19th ICCRTS

Conceptual Architecture for Obtaining Cyber Situational Awareness

Authors:

Maj André Ferreira Alves Machado

Prof. Edgar Toshiro **Yano**

Goal

- Present an architecture that helps to recognize the impacts in military operations caused by cyber-attacks, as well as present a way to identify vulnerabilities of a data network for a particular military mission. Finally, this architecture can also be used as a combat support tool for military planning.

Agenda

- Introduction
- Related Work
- Functionalities of the Architecture
  - Identification of Vulnerabilities
  - Identification of Impacts of a Cyber Attack
  - Mission Planning
- Assessment
- Final Remarks

Introduction 1/4

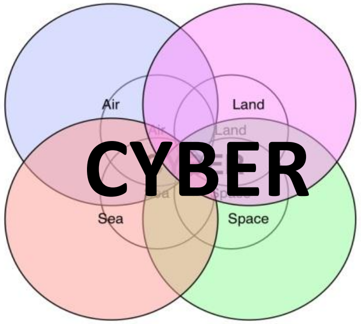
- With the growing capability of technological means and, consequently, increasing the speed of military operations, information on the battlefield has become valuable.

Introduction 2/4

- Situational Awareness (SA) of modern combat aims to meet the needs of the Command and Control (C2). In order to lead their military organizations, the commander would require concise information about his and the enemy troops.

Introduction 3/4

- The information should also be timely, because important information, that is late, loses its value. This way the agility of C2, in a Military Command Center, influences directly the power combat of a military organization.
- In this context, the study of cybernetics is extremely relevant.



Introduction 4/4

- For this reason, a military commander must know the **kinetic (tactical)** and **cybernetic** battlefields. Obtaining Situational Awareness of Cyberspace can produce significant results to **tactical** actions.

kinetic (tactical)

Cybernetic

Agenda

- Introduction
- Related Work
- Functionalities of the Architecture
  - Identification of Vulnerabilities
  - Identification of Impacts of a Cyber Attack
  - Mission Planning
- Assessment
- Final Remarks

18th ICCRTS

Architecture for Cyber Defense Simulator in Military Applications

Authors:

Maj André Ferreira Alves Machado

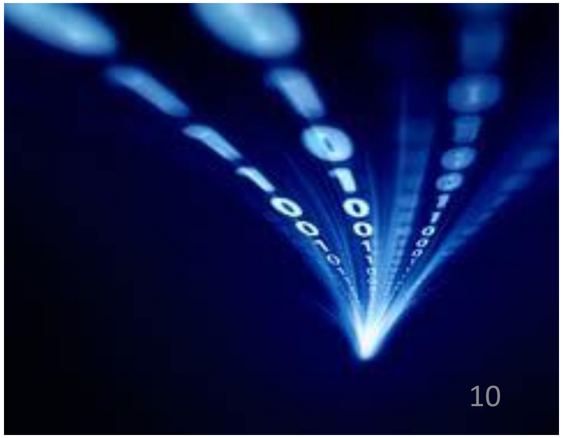
Maj Alexandre B. **Barreto**

Prof. Edgar Toshiro **Yano**

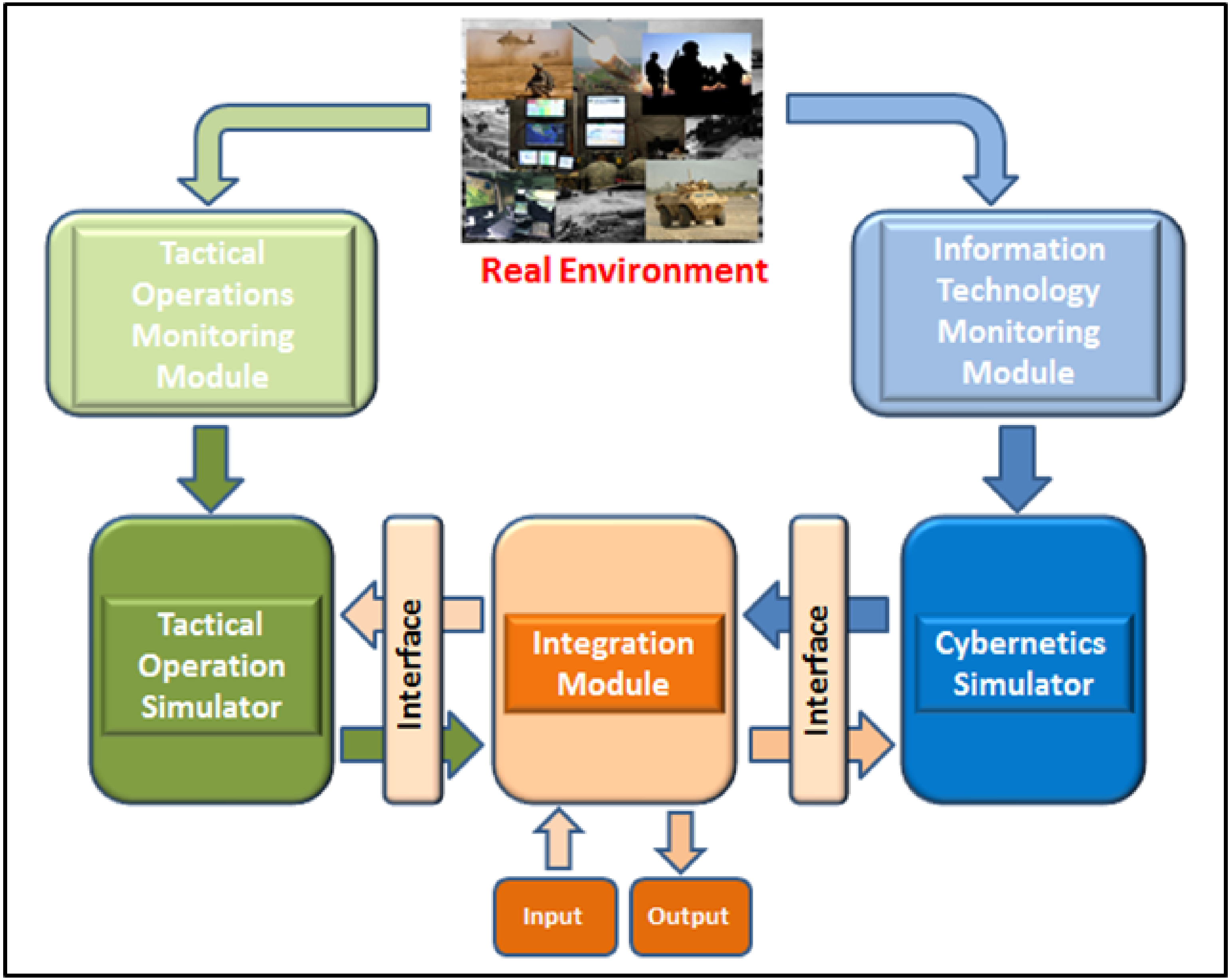
Core Idea

Any tactical event occurs only when we have an order or make a request.

So, we need a flow of information.



Architecture (overview)



Real Environment

Tactical Operations Monitoring Module

Information Technology Monitoring Module

Tactical Operation Simulator

Interface

Integration Module

Interface

Cybernetics Simulator

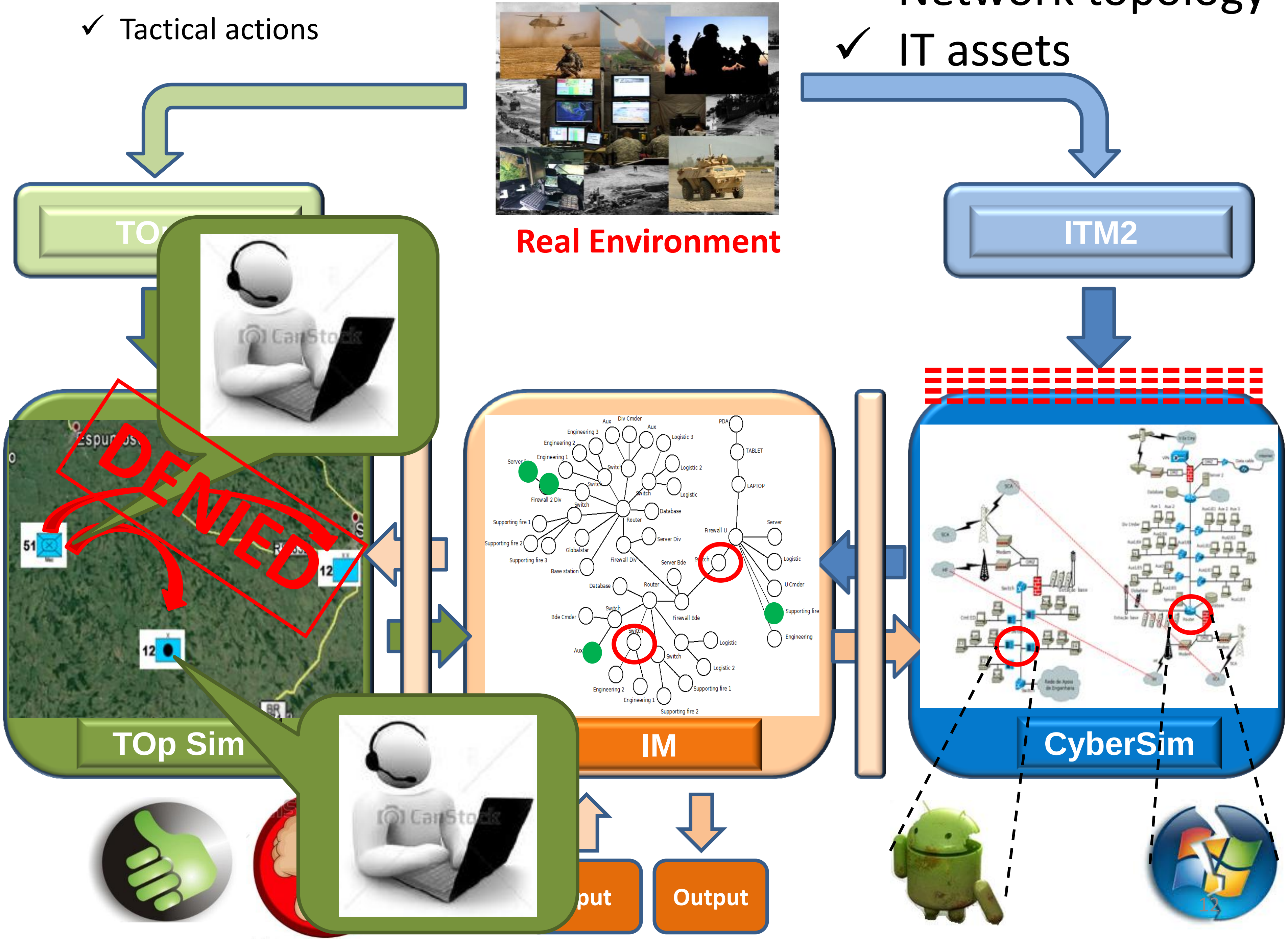
Input

Output

✓ Tactical actions

✓ Network topology

✓ IT assets



Real Environment

ITM2

TOp Sim

IM

CyberSim

put

Output

Main goal of the Architecture

Identify which vulnerabilities we have in our network.

Agenda

- Introduction
- Related Work
- **Functionalities of the Architecture**
  - Identification of Vulnerabilities
  - Identification of Impacts of a Cyber Attack
  - Mission Planning
- **Assessment**
- **Final Remarks**

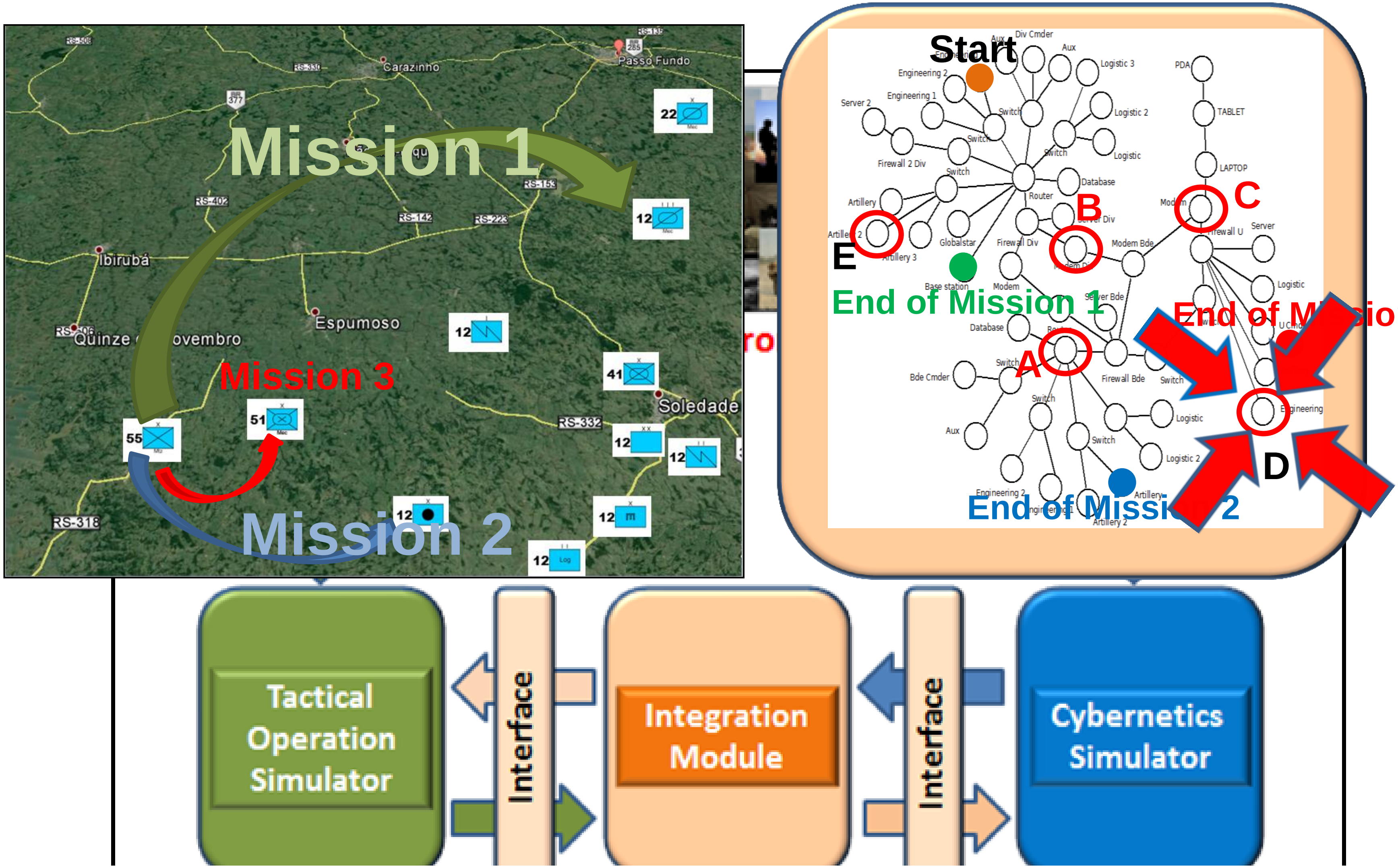
Identification of Vulnerabilities

- According to some references [10, 11, 12, 13], some cyber simulators already have the functionality to identify vulnerabilities of IT assets in a data network. But, in a large data network, or in a highly dynamic network, there may be from ten to hundreds of vulnerabilities.
- In such cases, will we have time and resources to solve all the problems, without damaging the progress of a military mission?

Identification of Vulnerabilities

- In complex data networks, we need to identify which vulnerable assets can disrupt the progress of important military tasks.
- **So, we need to Identify vulnerabilities in relation to the military mission.**

Identification of Vulnerabilities in Relation to Mission



Tactical Operation Simulator

Interface

Integration Module

Interface

Cybernetics Simulator

Mission	Type	Mission Status	Cyber Vulnerabilities
1	Attack order	Safe	-
2	Artillery Support	Unsafe	Assets A and B
3	Move order	Unsafe	Assets B and C

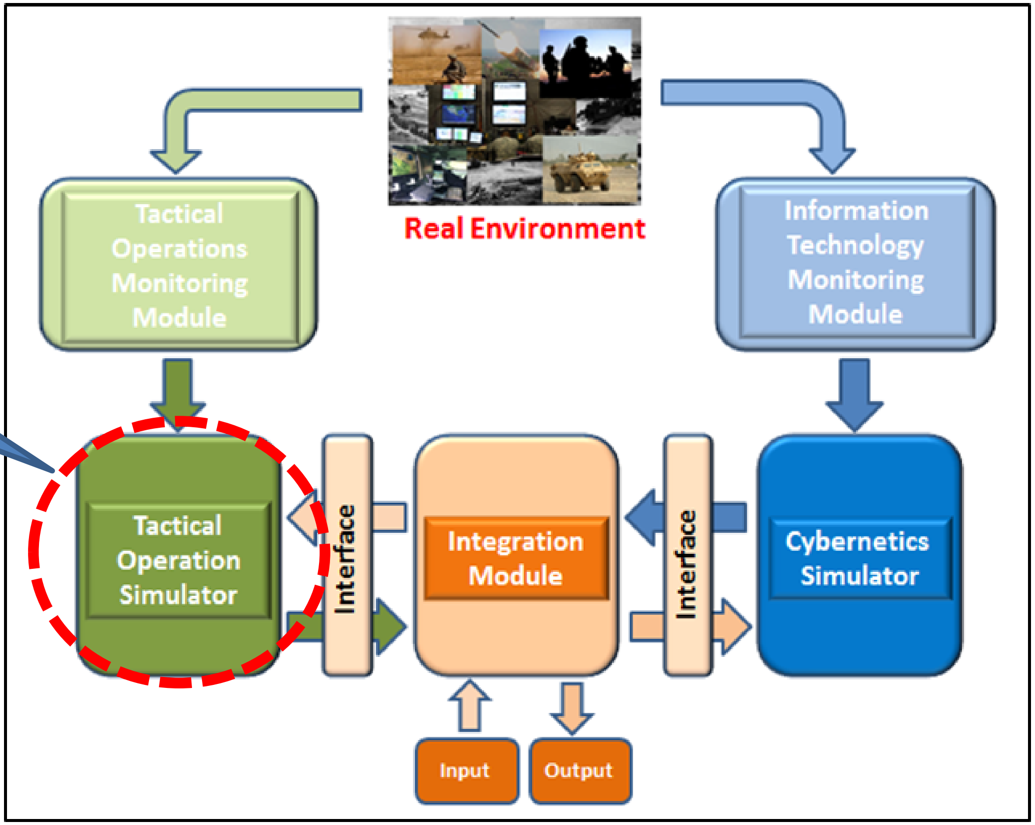
Agenda

- Introduction
- Related Work
- **Functionalities of the Architecture**
  - Identification of Vulnerabilities
  - **Identification of Impacts of a Cyber Attack**
  - **Mission Planning**
- **Assessment**
- **Final Remarks**

How are the impacts identified?

- Using the power of the simulator.

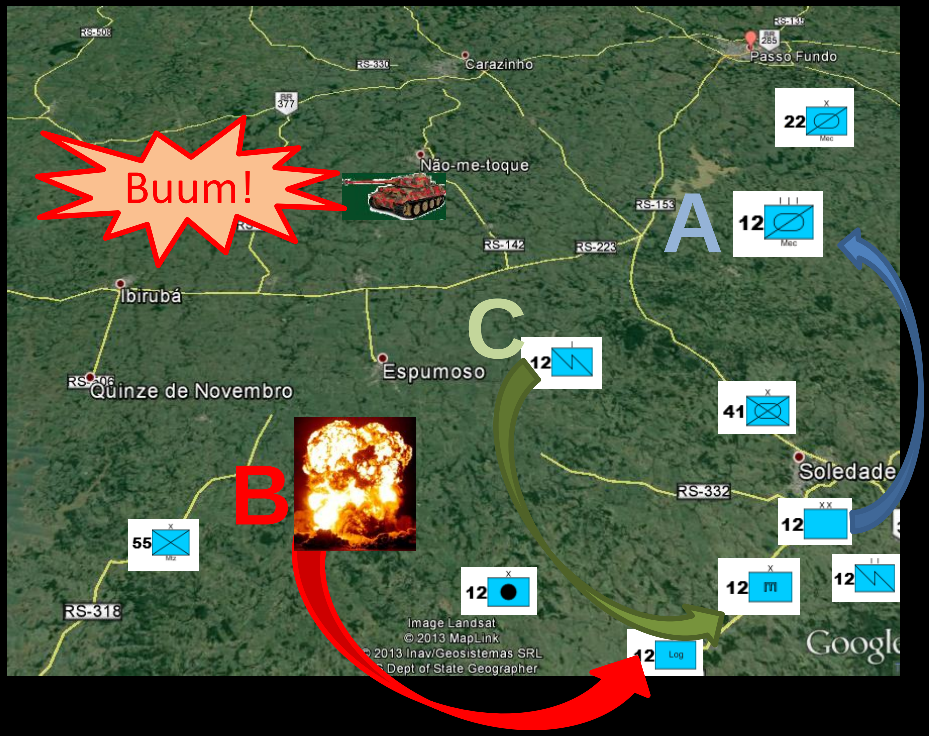
Comparing two different simulations (with and without cyber attack).

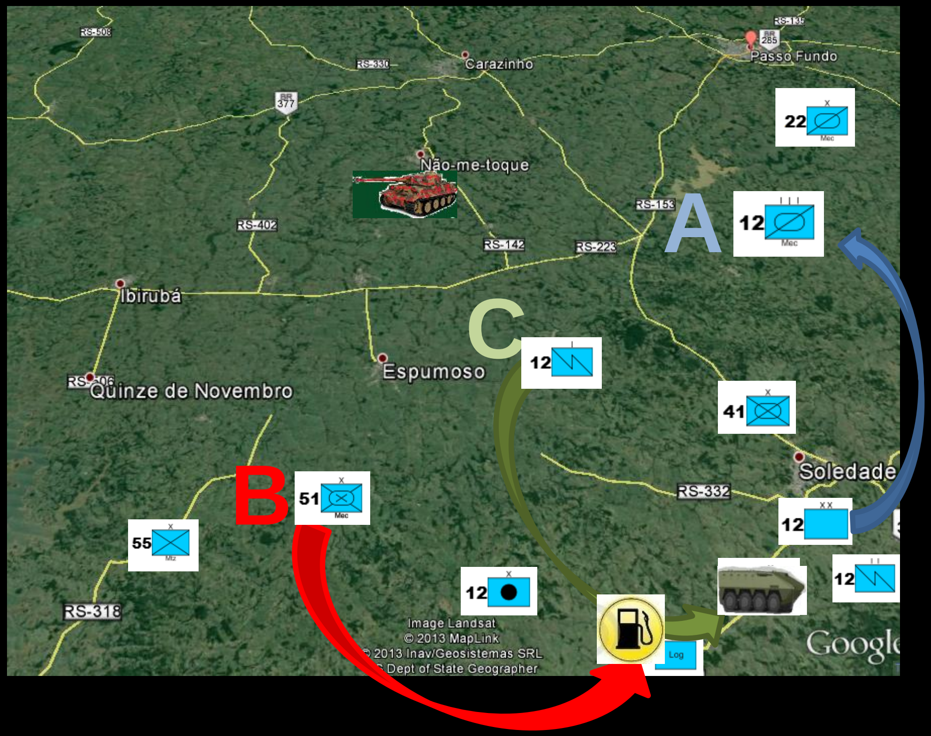

Real Environment
Tactical Operations Monitoring Module
Information Technology Monitoring Module
Tactical Operation Simulator
Interface
Integration Module
Interface
Cybernetics Simulator
Input
Output

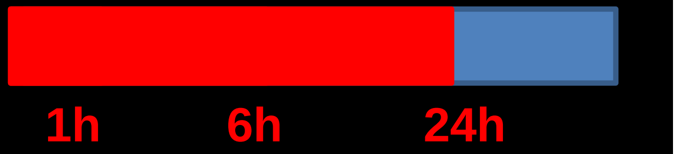
TATICO OPERACIONAL SIMULATOR (TOpSim) (According to Table 3)

With Cyber attack

Without Cyber attack







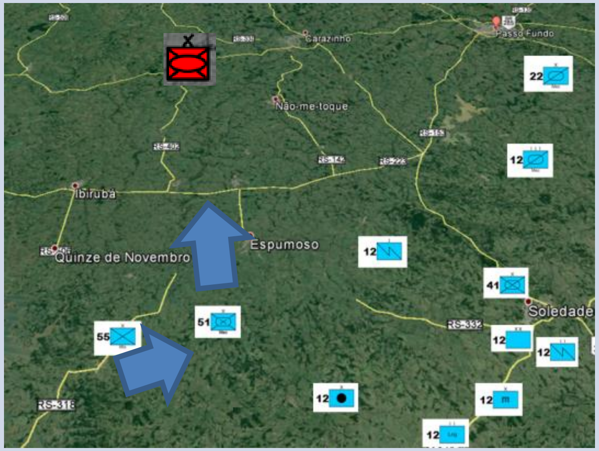
Agenda

- Introduction
- Related Work
- **Functionalities of the Architecture**
  - Identification of Vulnerabilities
  - Identification of Impacts of a Cyber Attack
  - **Mission Planning**
- Assessment
- Final Remarks

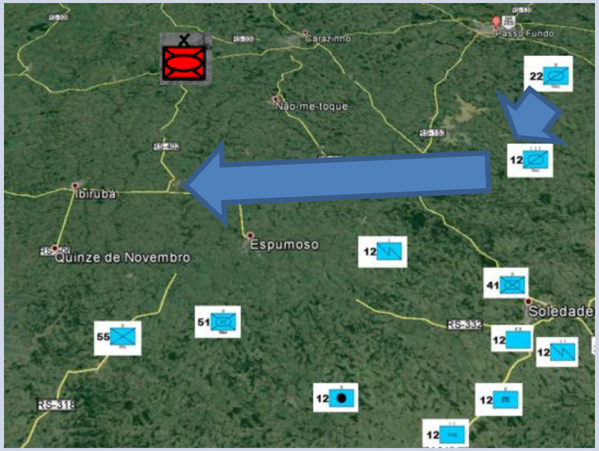
Mission Planning

- In planning a military mission, many decisions can be made. In this study, we focus on the movement of military troops (positioning of Units on the battlefield).
- For our approach we focus on the data network that supports military actions. When we change the position of a military Unit, we are indirectly changing the topology of the data network.

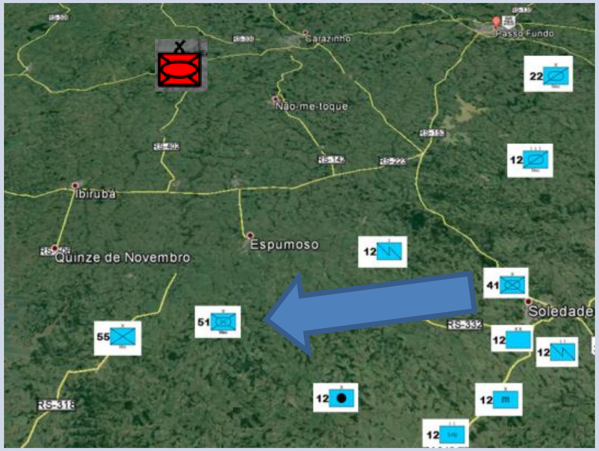
Planning Alpha



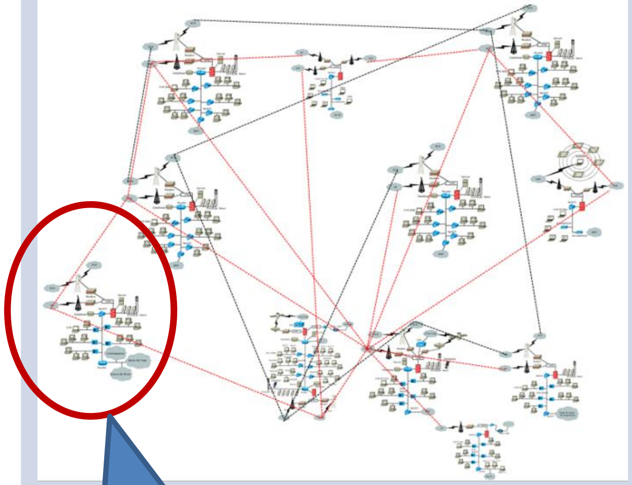
Planning Beta



Planning Gamma

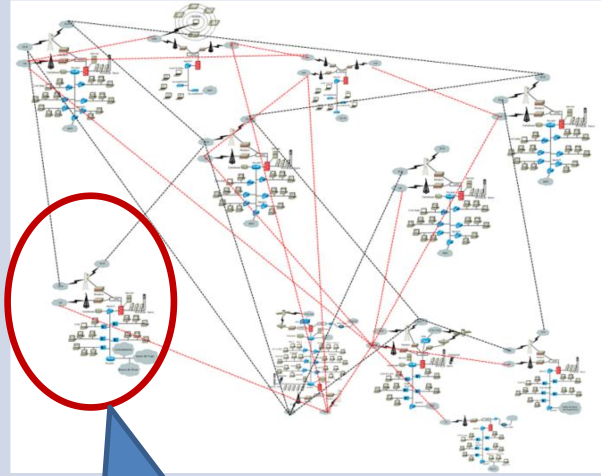


Planning Alpha



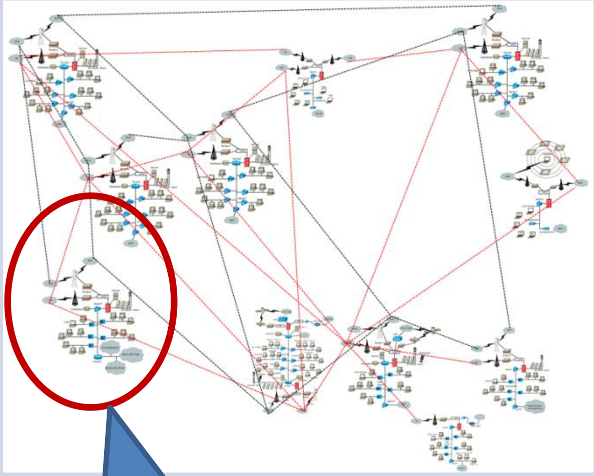
2 links

Planning Beta



3 links

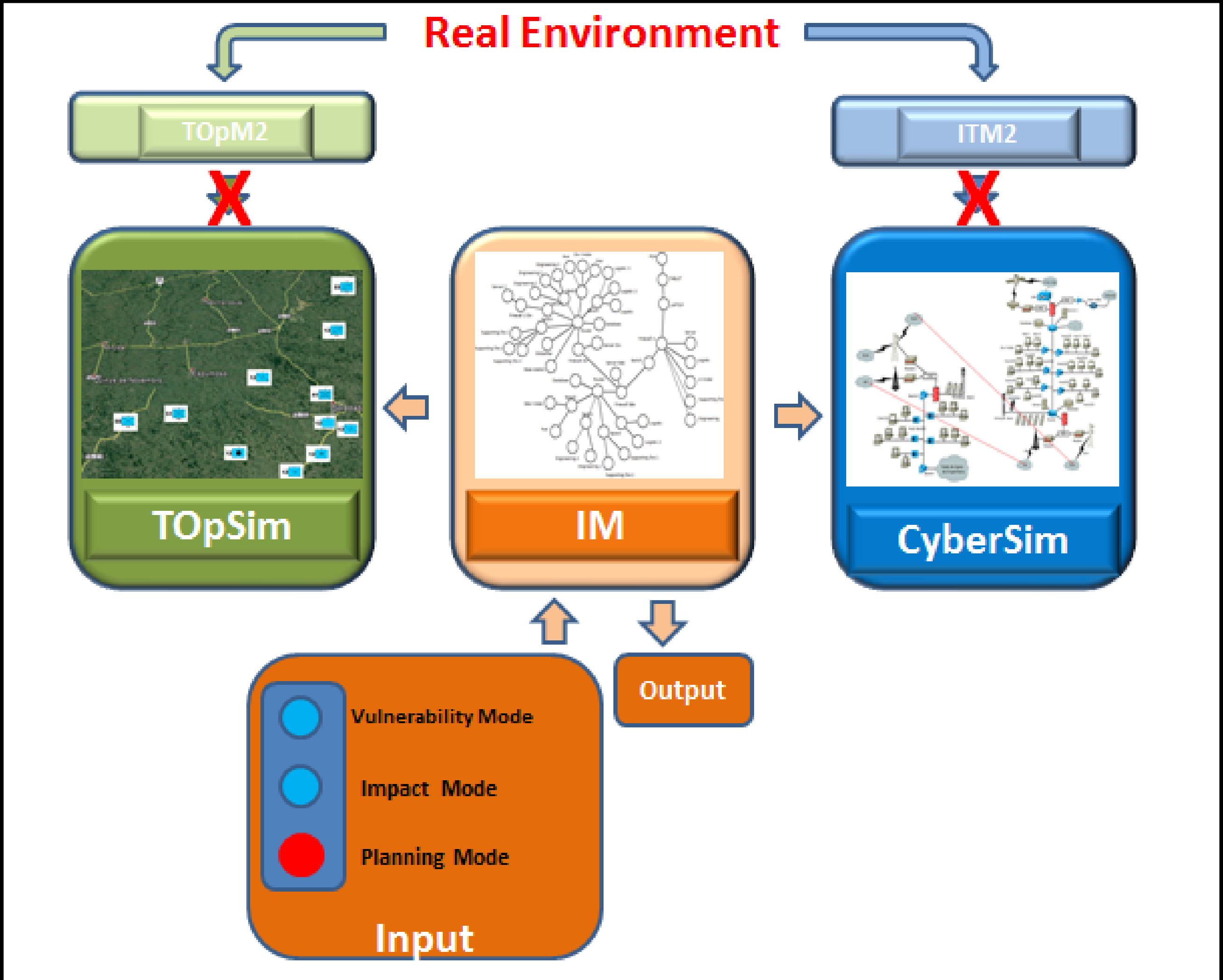
Planning Gamma



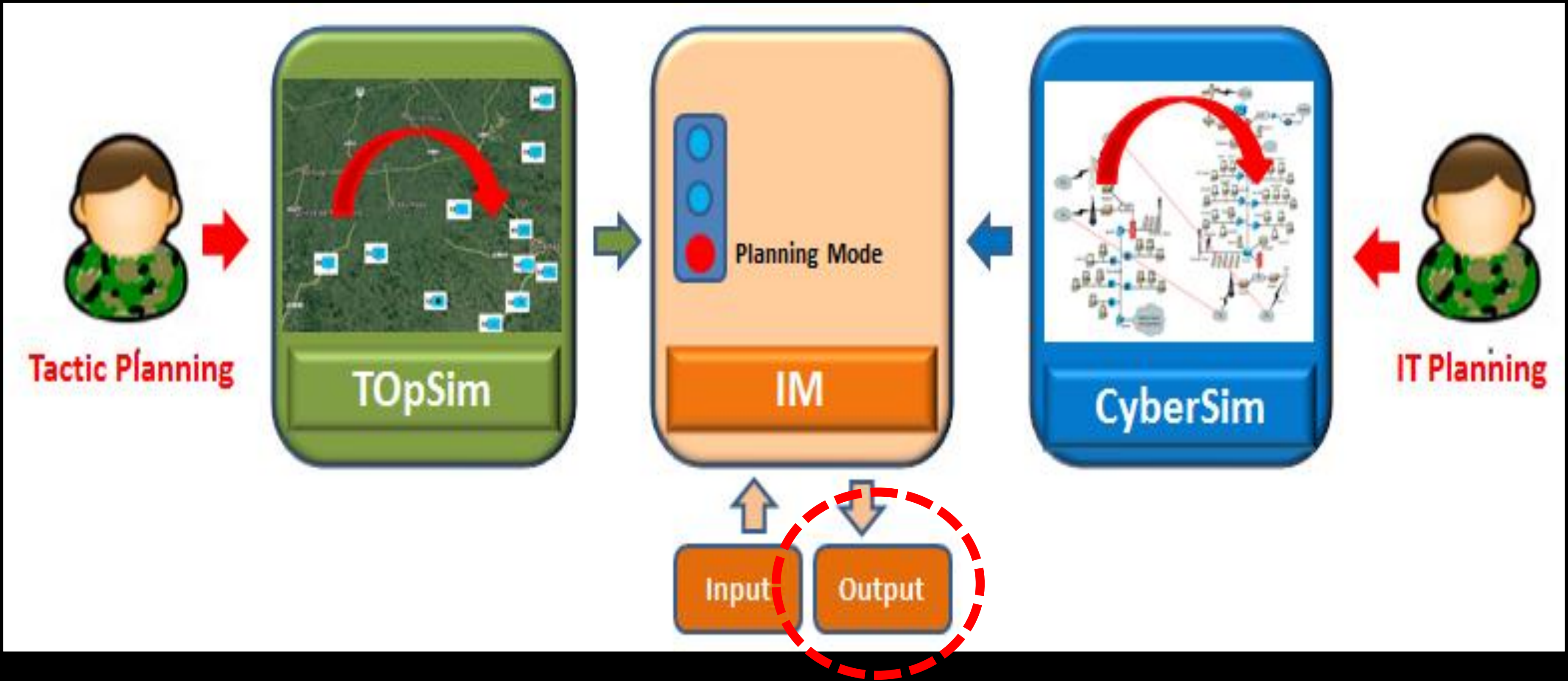
5 links

- These changes in connections can include or exclude a set of assets in a data network. According to [6], when new assets are added or removed from a network, the network vulnerabilities also change.

Mission Planning

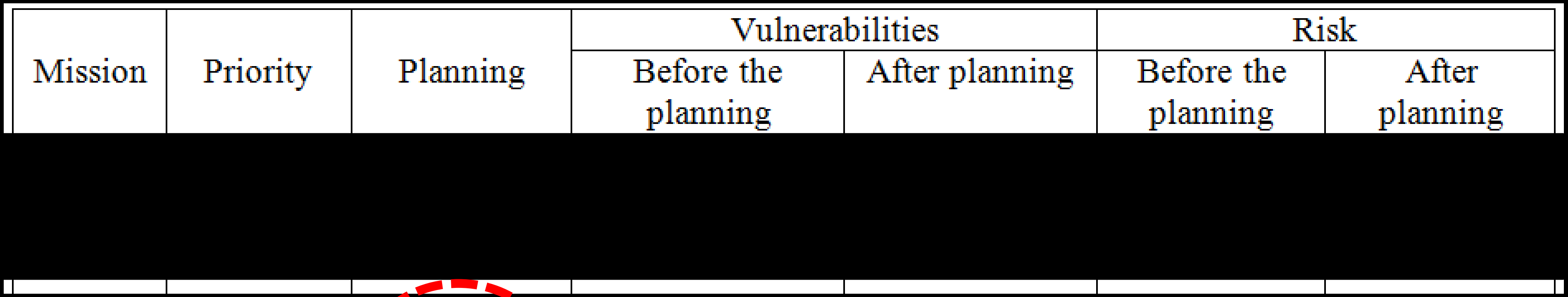


Mission Planning



Mission Planning

Table 4 – Plan Report [8]



Mission	Priority	Planning	Vulnerabilities		Risk	
			Before the planning	After planning	Before the planning	After planning

Is better

I want planning Beta

Commandant

Agenda

- Introduction
- Related Work
- Functionalities of the Architecture
  - Identification of Vulnerabilities
  - Identification of Impacts of a Cyber Attack
  - Mission Planning
- Assessment
- Final Remarks

Assessment

- The proposed architecture was not implemented by the time of this paper submission. However, some simulations were done for conceptual assessment of the main module of the architecture (Integration Module).
- For the integration of the environments, IM uses the graph structure to represent real world environment (kinetic and cyber).

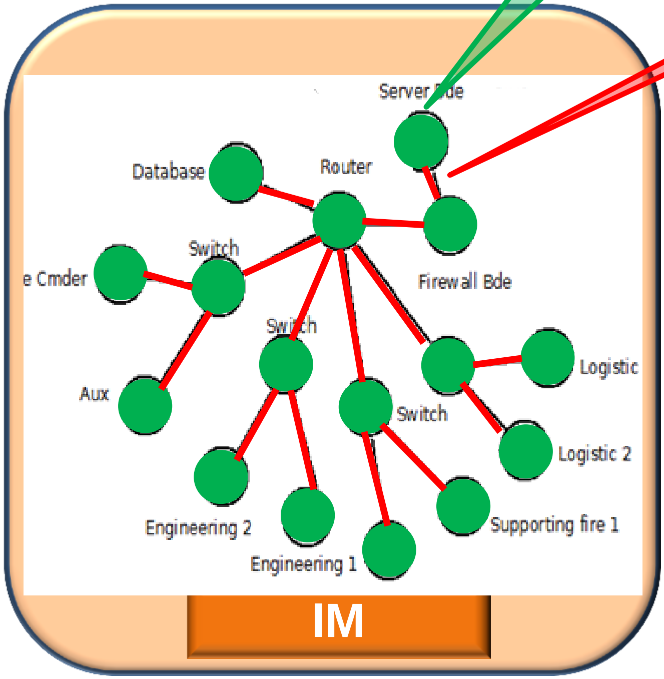
Assessment

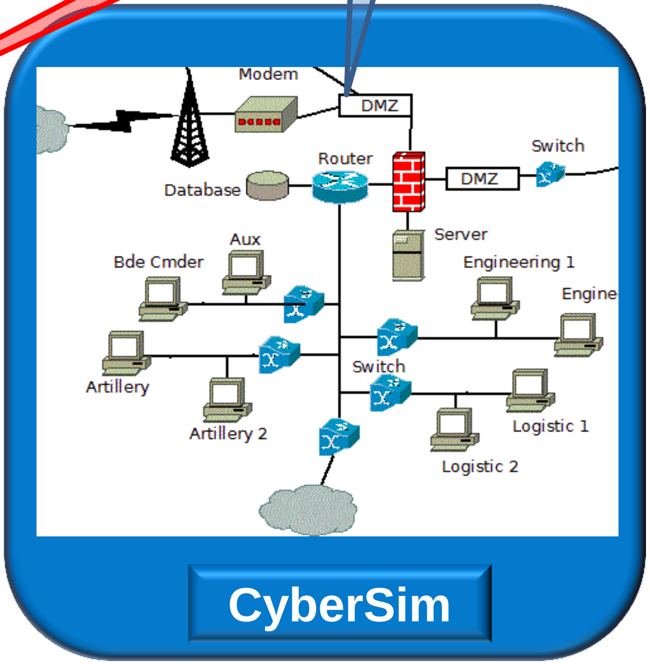
- Therefore, we propose the use of Java Universal Network Graph (JUNG) for necessary implementation (construction and analysis of graphs) of the IM. Which in turn will help us to realize the evaluation of the approach.

Assessment (Step 1)

Construction of the Graph

- Admitting that the CyberSim has 405 assets, the graph will have at least 405 nodes and 500 edges.
- To build this graph, the algorithm needed **49ms.**



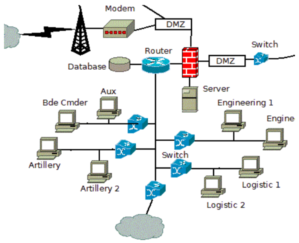


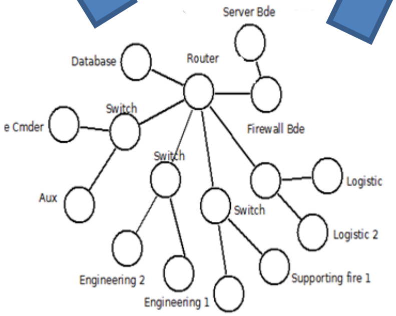
Assessment (Step 1)

Construction of the Graph

Table: Different size Graphs x time to build

Estimated Assets	Graph Nodes	Graph Edges	Average Time
1,620	1,620	2,000	79.8 ms
4,050	4,050	5,000	90.1 ms
40,500	40,500	50,000	1,570 ms
65,000	65,000	80,000	3,575 ms





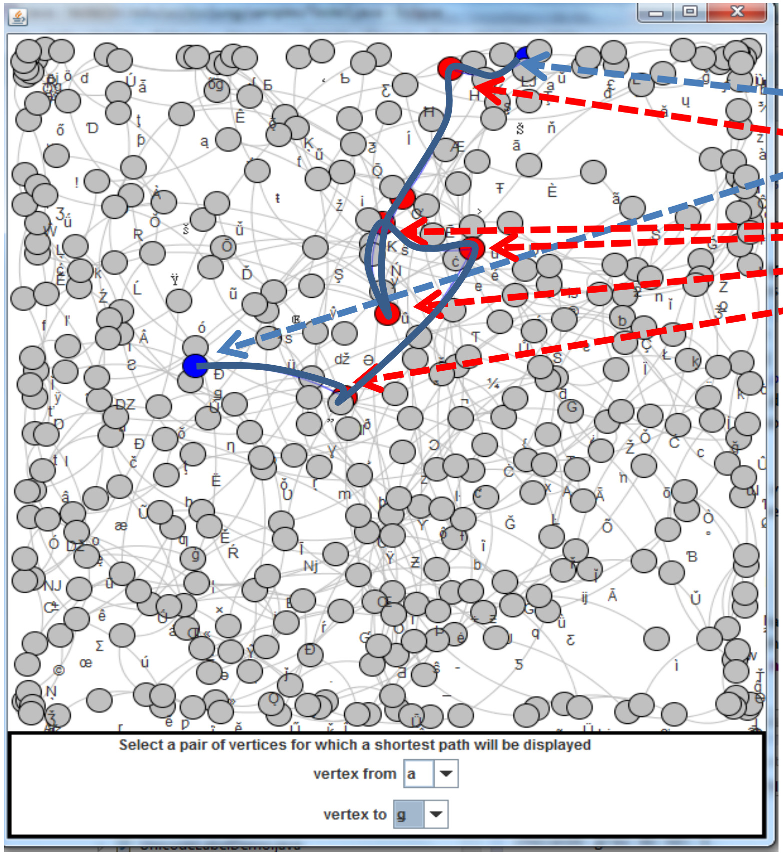
Assessment (Step 2)

Analysis of Paths in Graph

Continuing with the assessment of IM, we highlight the important requirements to verify the existence of "paths" between two nodes of the graph. For this activity, we can use *DijkstraShortestPath* algorithm.

Assessment (Step 2)

Analysis of Paths in Graph



Select a pair of vertices for which a shortest path will be displayed

vertex from a

vertex to g

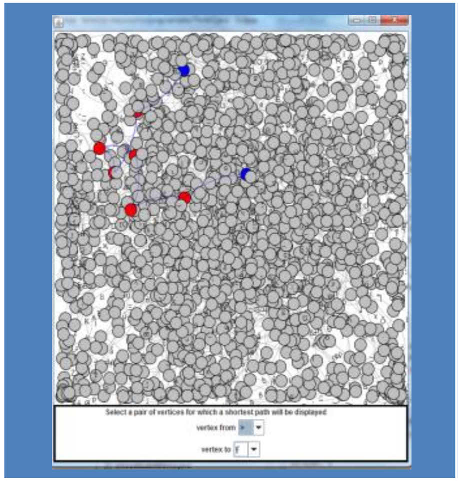
The **blue nodes** are the “start” and the “end” nodes of the path, the intermediate nodes (of the path) are **red**, and the **blue edges** are the paths taken by the algorithm.

To generate this path in a graph with 405 nodes, the algorithm took an average of **1.83 ms**.

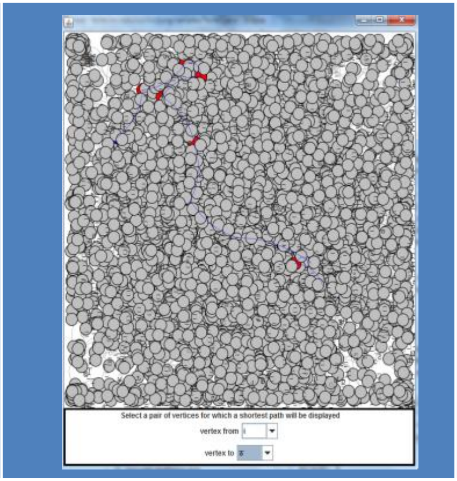
Assessment (Step 2)

Analysis of Paths in Graph

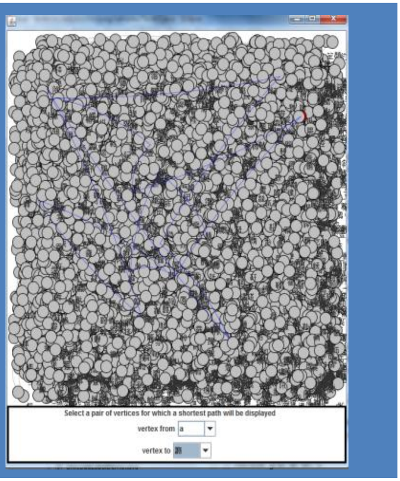
Estimated Assets	Graph Nodes	Graph Edges	Average Time
1,620	1,620	2,000	4.77 ms
4,050	4,050	5,000	12 ms
40,500	40,500	50,000	221.5 ms
65,000	65,000	80,000	229.25 ms


Select a pair of vertices for which a shortest path will be displayed

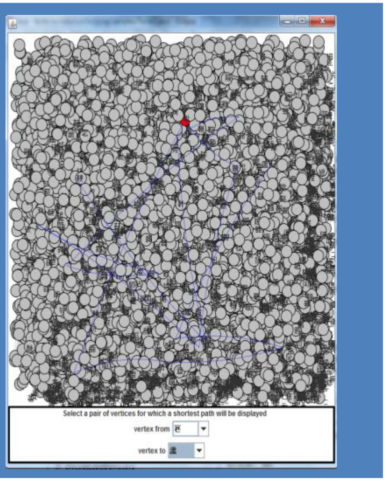
1,620 nodes


Select a pair of vertices for which a shortest path will be displayed

4,050 nodes


Select a pair of vertices for which a shortest path will be displayed

40,500 nodes


Select a pair of vertices for which a shortest path will be displayed

65,000 nodes

Agenda

- Introduction
- Related Work
- Functionalities of the Architecture
  - - Identification of Vulnerabilities
  - – Identification of Impacts of a Cyber Attack
  - – Mission Planning
- Assessment
- **Final Remarks**

Final Remarks 1/3

- The main purpose of this article is to extend conceptual understanding about the approach developed in our previous article [7].
- With this goal, in this article, we present the functionalities expected for Architecture. They are: identify the vulnerabilities of IT assets, in relation to tactical missions; identify the impacts of a cyber-attack in the kinetic environment; and achieve a tactical, cyber and combined planning.

Final Remarks 2/3

- The approach focuses only on the terrestrial military environment and Denial of Service in cybernetic environment. The undocumented attacks will not be identified by the proposed Architecture.
- The assessment was not to identify a tool or an ideal programming language to perform the analyzes in graph, but rather to verify the viability (in terms of processing speed) of the use of graph theory for IM.

Final Remarks 3/3

- As future work, we propose to implement other components of the proposed Architecture; and other types of cyber-attacks, such as: interception actions, degradation and production of false data.
- Concluding this work, we believe that Architecture can also be used in other areas.

Acknowledgment

- I would like to thank the Aeronautic Technology Institute (ITA), the Technology Science Department (DCT), the Center for Integrated Electronic Warfare (CIGE) and the Brazilian Army .

References

- [1] BARFORD, P; DACIER, M.; DIETTERICH, T. G.; FREDRIKSON, M.; GIFFIN, J.; JAJODIA, S.; JHA, S.; LI, J.; LIU, P.; NING, P.; SONG, D.; STRATER, L.; SWARUP, V.; TADDA, G.; WANG, C.; YEN, J. Advances in Information Security. **Cyber situational awareness**: issues and research. New York: Springer, 2009. (Advances in Information Security, v. 46) ISBN 978-1-4419-0139-2.
- [2] DENNING, D. E. An intrusion-detection model. **IEEE Transactions on Software Engineering,** v.13, p. 222-232, 1987.
- [3] BASS, T. **Multi sensor data fusion for next generation distributed intrusion detection systems.** IRIS National Symposium on Sensor and Data Fusion. [S.l.: s.n.]. 1999.
- [4] SCHNEIER, B. (1999). Attack trees: Modeling security threats. Dr. Dobb's journal. Available: https://www.schneier.com/paper-attacktrees-ddj-ft.html. Accessed: 11 out. 2013.
- [5] MUSMAN, S.; TEMIN, A.; TANNER, M.; FOX, D.; PRIDEMORE, B. (2010). Evaluating the Impact of Cyber Attacks on Missions. MITRE Corp, McLean, VA, 22102.
- [6] JAJODIA, S.; NOEL, S. Topological vulnerability analysis. In: JAJODIA, S. et al. **Cyber situational awareness**: issues and research. New York: Springer, 2010. p. 139-153. (Advances in Information Security, v. 46)

References

- [7] MACHADO, A; BARRETO, A; YANO, E. Architecture for cyber defense simulator in military applications. In: INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM, 18., 2013, Alexandria. **Proceedings...** Alexandria: CCRP, 2013.
- [8] MACHADO, A. F. A.; YANO, E. T. Architectural concept of a simulator for cyber situational awareness. 2013. Thesis (Master degree in computer engineering). Instituto Tecnológico de Aeronáutica. São José dos Campos, 2013.
- [9] ALBERTS, D. S.; HAYES, R. E. **Understanding command and control**. Washington, D.C.: CCRP Publication Series, 2006. 255 p. ISBN 1-893723-17-8.
- [10] SKYBOX SECURITY. Developer´s Guide. Skybox View. Manual.Version 11. 2010.
- [11] SCALABLE Network. EXata communications simulation platform. Available: <http://www.scalable-networks.com>. Accessed: 16 jun. 2012.
- [12] DECATRON. **Executive project**. Cyberwar operation simulator. Rio de Janeiro. Nov. 2011.
- [13] LEEUWEN, V. et al. Cyber Security Analysis Testbed: combining real, emulation, and simulation. In: INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY. **Proceedings…** San Jose: IEEE, 2010.
- [14] STOREY, N. **Safety-Critical Computer Systems**. [S.l.]: Prentice-Hall, 1996.
- [15] JUNG. Java universal network graph framework. Available: http://jung.sourceforge.net/index.html. Accessed: 10 set. 2013.

Thank you for your attention

Conceptual Architecture for Obtaining Cyber Situational Awareness

André F. A. Machado - Major
Instituto Tecnológico de Aeronáutica
Brazil
majandre@ita.br
majafam97@gmail.com