the same probability of an attack.

In summary, the cyber-actions take place in the CyberModule and affect the CSimMan graph (specifically the nodes). As the missions generated in OperaModule can only be performed if supported by the flow of information resources, which occurs in the graph, it generates a dependency between the kinetic and cyber environments. That is an action only occurs in the kinetics environment if the cyber environment allows the enabling communications to occur. In addition, kinetic action on the environment may also cause changes in cyber environment, which makes the proposed architecture more complete and interesting.

Finally, in order to illustrate the working of the proposed architecture, the next section will present an evaluation framework based on the scenarios and the infrastructure built in the previous sections.

6. Architecture Assessment

The scenario and infrastructure proposed in the previous sections was used to evaluate the proposed architecture in terms of proof of concept.

The LDMP loads the kinetic simulator scenario (*OperaModule*) and cyber simulator (*CyberModule*) is loaded, through scanning the network for its current status.

After the *CyberModule* retrieves all the information required from infrastructure, *CSimMan* builds a graph that represents the infrastructure status (Figure 10), and the environment is ready to evaluate any mission scenario.

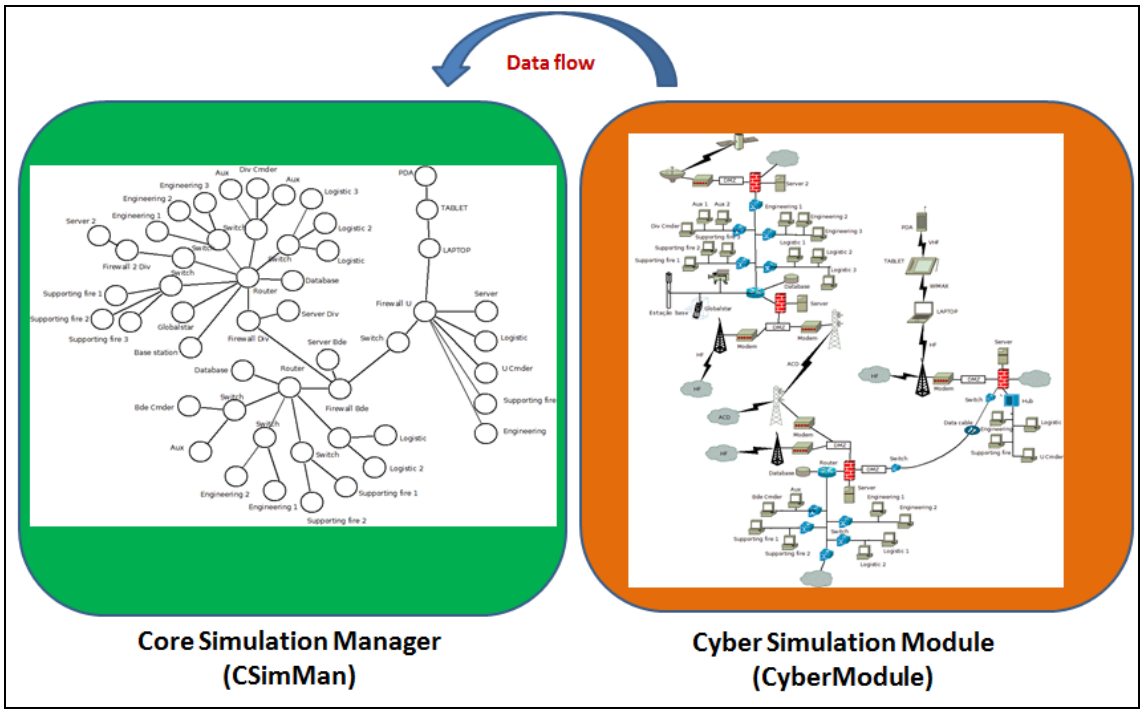

Figure 10 - Build the graph

With data loaded, we're ready for evaluation. We will present three case studies:

6.1 Case Study 1 - Evaluation without cyber-attack

The Platoon Commander (P Cmdr), that received information about the enemy, requests permission to attack. The request is sent to the Squadron Commander (S Cmdr), who answers that he cannot authorize the attack and will query the Unit Commander (U Cmdr).

All data (P Cmdr request, response of S Cmdr and the new information flow to the U Cmdr) are generated using *OperaModule* while the CSimMan generates the path of this information (Figure 11).

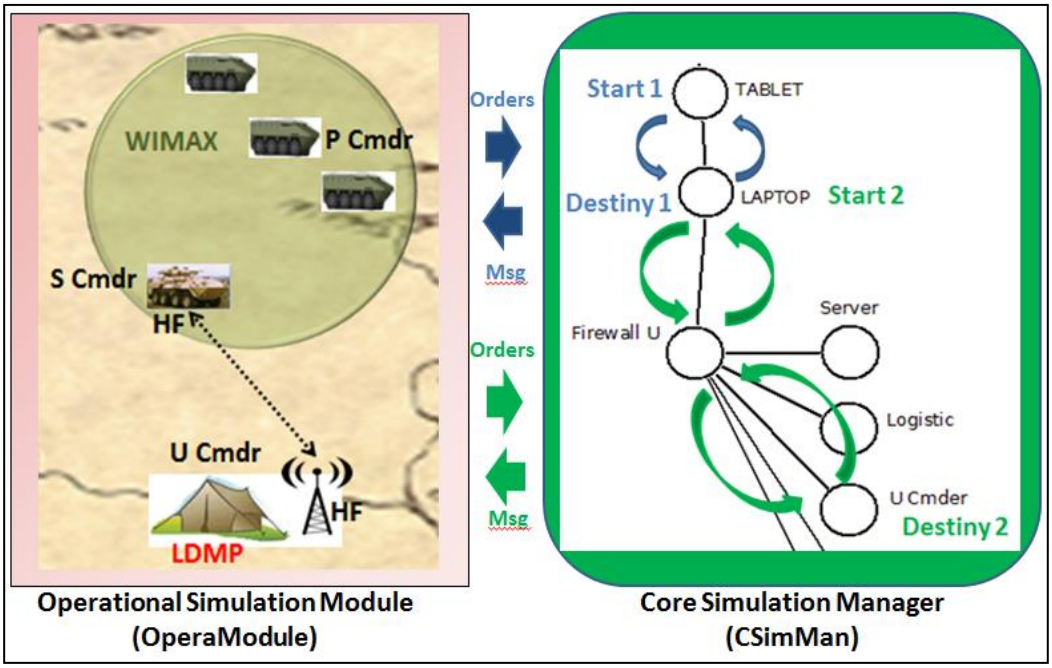

Figure 11 – Case Study 1 - Data flow between OperaModule and CSimMan

In this case, two life cycles can be identified by different colors. The *OperaModule* makes a request from P Cmdr to S Cmdr and sends this order by an interface (not shown in the figure above) to *CSimMan.* *CSimMan* conducts the data flow (round trip) from START 1 until the DESTINY 1. The S Cmdr's answering message to the P Cmdr came back to *OperaModule*, and first cycle life ends. However, the S Cmdr decides to consult the U Cmdr and a new order is sent to the CSimMan containing a START 2 and DESTINY 2.

In this case study there are no cyber-attacks and the information is transmitted, received and processed without problems.

6.2 Case Study 2 - Evaluation with cyber attack

The *CyberModule* analyzes the data and identifies network vulnerabilities on a Brigade switch. For this reason, the switch is chosen to become a denial of service attack target (wherein the node is overwhelmed with input data and cannot respond to valid service requests). The way this attack is performed is irrelevant to the current study. It may be an internal enemy using a USB stick or an external attacker. To finalize this process, CSimMan reports all information from this situation (see figure 12).

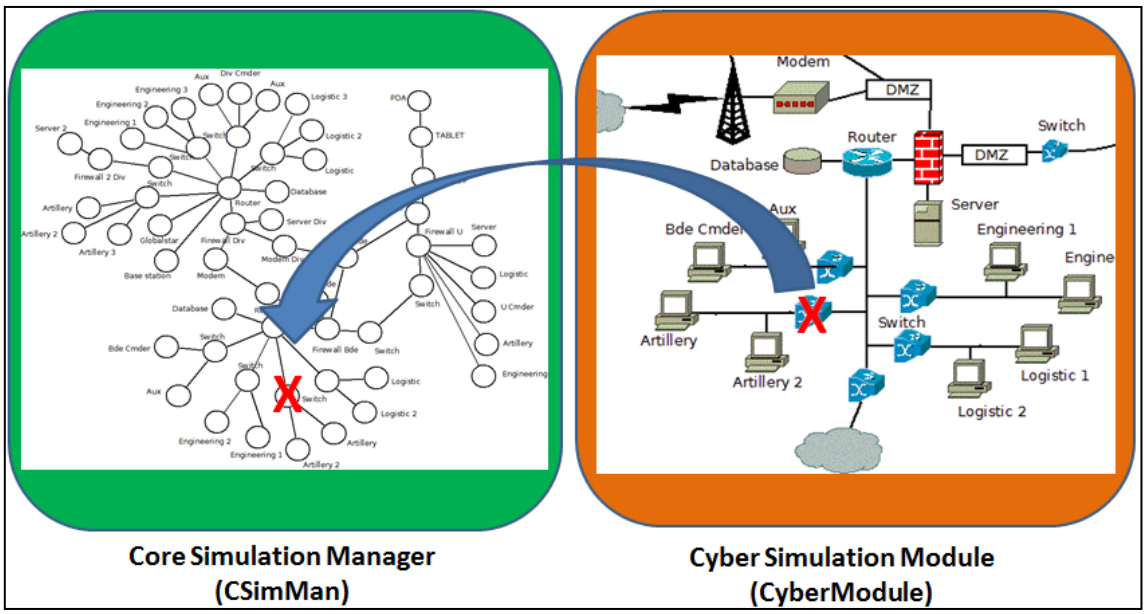

Figure 12 – Case Study 2 - Data flow between CyberModule and CSimMan

Before the environment recovers his normal condition, U Cmdr receives a new mission. The unit must attack the enemy identified. To fulfill this mission, U Cmdr decides to ask a Brigade artillery support in sustenance of its mission attack. Thus, one information flow is generated (figure 13).

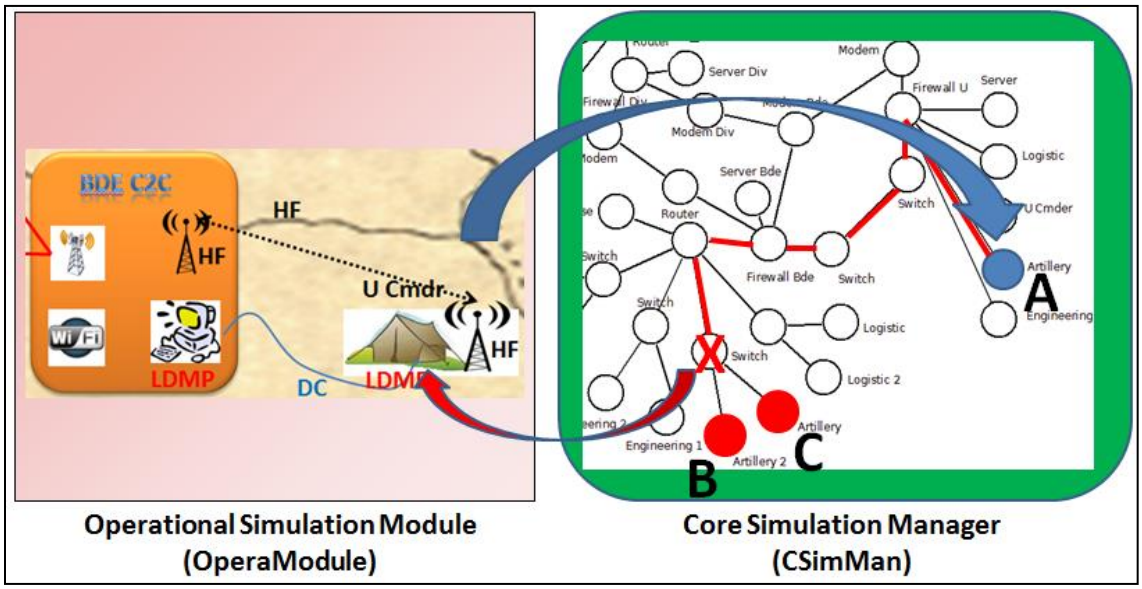

Figure 13 – Case Study 2 - Data flow between OperaModule and CSimMan

In the *CSimMan* graph in Figure 13, the node labeled with the letter "A" needs to have a clear path to the node "B" or "C", without it the request artillery support is not performed. However, due to the attack the node that has an "X" does not allow the path information in graph and the lifecycle of the information are not complete.

This data (information interrupted) is transferred to *OperaModule*, which does not allow the request for artillery support. The future consequences of this lack of support may be a delay in the attack mission to the enemy or even mean the loss of the Unit (destroyed by the enemy). Note that the result is not generated by *CSimMan*, but in *OperaModule*. It happens because it is *OperaModule* that has all kinetic data about the entities that will be in conflict (military Unit and the enemy).

In this situation, to emphasize the consequences of cyber-attack, we can generate a simulation without cyber-attack (request artillery support performed) and another with the cyber-attack (without artillery support). The comparison of the results will be coordinated by CSimMan, which generates a final report.

Note that *OperaModule* provides kinetic simulations and *CyberModule* vulnerability analysis and cyber-attack.

6.3 Case Study 3 - Evaluation with cyber attack

In this evaluation, the *CyberModule* analyzes the data network, identifies vulnerabilities in the Unit's switch and performs a denial of service. Following in *OperaModule*, Div Cmdr makes an order to the Bde Cmdr to do a video conference with the U Cmdr, starting this information flow through the graph (Figure 14).

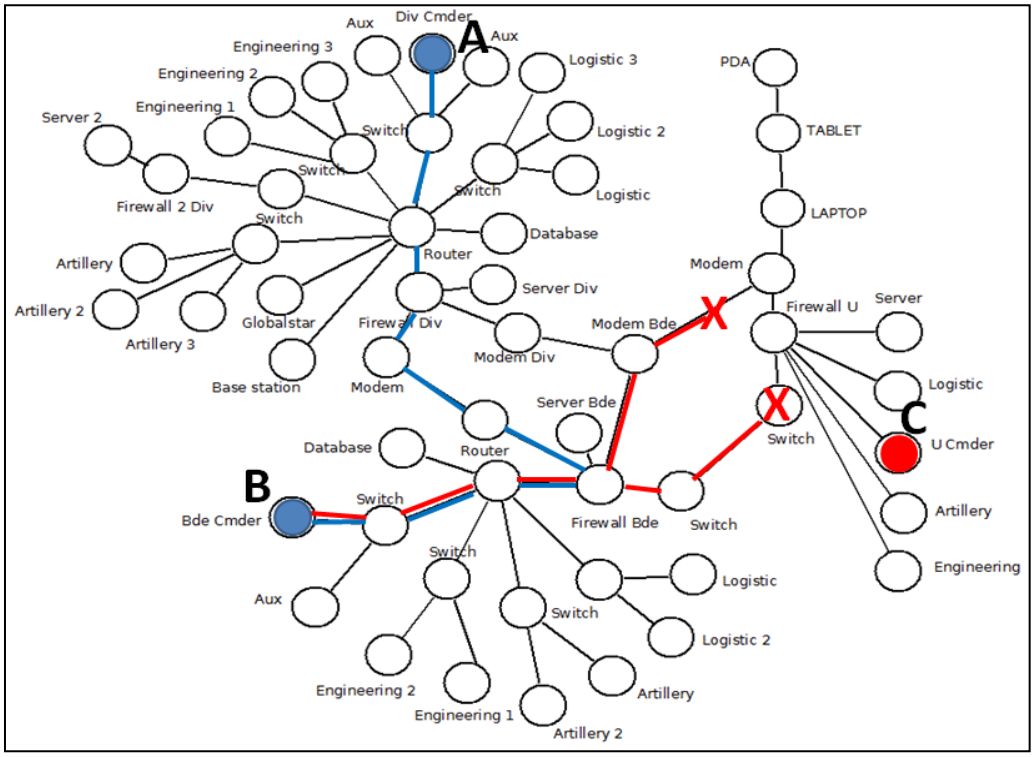

Figure 14 – Case Study 3 with stopped path in the CSimMan graph

When the figure above is analyzed, two streams of information are perceived. The first starts at node "A" (Div Cmdr) and ends at node "B" (Bde Cmdr) successfully. However, the

second flow of information does not have any way to get to the node "C" (U Cmdr). The "X" (under the edge) identifies that this edge has no weight (capacity) sufficient to support the requested service (videoconferencing) and "X", under the node, identifies that this was attacked. This information is sent to the *OperaModule* and, as a result of the attack, the Div Cmdr is not able to conduct a videoconference with U Cmdr. The result of this lack of communication may be the most varied possible, depending on the context of the situation but in any event causes a delay in the force's conduct of the mission.

Final Remarks

The study of the cyber world and its complexity has become an important topic in military science. The use of automated tools can help commanders to make more accurate decisions. Within this context, simulators can be used to provide a picture of both the kinetic and cyber environments. However, approaches that fuse these two domains are new and incipient.

This paper proposes an architecture that is able to jointly simulate cyber and kinetic environments. In this sense, our contribution is a new way to accomplish this interaction. An advantages of this approach are the possibility to update the scenarios in real-time, the generation of attack-graphs without the identification of cyber-attacks, the operation under multiple attacks, and the possible identification of the consequences of cyber-attacks in the kinetic and cyber environment.

To show it, a tactical scenario for military land operations was analyzed. In this environment the Command and Control (C2) increases its importance, while it is complicated by the mobility of the military units, which causes constant changes in infrastructure. The decision to shift troops or their possible destruction by the enemy causes changes in the data network and directly affects the flow of information, which could make impracticable military actions.

The way that a cyber-attack is conducted is not the focus of this work. Once you have identified that there is vulnerability in a certain asset of Information Technology (IT), we want to identify what is the importance of that infrastructure for the mission. With this information, commanders can manage the problems, plan future actions and decisions involving kinetic and cyber environments.

The proposed architecture allows for the identification of which IT assets are most important to a particular mission, intends to builds the possible paths of information flow in graph form, supports sequential effects (changes in the attacks and infrastructure), compares missions (with and without cyber-attack), can be constantly updated, and aims to portray the reality of military actions.

To accomplish these activities, the suggested model has a great dependence on the simulators used. The power of realism provided by the architecture depends on the refresh rate of the kinetic data. As well as the power analysis of the vulnerabilities of infrastructure, the form of cyber-attacks predicted depends on the cyber simulator.

This article presented only denial of service attacks, but other types of attacks can also be implemented influencing the integrity and the confidentiality of information. For this, relationship tables need to be constructed and probabilistic algorithms need to be implemented.

As a final consideration, we emphasize that the proposed model can also be used in military training. With this objective, the kinetic simulator should be replaced by a training simulator, where the actions take place only by order of the participants of the "game".

Acknowledgment

The authors would like to thank the staff of the laboratory of Command and Control, Operational Applications Postgraduate Program, Instituto Tecnológico de Aeronáutica (ITA); and the Core of Cyber Defense Center.

References

[1] King, M. (2002) Security Lifecycle – Managing the threat. SANS Institute.

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

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

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

[5] Thiem ,L. "A Study to Determine Damage Assessment Methods or Models on Air Force networks," Department of Engineering and Management, Air Force Institute of Technology, Wright Patterson Air Force Base, OH, 2005.

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

[7] Schneier, B. (1999). Attack trees: Modeling security threats. December 1999. Dr. Dobb's journal.

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

[9] D.L. Buckshaw, G. S. Parnell, W.L. Unkenholz, D.L. Parks, J.M. Wallner, and O. S. Saydjari. "Mission Oriented Risk and Design Analysis of Critical Information Systems.", Military Operations Research, v10 N2 2005.

[10] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, "A systems engineering approach for crown jewels estimation and mission assurance decision making."

Computational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on, vol., no., pp.210-216, 11-15 April 2011 doi: 10.1109/CICYBS.2011.5949403.URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5949403&isnumber=5949383.

[11] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, "Computing the Impact of Cyber Attacks on Complex Missions.", Systems Conference (SysCon), 2011 IEEE International , vol., no., pp.46-51, 4-7 April 2011 doi: 10.1109/SYSCON.2011.5929055 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5929055&isnumber=5929032.

[12] Sushil Jajodia, Steven Noel, "Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection, and Response," in Algorithms, Architectures, and Information Systems Security, B. Bhattacharya, S. Sur-Kolay, S. Nandy, and A. Bagchi (eds.), World Scientific Press, 2007.

[13] Sushil Jajodia, Steven Noel, Pramod Kalapa, Massimiliano Albanese, John Williams, "Cauldron: Mission-Centric Cyber Situational Awareness with Defense in Depth," 30th Military Communications Conference (MILCOM), Baltimore, Maryland, November 2011.

[14] Steven Noel, Sushil Jajodia, Lingyu Wang, Anoop Singhal, "Measuring Security Risk of Networks Using Attack Graphs," International Journal of Next-Generation Computing, Vol. 1, No. 1, July 2010.

[15] Holsopple, J.; Yang, S.J. "FuSIA: Future Situation and Impact Awareness," Information Fusion, 2008 11th International Conference on , vol., no., pp.1-8, June 30 2008-July 3 2008.

[16] Jakobson, G.; , "Extending situation modeling with inference of plausible future cyber situations," Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2011 IEEE First International Multi-Disciplinary Conference on , vol., no., pp.48-55, 22-24 Feb. 2011 doi: 10.1109/COGSIMA.2011.5753753. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5753753&isnumber=5753422.

[17] Jakobson, G.; , "Mission cyber security situation assessment using impact dependency graphs," Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on , vol., no., pp.1-8, 5-8 July 2011. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5977648&isnumber=5977431

[18] Goodall, J.R.; D'Amico, A.; Kopylec, J.K.; , "Camus: Automatically mapping Cyber Assets to Missions and Users," *Military Communications Conference, 2009. MILCOM 2009. IEEE* , vol., no., pp.1-7, 18-21 Oct. 2009. doi: 10.1109/MILCOM.2009.5380096. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5380096&isnumber=5379

[19] Barreto, A. B.; Hieb, M.; Yano, E. (2012). Developing a Complex Simulation Environment for Evaluating Cyber Attacks. Interservice /Industry Training, Simulation and Education Conference, Orlando, Fl.