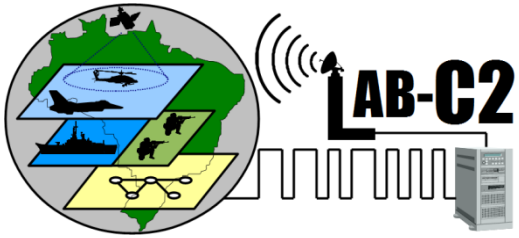


18th ICCRTS

Architecture for Cyber Defense Simulator in Military Applications

Authors:

Maj André Ferreira Alves Machado

Maj Alexandre B. **Barreto**

Prof. Edgar Toshiro **Yano**

Goal

- Proposal of an architecture that fuses kinetic and cyber behaviors in an integrate view for planning or evaluation of military defense.

Agenda

- **Introduction**
- **Cyber defense simulator Architecture**
- **Assessment Model**
  - **Tactical Level Scenario**
  - **– Information Technology Infrastructure**
  - **– Evaluation through case studies**
- **Final Remarks**

Introduction 1/4

- The modern battlefield has been increasingly relying on digital technology based on computers networks and systems.

Introduction 2/4

- Problems on a single network node can result in a full or partial loss of capacity to perform a mission.

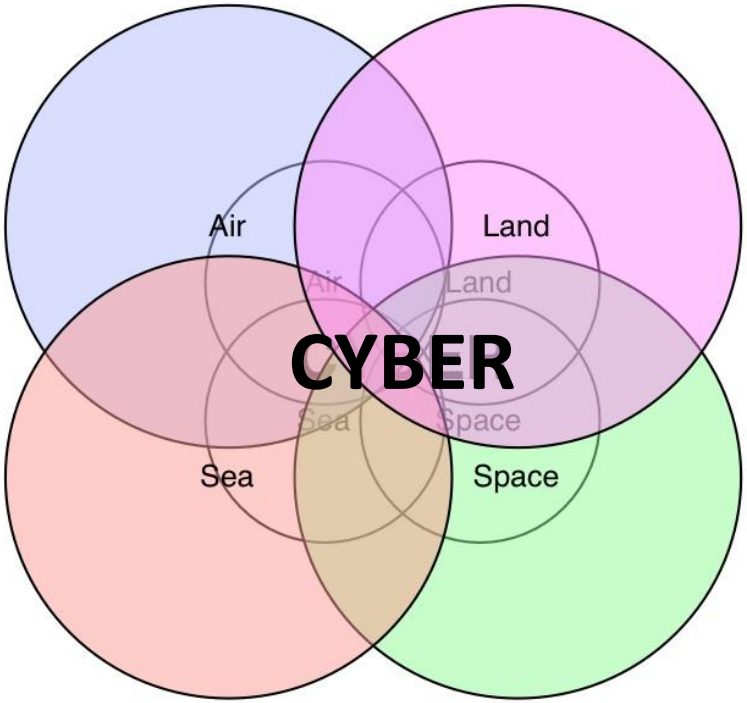
network

Affect

mission

Introduction 3/4

- This has led to the identification of the cyber domain as a new way to perform a war and increase the effects in the other domains (land, air and sea).



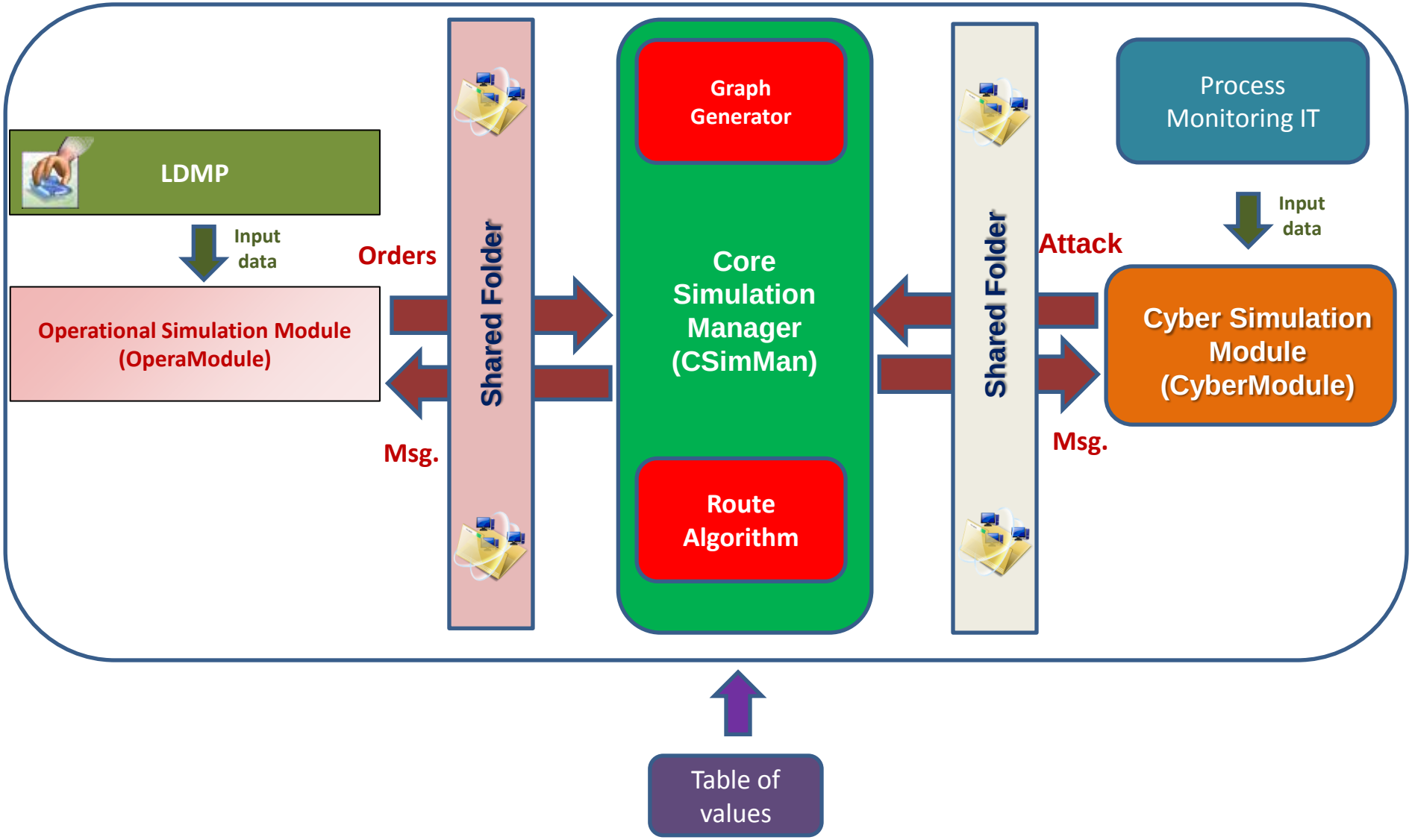
Introduction 4/4

- The knowledge and the measure of cyber effects in the other domains are crucial to discover how an event in the cyber domain can affect a process executed in a physical domain.

Agenda

- Introduction
- Cyber defense simulator Architecture
- Assessment Model
  - Tactical Level Scenario
  - Infrastructure of Information Technology
  - Evaluation through case studies
- Final Remarks

Architecture (overview)

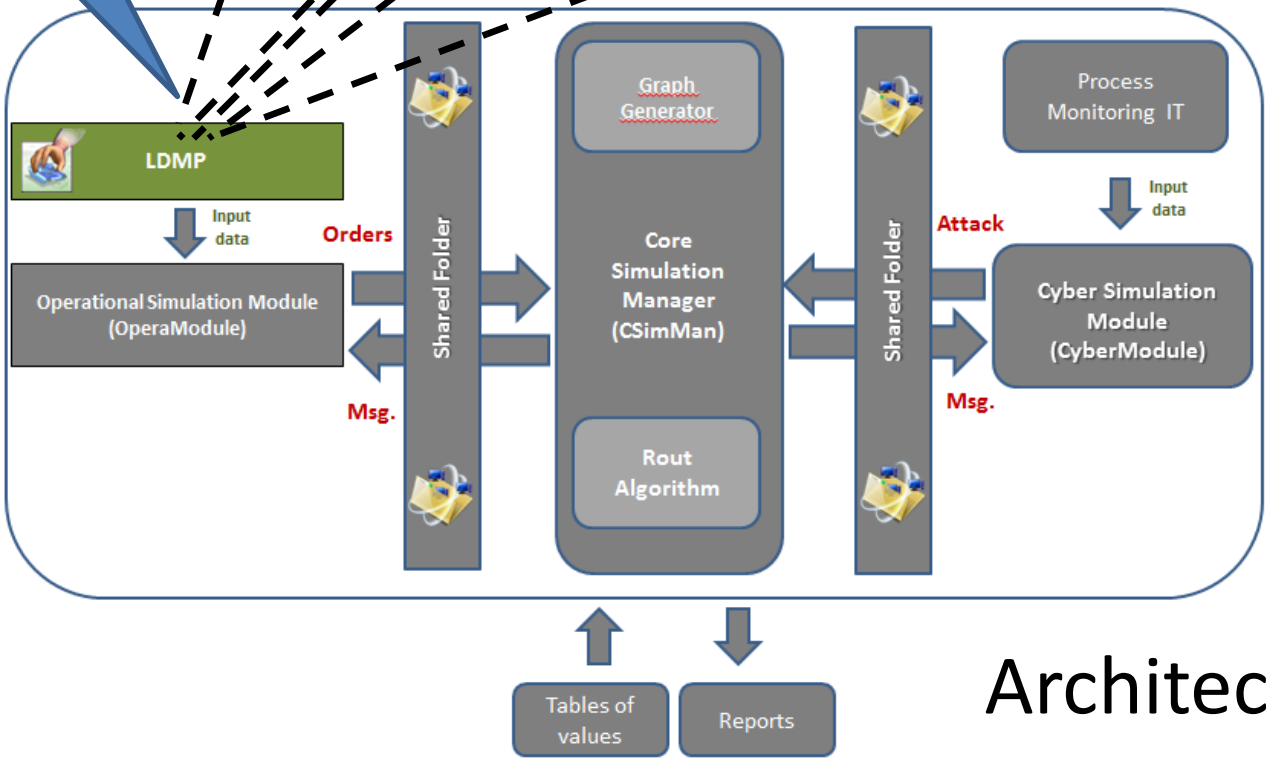


Real environment

Real environment

Coordinates tactical actions

Land Data Management Program

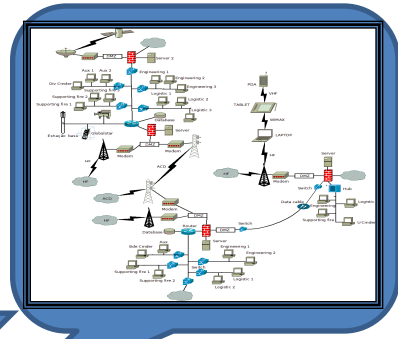


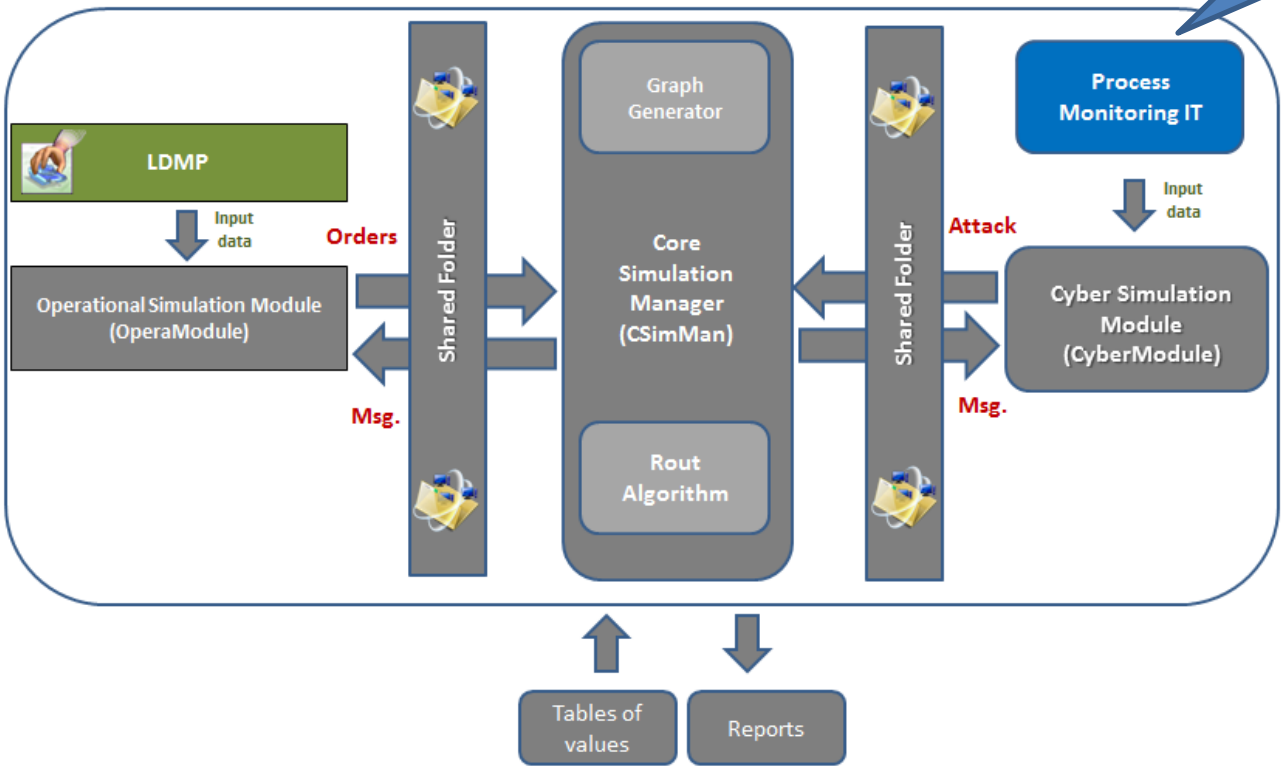
Architecture

Real environment

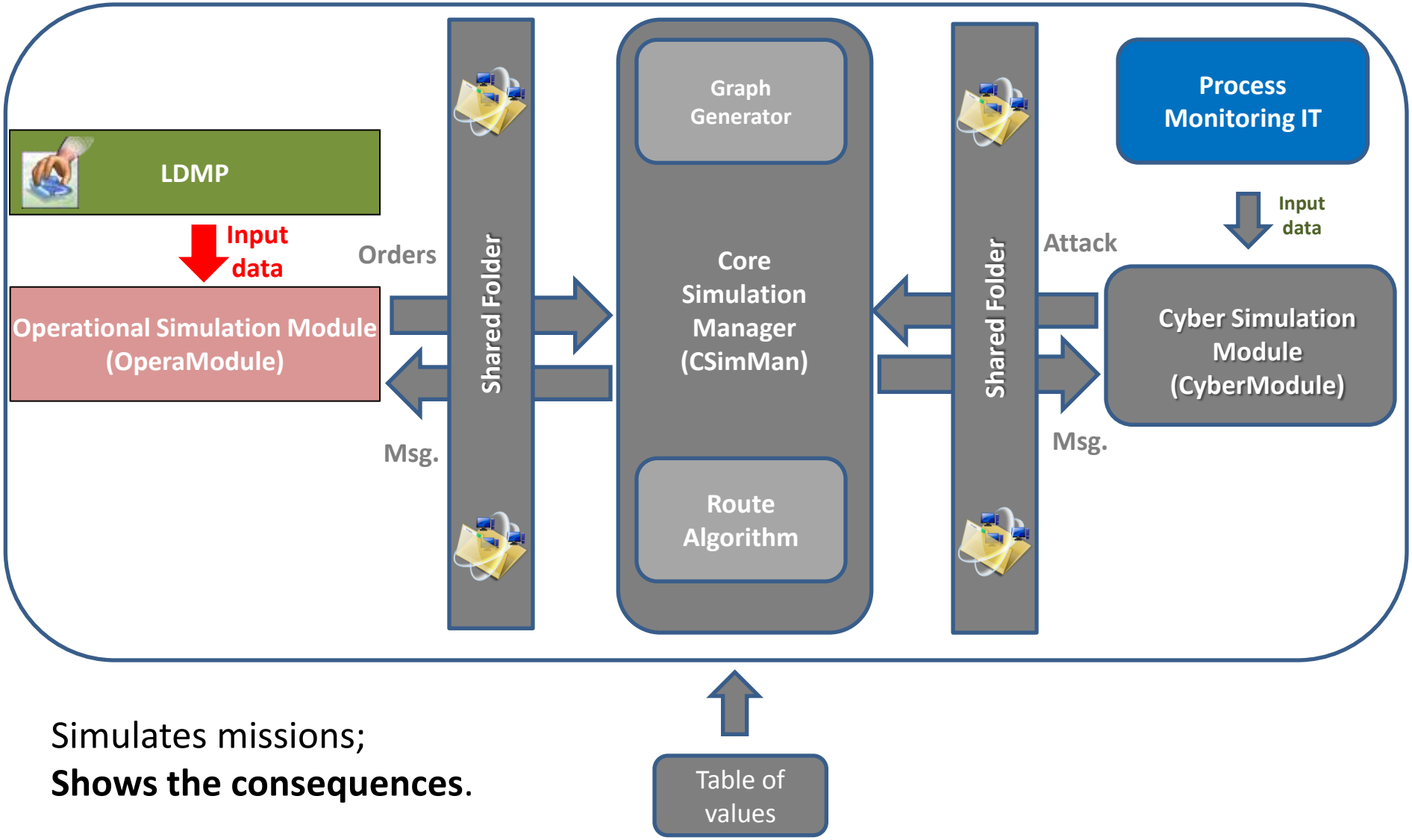
SCAN

- ✓ Topology
- ✓ IT assets



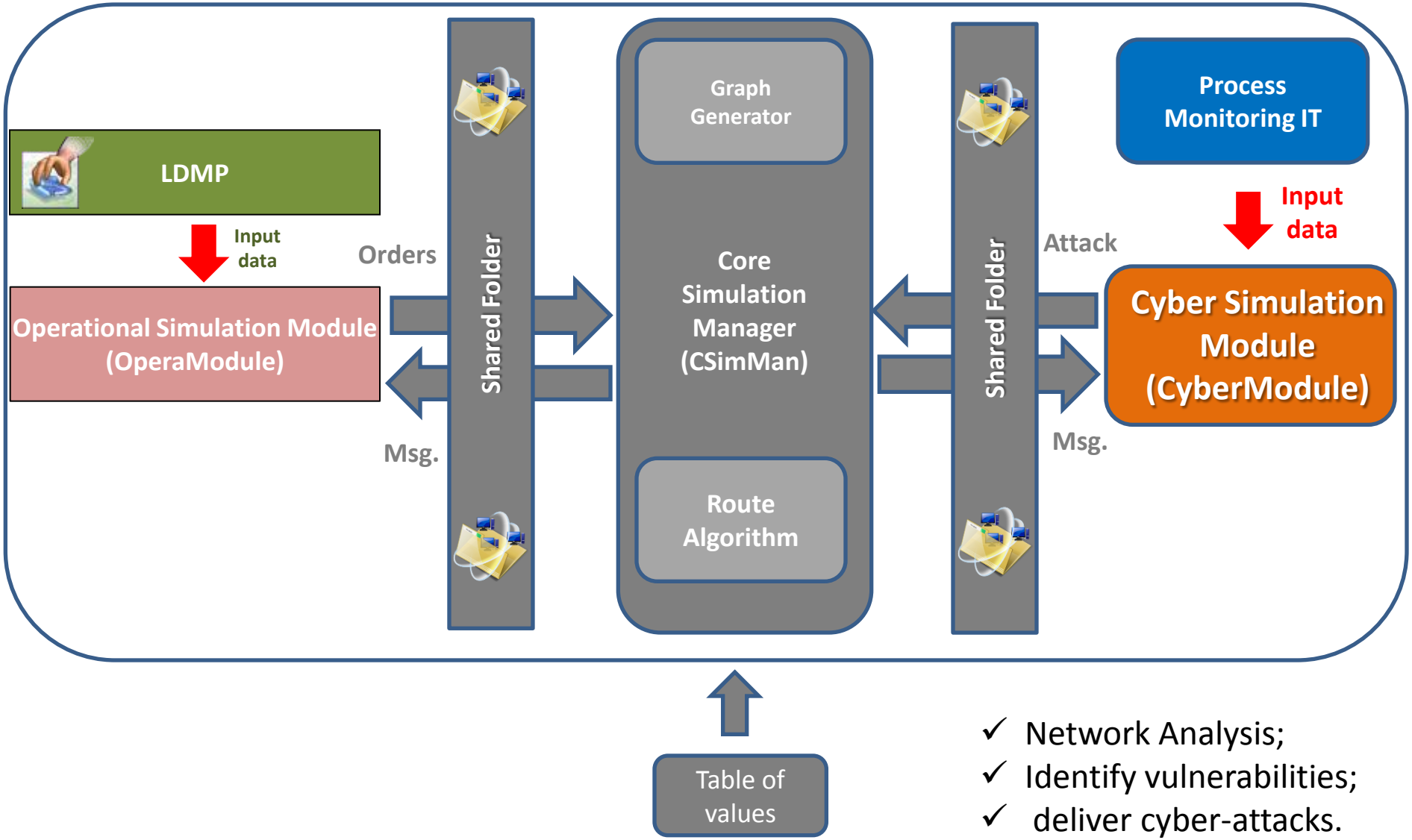


Architecture



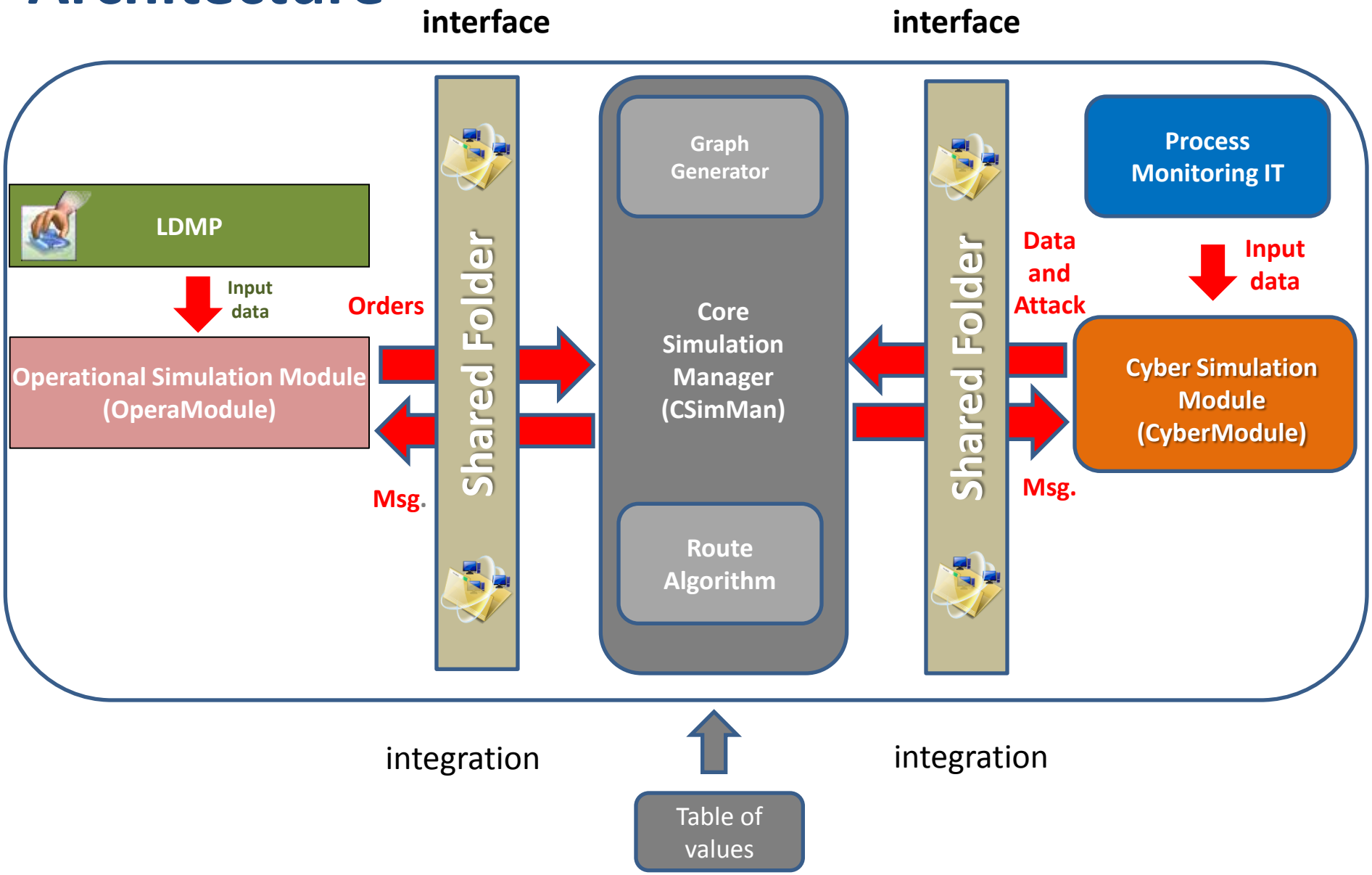
Simulates missions;
Shows the consequences.

Architecture

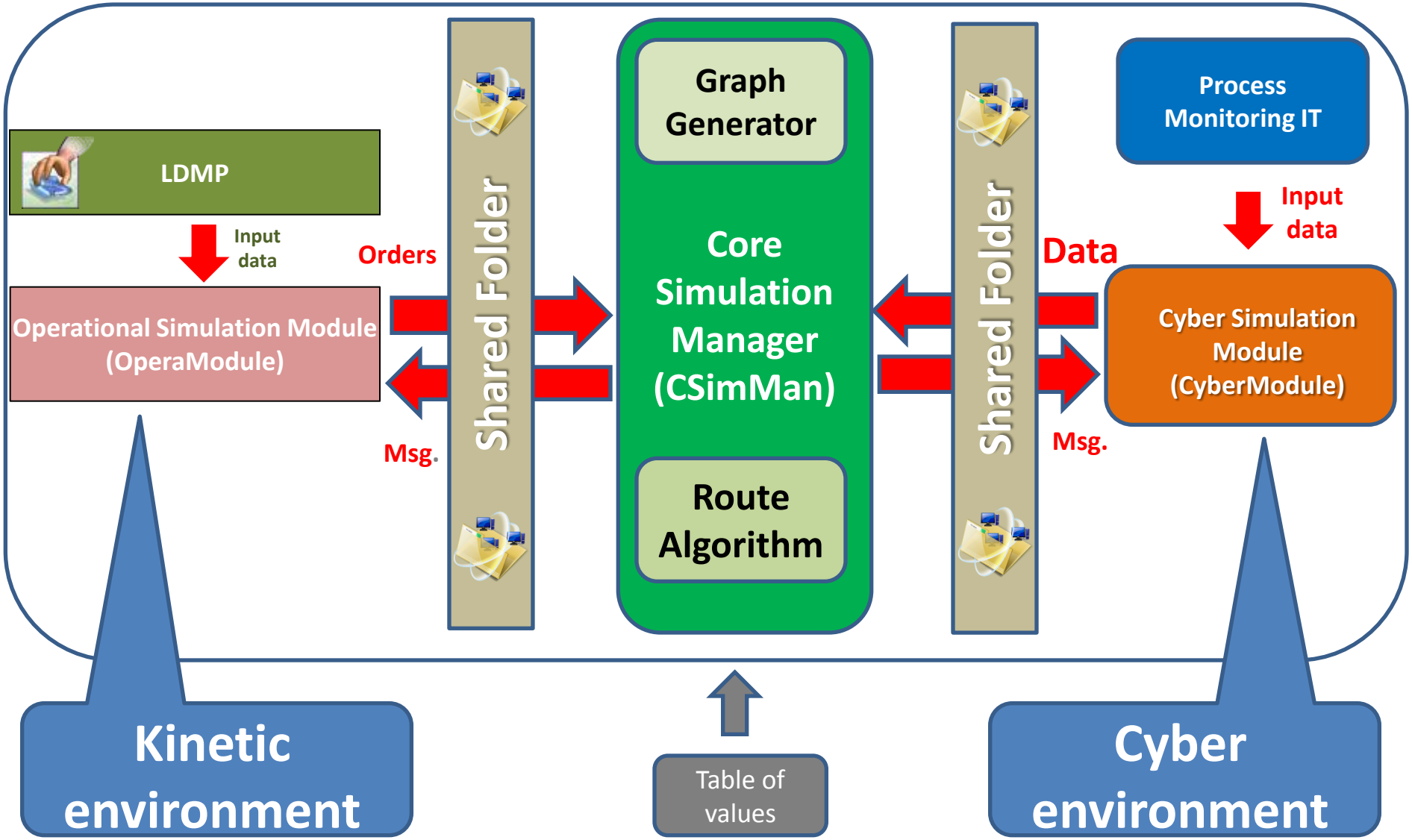


- ✓ Network Analysis;
- ✓ Identify vulnerabilities;
- ✓ deliver cyber-attacks.

Architecture

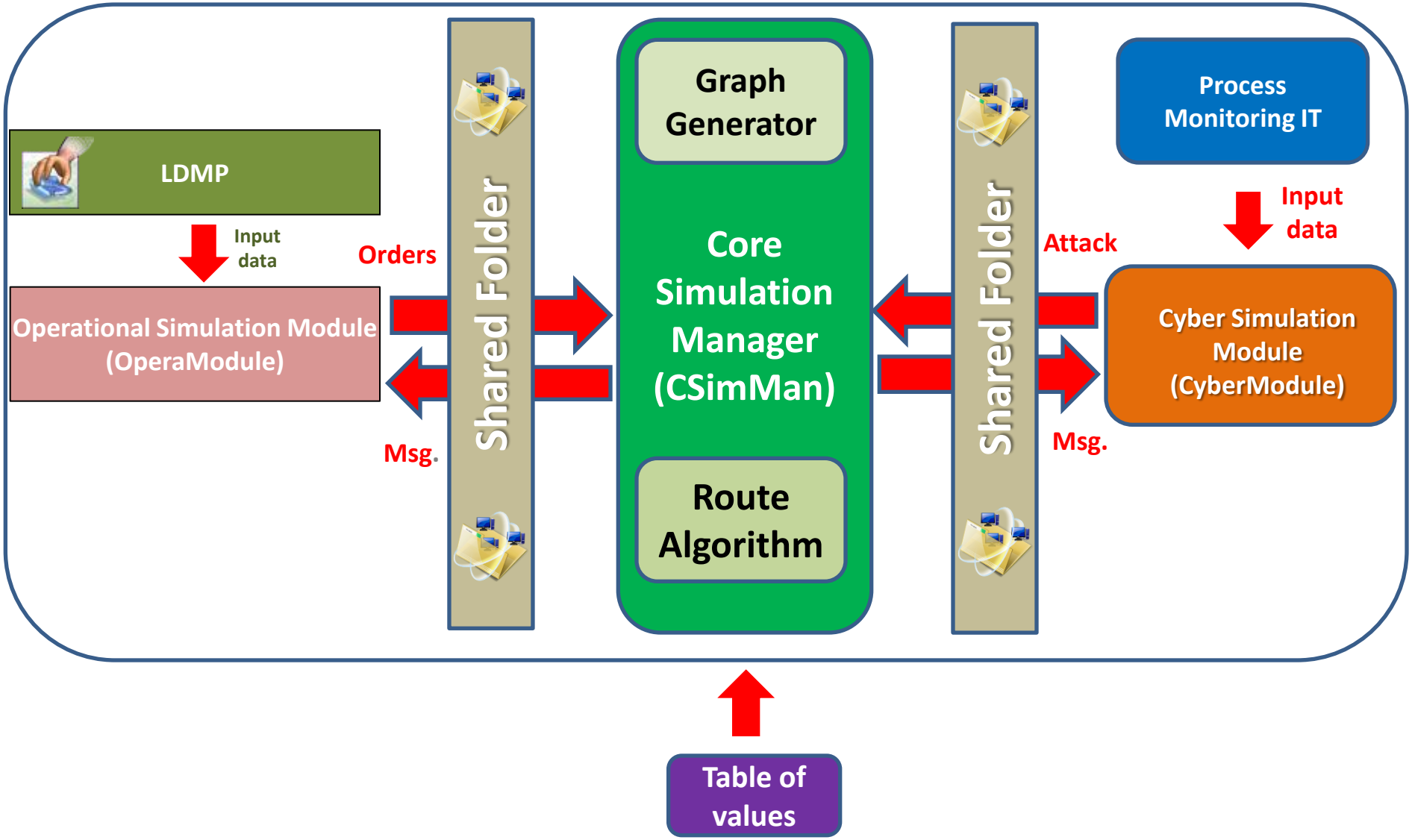


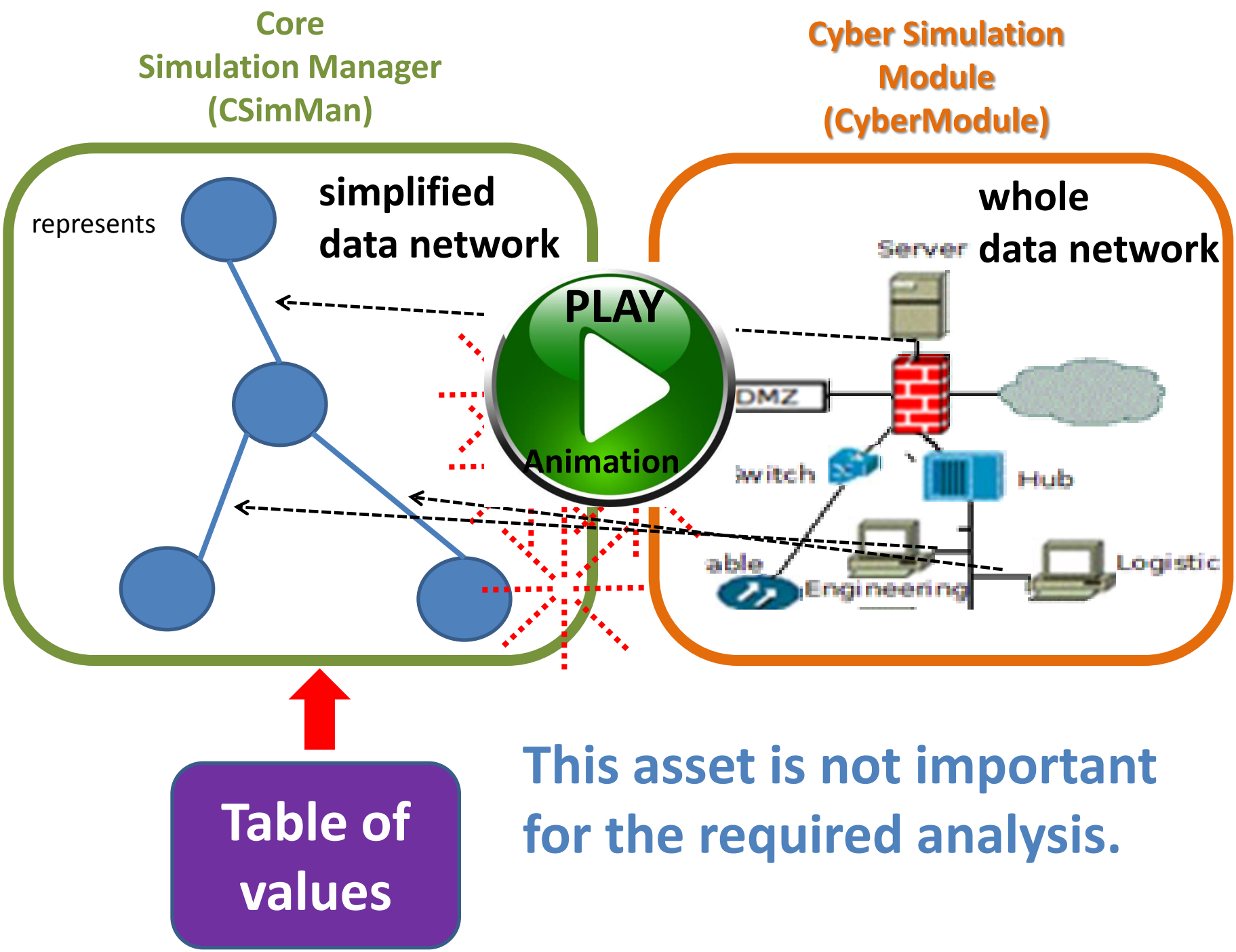
Architecture



integration

Architecture




Core
Simulation Manager
(CSimMan)
Cyber Simulation
Module
(CyberModule)
represents
simplified
data network
whole
data network
Server
PLAY
Animation
DMZ
witch
Hub
able
Engineering
Logistic
Table of
values
This asset is not important
for the required analysis.

Tables of Values

Note:

Only the asset considered the most important in the cyber-attack will be represented in the graph.

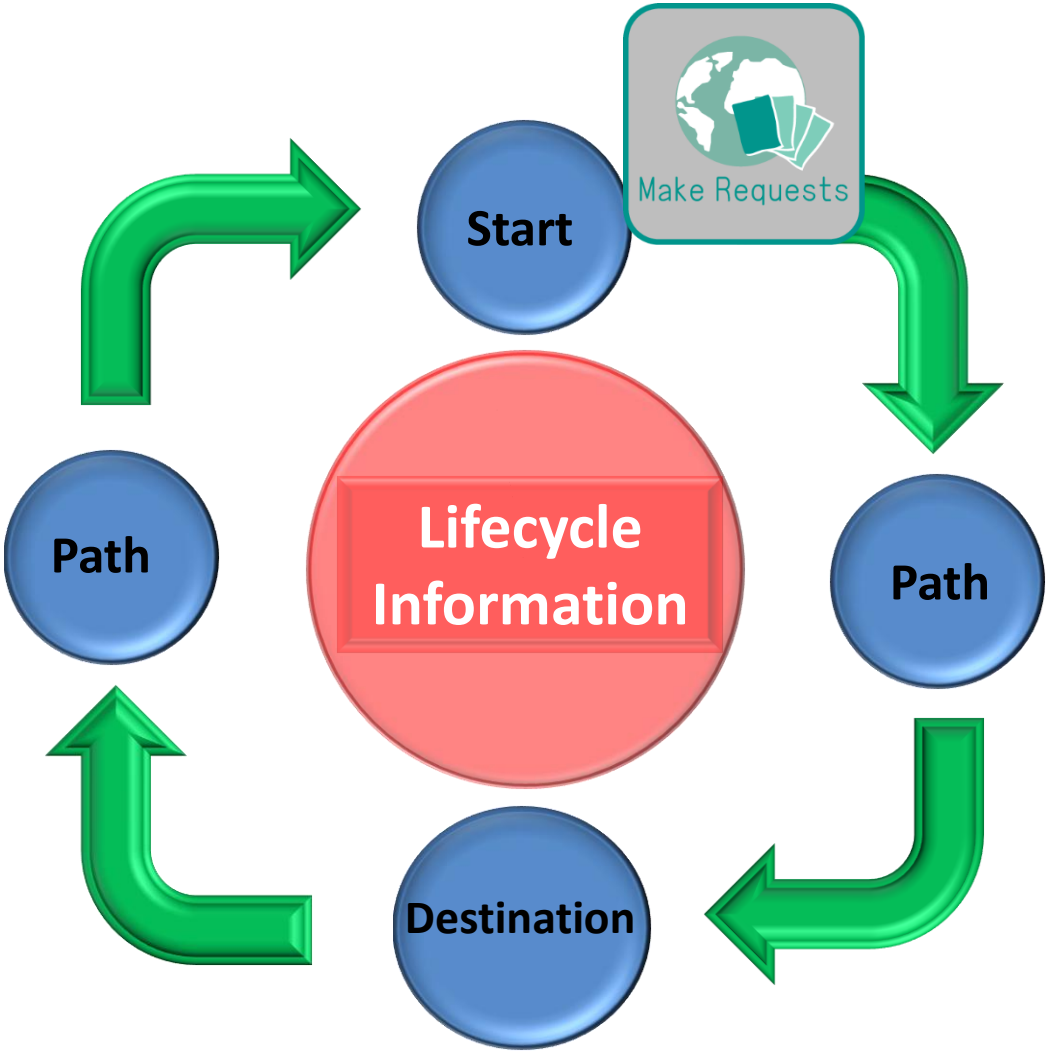
All communication means will be represented by edges with different weights.

Architecture

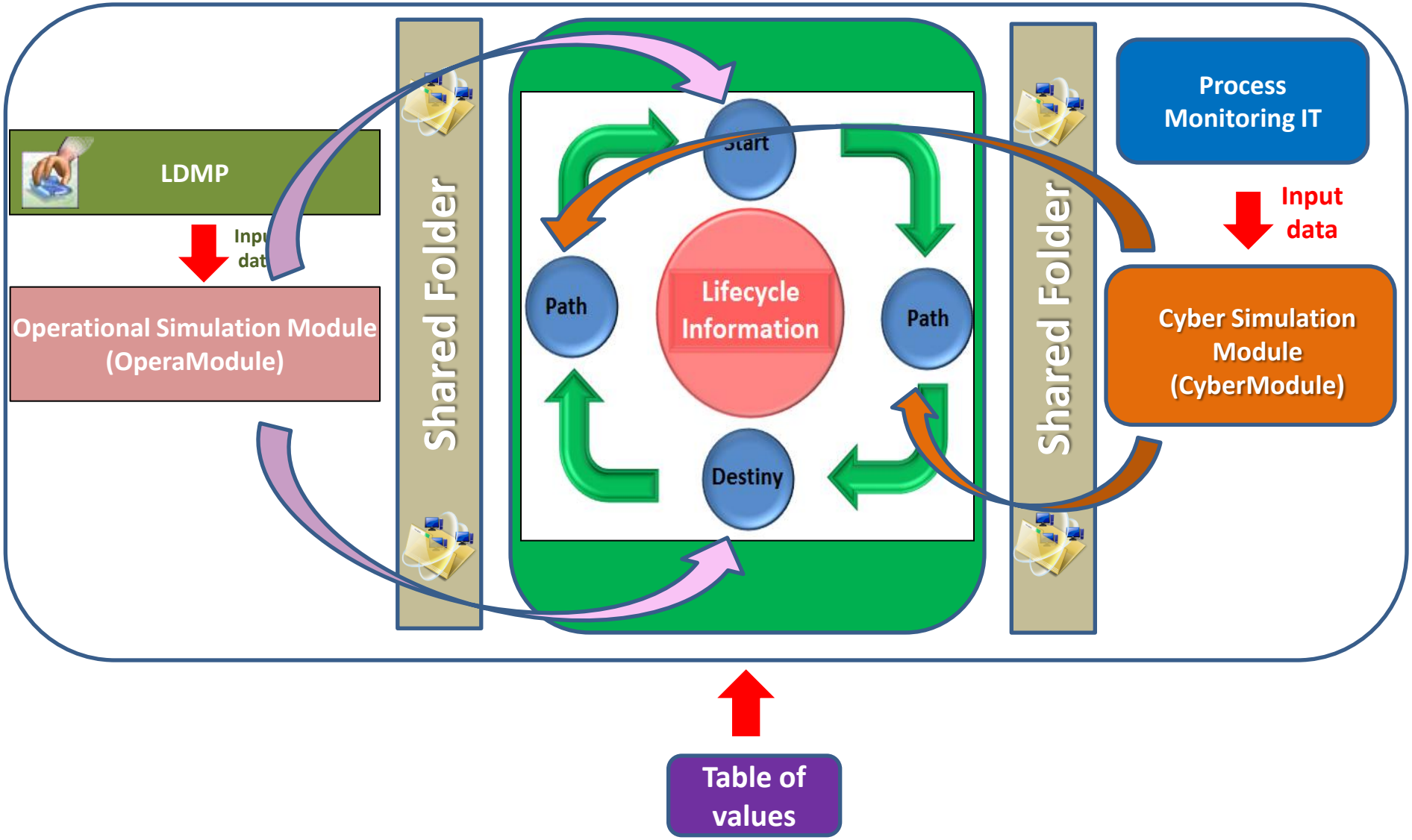
Any tactical event occur only when we have an order or make a request.

So, we have a flow of information.

Thus, we identified a lifecycle information.



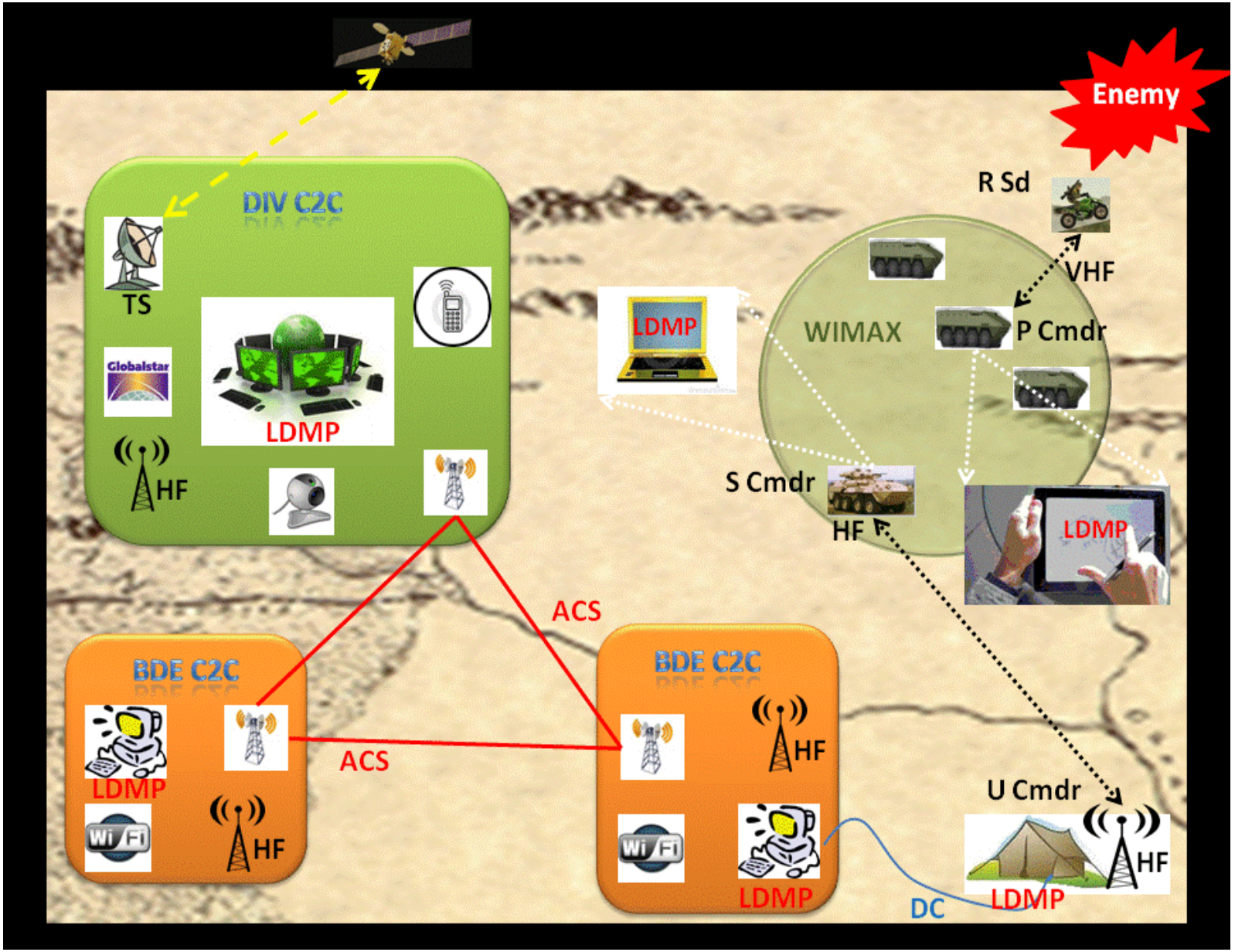
Lifecycle Information in architecture



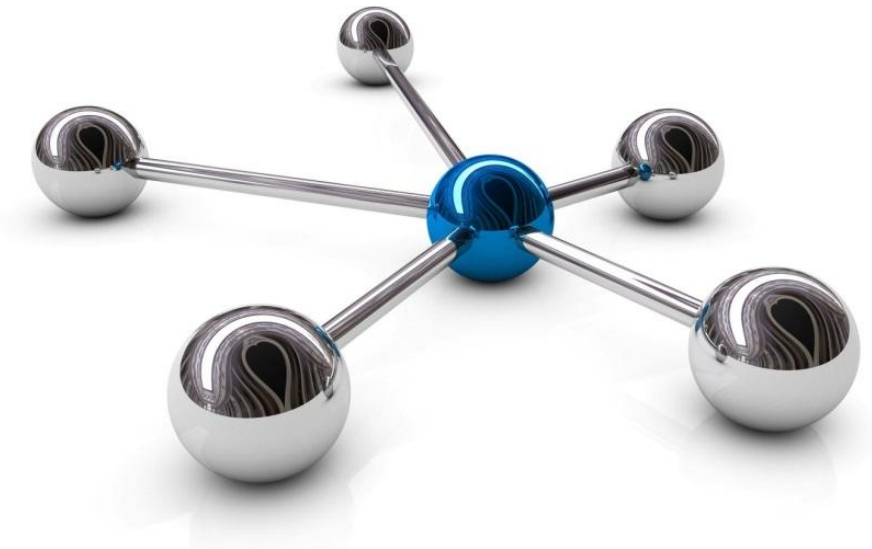
Agenda

- Introduction
- Cyber defense simulator Architecture
- Assessment Model
  - Tactical Level Scenario
  - Infrastructure of Information Technology
  - Evaluation through case studies
- Final Remarks

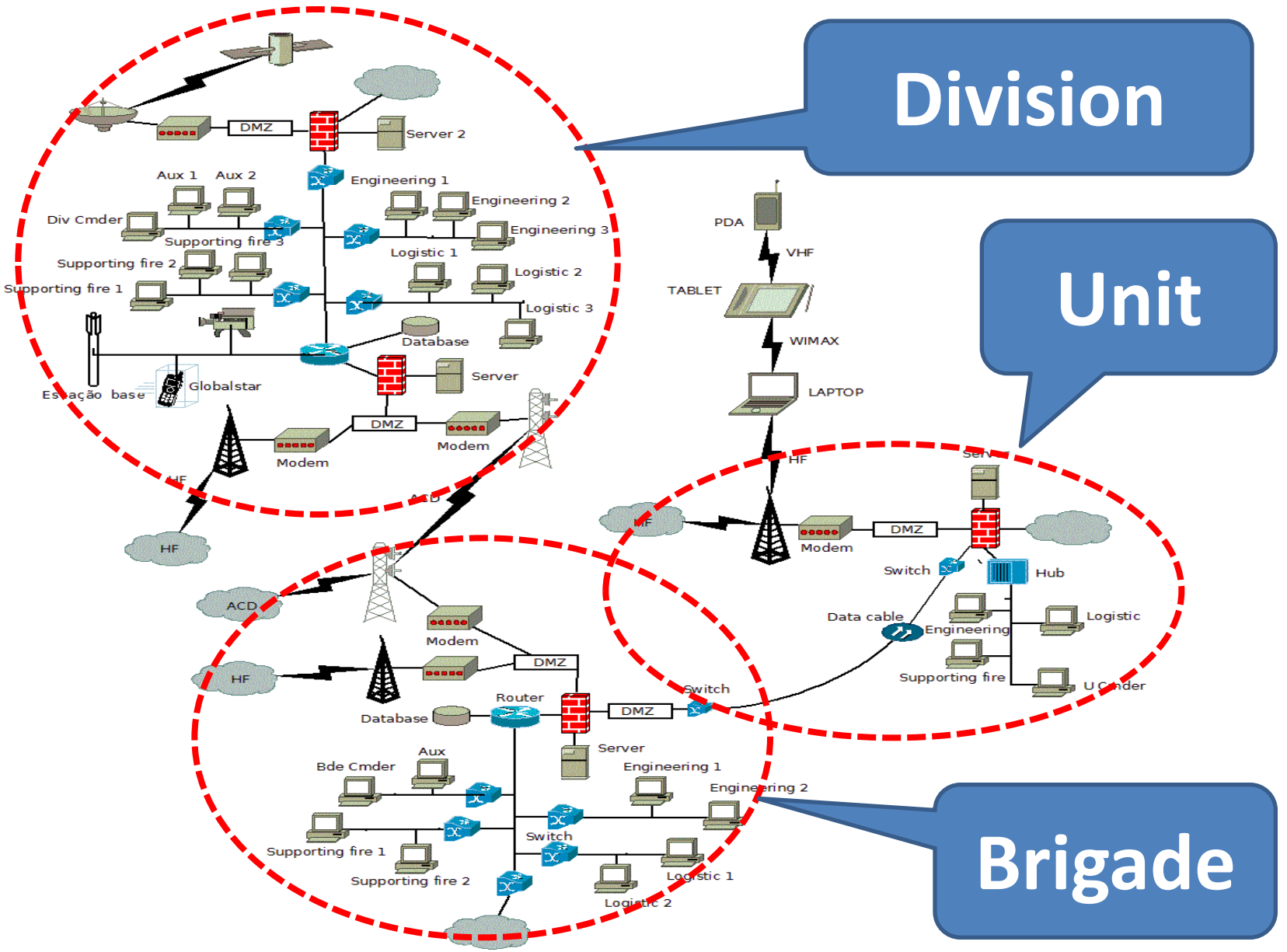
Tactical Level Scenario



To enable the order to be sent, its required an IT infrastructure.



IT Infrastructure



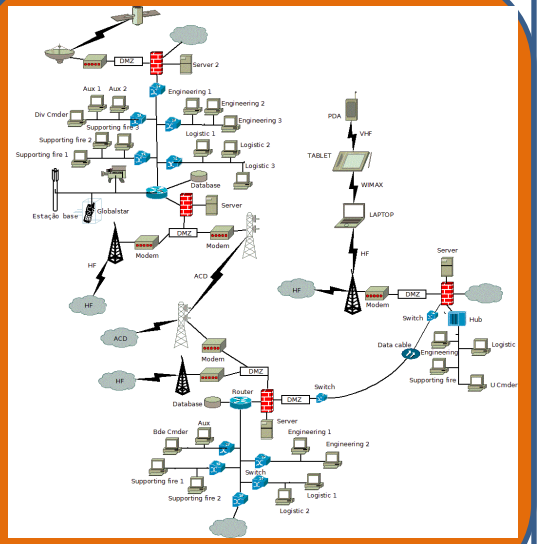
Simplified Architecture

Tactical Scenario

Operational Simulation Module
(OperaModule)

Core
Simulation Manager
(CSimMan)

IT Scenario

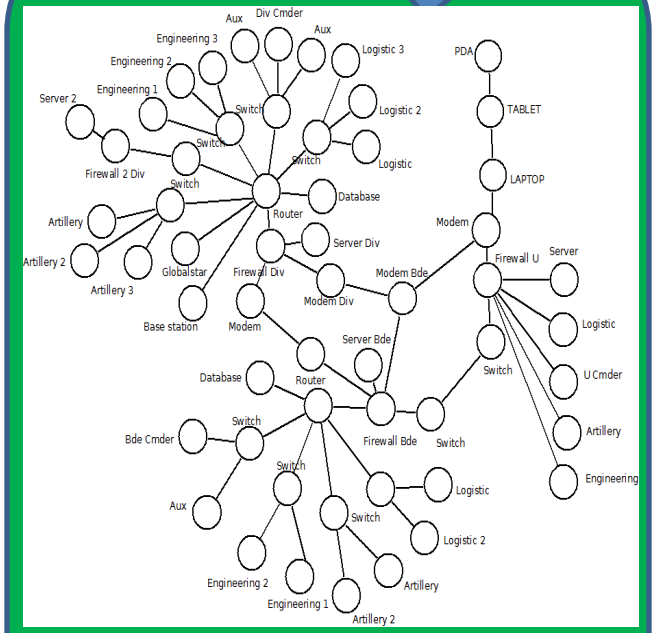


Cyber Simulation Module
(CyberModule)

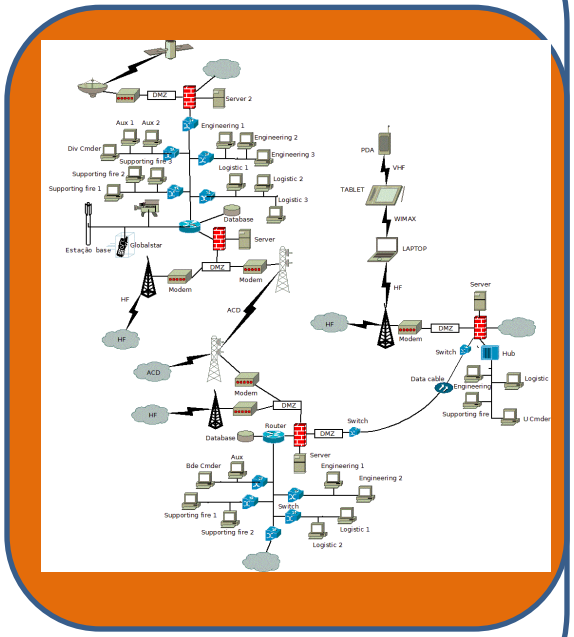
Case Study 1 - Evaluation without the cyber-attack

Simplified Architecture

Data flow



Core Simulation Manager



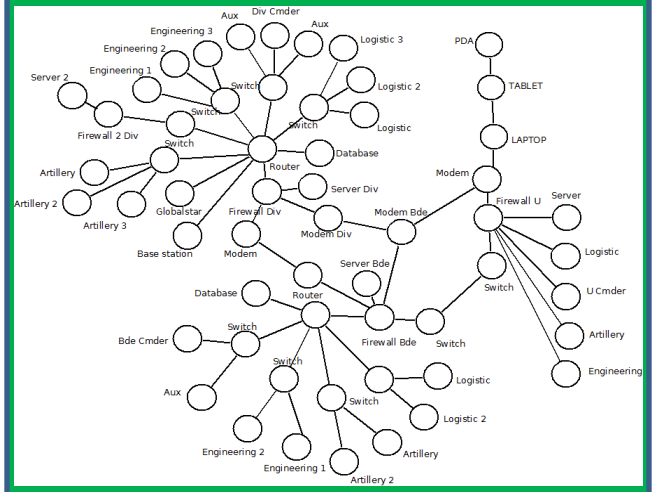
Operational Simulation Module (OperaModule)

Table of values

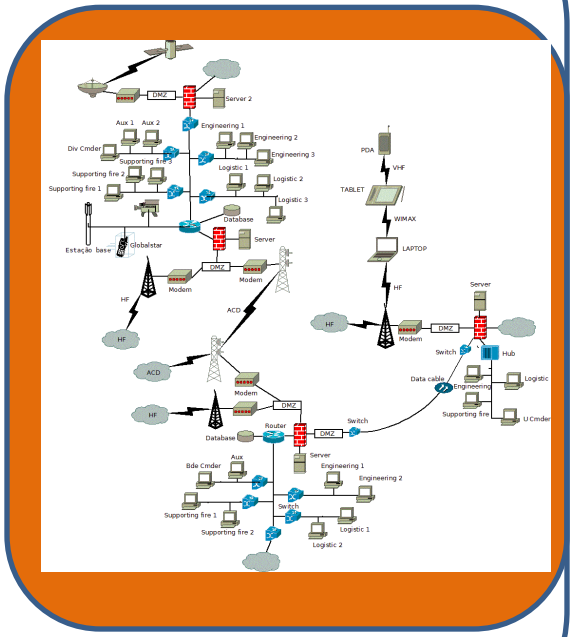
Cyber Simulation Module (CyberModule)

Simplified Architecture

Operational Simulation Module
(OperaModule)

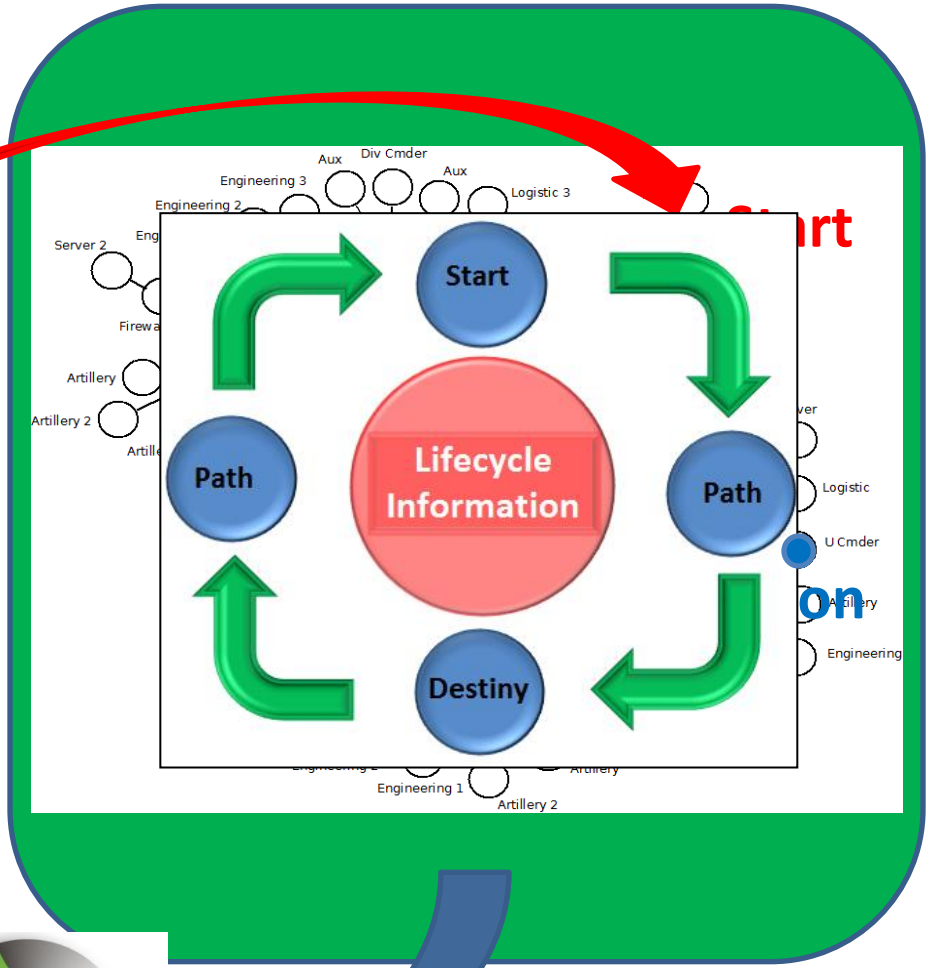


Core
Simulation Manager
(CSimMan)



Cyber Simulation Module
(CyberModule)

Architecture Expanded



Operational Simula[illegible] Module (OperaModule)

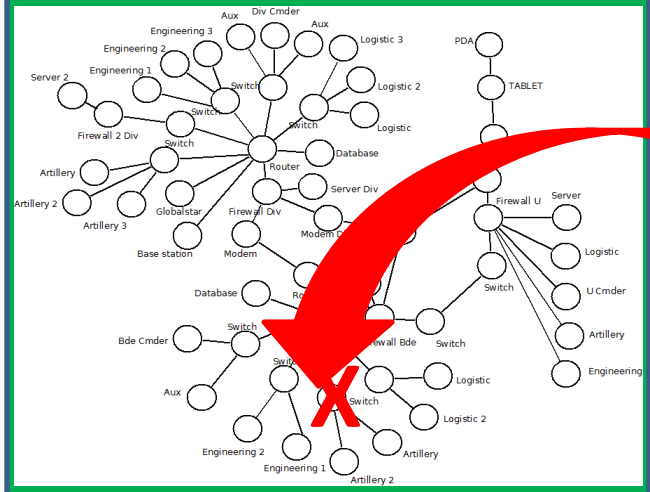
Core S[illegible]ulation Manager (CSimMan)

Case Study 2 - Evaluation with the cyber attack

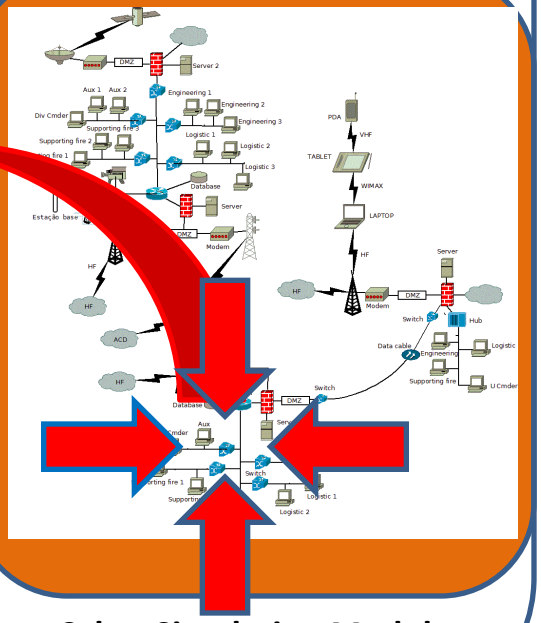
Simplified Architecture

Data flow

Operational Simulation Module
(OperaModule)



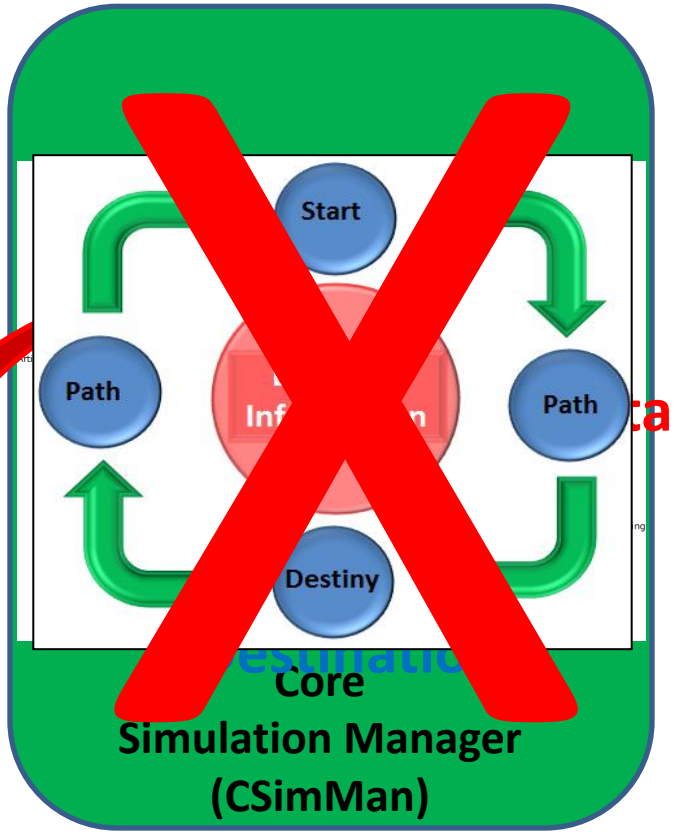
Core
Simulation Manager
(CSimMan)



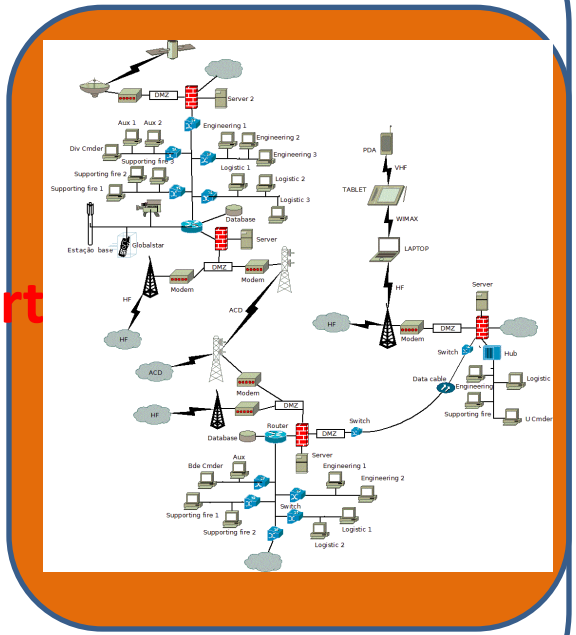
Cyber Simulation Module
(CyberModule)

Simplified Architecture

Operational Simulation Module (OperaModule)



Core Simulation Manager (CSimMan)



Cyber Simulation Module (CyberModule)

Denial of Service Attack

Architecture evaluation

In resume:

Fuel

Architecture evaluation

In resume:

PROPAGATE

Operational Simulation Module

We can have many vulnerabilities in the network.

We don´t have resources, time and condition to address all vulnerabilities.

Main goal of the Architecture

Identify which vulnerabilities have the biggest impact on the mission.

Agenda

- Introduction
- Architecture of a cyber defense simulator
- Assessment Model
  - Tactic Level Scenario
  - Infrastructure of Information Technology
  - Evaluation through case studies
- **Final Remarks**

Final Remarks 1/2

- The study of cyber domain and its complexity has become an important topic in the military science.
- This paper proposes an architecture that enables the joining of the cyber and kinetic environments. In this sense, our contribution is a new way to accomplish this interaction.
- 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.

Final Remarks 2/2

- The proposed architecture allows the identification of the most important IT assets to a particular mission; intends to build the possible paths of information flow in the graphs; supports sequential effects (changes in the attacks and infrastructures); compares missions (with or without cyber-attack); and can be constantly updated.
- To accomplish these activities, the suggested model has a great dependence on the simulators used.

Acknowledgment

- The authors would like to thank the staff of the laboratory of Command and Control, in Instituto Tecnológico de Aeronáutica (ITA); and the Core of Cyber Defense Center.
- I would like to thank the Technology Science Department and the Brazilian Army .

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.

References

- [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.

Architecture for Cyber Defense Simulator in Military Applications

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