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

Land Data Management Program

Coordinates tactical actions

Architecture
Real environment

- Topology
- IT assets

SCAN
Operational Simulation Module (OperaModule)

- LDMP
- Input data
- Operational Simulation Module (OperaModule)

Shared Folder
- Orders
- Core Simulation Manager (CSimMan)
- Route Algorithm
- Shared Folder
- Attack
- Cyber Simulation Module (CyberModule)

Process Monitoring IT
- Input data

Simulates missions;
Shows the consequences.
Operational Simulation Module (OperaModule)

LDMP

Input data

Orders

Shared Folder

Graph Generator

Core Simulation Manager (CSimMan)

Route Algorithm

Shared Folder

Attack

Shared Folder

Cyber Simulation Module (CyberModule)

Process Monitoring IT

Input data

Network Analysis;
Identify vulnerabilities;
Deliver cyber-attacks.
Architecture

- Operational Simulation Module (OperaModule)
- LDMP
- Shared Folder
- Input data
- Orders
- Msg.
- Core Simulation Manager (CSimMan)
- Graph Generator
- Route Algorithm
- Cyber Simulation Module (CyberModule)
- Process Monitoring IT
- Data and Attack
- Input data
- Shared Folder
- Interface
- Integration
- Table of values
Architecture

Operational Simulation Module (OperaModule)
- Input data
- Orders
- Msg.

Core Simulation Manager (CSimMan)
- Graph Generator
- Route Algorithm

Cyber Simulation Module (CyberModule)
- Data
- Input data
- Msg.

LDMP
- Input data

Shared Folder
- Orders
- Msg.

Kinetic environment
- Table of values
- Integration

Cyber environment
Architecture

Operational Simulation Module (OperaModule)

Shared Folder

LDMP

Input data

Orders

Graph Generator

Core Simulation Manager (CSimMan)

Route Algorithm

Shared Folder

Shared Folder

Process Monitoring IT

Input data

Attack

Cyber Simulation Module (CyberModule)

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, it's required an IT infrastructure.
IT Infrastructure

Division

Unit

Brigade
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

Operational Simulation Module (OperaModule)

Core Simulation Manager (CSimMan)

Cyber Simulation Module (CyberModule)
Architecture Expanded

Operational Simulation Module (OperaModule)

Core Simulation 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)

Denial of Service Attack
Simplified Architecture

Core Simulation Manager (CSimMan)

Operational Simulation Module (OperaModule)

Cyber Simulation Module (CyberModule)

Denial of Service Attack
Architecture evaluation

In resume:
Architecture evaluation

In resume:

- PROPAGATE

- DENIED

- 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


References


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