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

• Introduction

• Related Work

• Functionalities of the Architecture
  - Identification of Vulnerabilities
    – Identification of Impacts of a Cyber Attack
    – Mission Planning

• Assessment

• Final Remarks
Architecture for Cyber Defense Simulator in Military Applications

Authors:
Maj André Ferreira Alves Machado
Maj Alexandre B. Barreto
Prof. Edgar Toshiro Yano
Any tactical event occurs only when we have an order or make a request.

So, we need a flow of information.
Architecture (overview)
✓ Tactical actions

✓ Network topology
✓ IT assets

Real Environment

TOp Sim

ITM2

CyberSim

Input
Output

 Network topology
 IT assets

Tactical actions
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

<table>
<thead>
<tr>
<th>Mission</th>
<th>Type</th>
<th>Mission Status</th>
<th>Cyber Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Attack order</td>
<td>Safe</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Artillery Support</td>
<td>Unsafe</td>
<td>Assets A and B</td>
</tr>
<tr>
<td>3</td>
<td>Move order</td>
<td>Unsafe</td>
<td>Assets B and C</td>
</tr>
</tbody>
</table>
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).
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.
<table>
<thead>
<tr>
<th>Planning Alpha</th>
<th>Planning Beta</th>
<th>Planning Gamma</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Planning Alpha" /></td>
<td><img src="image2" alt="Planning Beta" /></td>
<td><img src="image3" alt="Planning Gamma" /></td>
</tr>
<tr>
<td><img src="image4" alt="Planning Alpha" /></td>
<td><img src="image5" alt="Planning Beta" /></td>
<td><img src="image6" alt="Planning Gamma" /></td>
</tr>
<tr>
<td><strong>2 links</strong></td>
<td><strong>3 links</strong></td>
<td><strong>5 links</strong></td>
</tr>
</tbody>
</table>
• 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]

<table>
<thead>
<tr>
<th>Mission</th>
<th>Priority</th>
<th>Planning</th>
<th>Vulnerabilities</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Before the planning</td>
<td>After planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Before the planning</td>
<td>After planning</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Estimated Assets</th>
<th>Graph Nodes</th>
<th>Graph Edges</th>
<th>Average Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,620</td>
<td>1,620</td>
<td>2,000</td>
<td>79.8 ms</td>
</tr>
<tr>
<td>4,050</td>
<td>4,050</td>
<td>5,000</td>
<td>90.1 ms</td>
</tr>
<tr>
<td>40,500</td>
<td>40,500</td>
<td>50,000</td>
<td>1,570 ms</td>
</tr>
<tr>
<td>65,000</td>
<td>65,000</td>
<td>80,000</td>
<td>3,575 ms</td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>Estimated Assets</th>
<th>Graph Nodes</th>
<th>Graph Edges</th>
<th>Average Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,620</td>
<td>1,620</td>
<td>2,000</td>
<td>4.77 ms</td>
</tr>
<tr>
<td>4,050</td>
<td>4,050</td>
<td>5,000</td>
<td>12 ms</td>
</tr>
<tr>
<td>40,500</td>
<td>40,500</td>
<td>50,000</td>
<td>221.5 ms</td>
</tr>
<tr>
<td>65,000</td>
<td>65,000</td>
<td>80,000</td>
<td>229.25 ms</td>
</tr>
</tbody>
</table>
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.
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


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