NORTHROP GRUMMAN

Architecture Design, Simulation and Visualization Using SysML

August 18, 2010

Gundars Osvalds
Senior Principal Enterprise Architect
gundars.osvalds@ngc.com

Northrop Grumman
Information Systems Sector
Intelligence Systems Division
Essex Business Unit

Objectives

NORTHROP GRUMMAN

- Motivation and description of an Model-Based Systems Engineering (MBSE) approach
- Present a sample Architecture, Simulation and Visualization
- Application of processes and tools for MBSE
  - OMG Systems Modeling Language (SysML)
  - IBM Rational Harmony Process for Systems Engineers
  - IBM Rational Rhapsody modeling tool for SysML and Harmony

Agenda

NORTHROP GRUMMAN

- Applying Modeling and Simulation for Systems Engineering
- Conceptual Model – Black Box
- Logical Model – White Box
- Visualization – Executable Model

Outline

NORTHROP GRUMMAN

- Applying Modeling and Simulation to System Engineering
  - Architectural Modeling Purpose
  - Advantages Model Based Systems Engineering (MBSE)
  - SysML and Model Based Systems Engineering
  - SysML Model Functional Grouping
  - MBSE Process Using SysML Rhapsody and Harmony
  - Application of Modeling
  - Demo Problem Description

Architectural Modeling Purpose

NORTHROP GRUMMAN

- Why
  - To provide a solution that satisfies the Stakeholders
- When
  - Before implementation is started
- What
  - Documents the design of the solution
- How
  - Use the Systems Modeling Language (SysML) specification for models
- Where
  - Executable Architecture provides system Simulation and Visualization
- Who
  - Systems Engineer and Architect

Advantages of Model Based Systems Engineering (MBSE)

NORTHROP GRUMMAN

- Provides a mechanism to capture and verify requirements
- Requirements can be allocated and traced to its source
- Diagrams are integrated with each other to provide a cohesive view of the architecture
- Models are used to define message definition and port interfaces that define the systems interface specification
- System integration and testing risks are reduced with the use of model diagrams that are the basis for system specifications and test plans
- Objects can be defined with interfaces (messages, message formats, and ports) and functions be defined with models that can be simulated

SysML and Model Based Systems Engineering (MBSE)

NORTHROP GRUMMAN

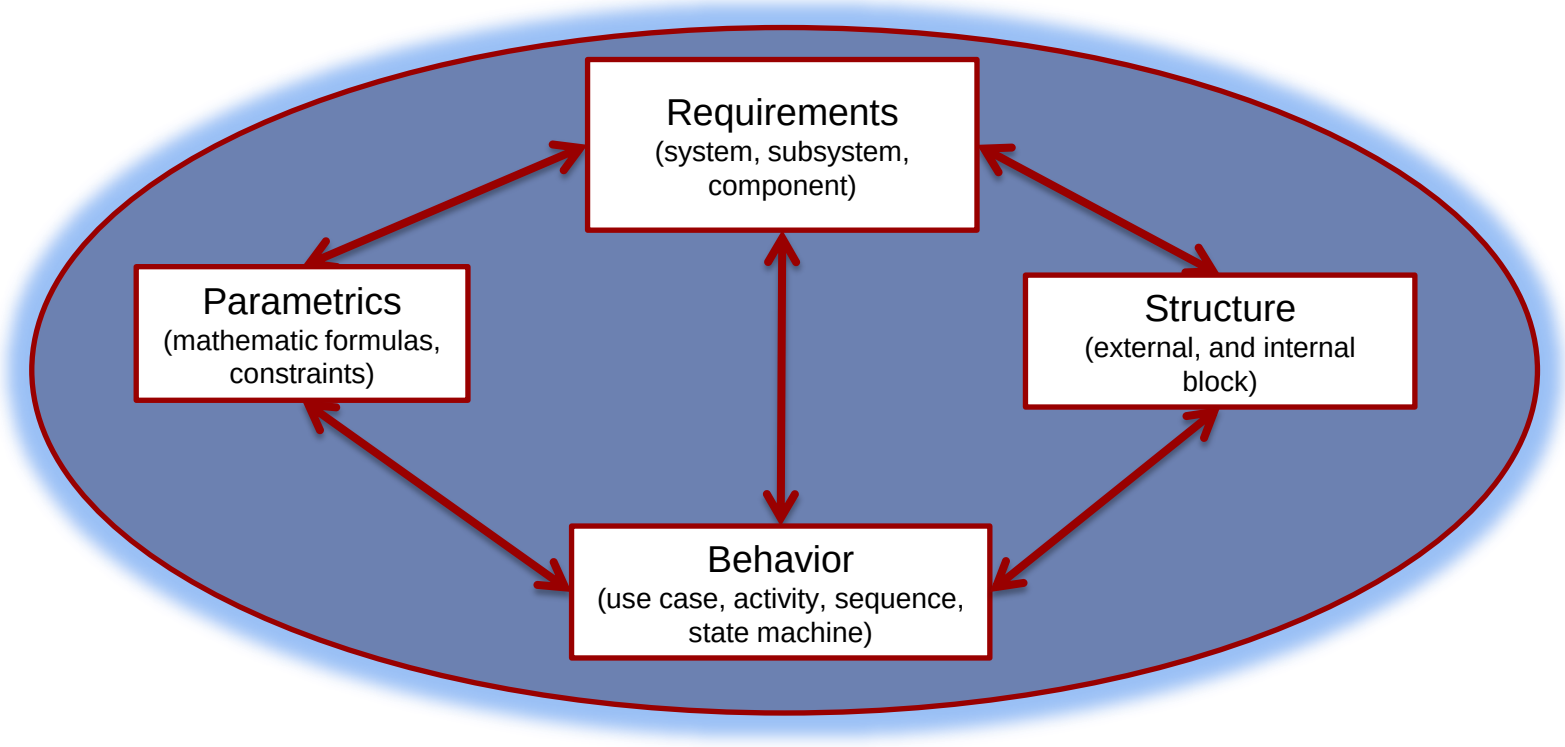
- SysML was developed as an extension to UML to provide a modeling capability for the Systems Engineers to create static and dynamic models of the systems architecture

- Uses SysML to:
  - Support the concepts of describing a model with all activities performed by one or more system scenarios
  - Provide allocation of scenario activates to objects that can then be defined as system hardware components
  - Implement the architectural model using state diagram that when executed provide a simulation of the scenario execution on the architectural model
  - Provides a verification of model execution state diagram functionality against the designed scenario activities and interactions between actors and the system

SysML Model Functional Grouping

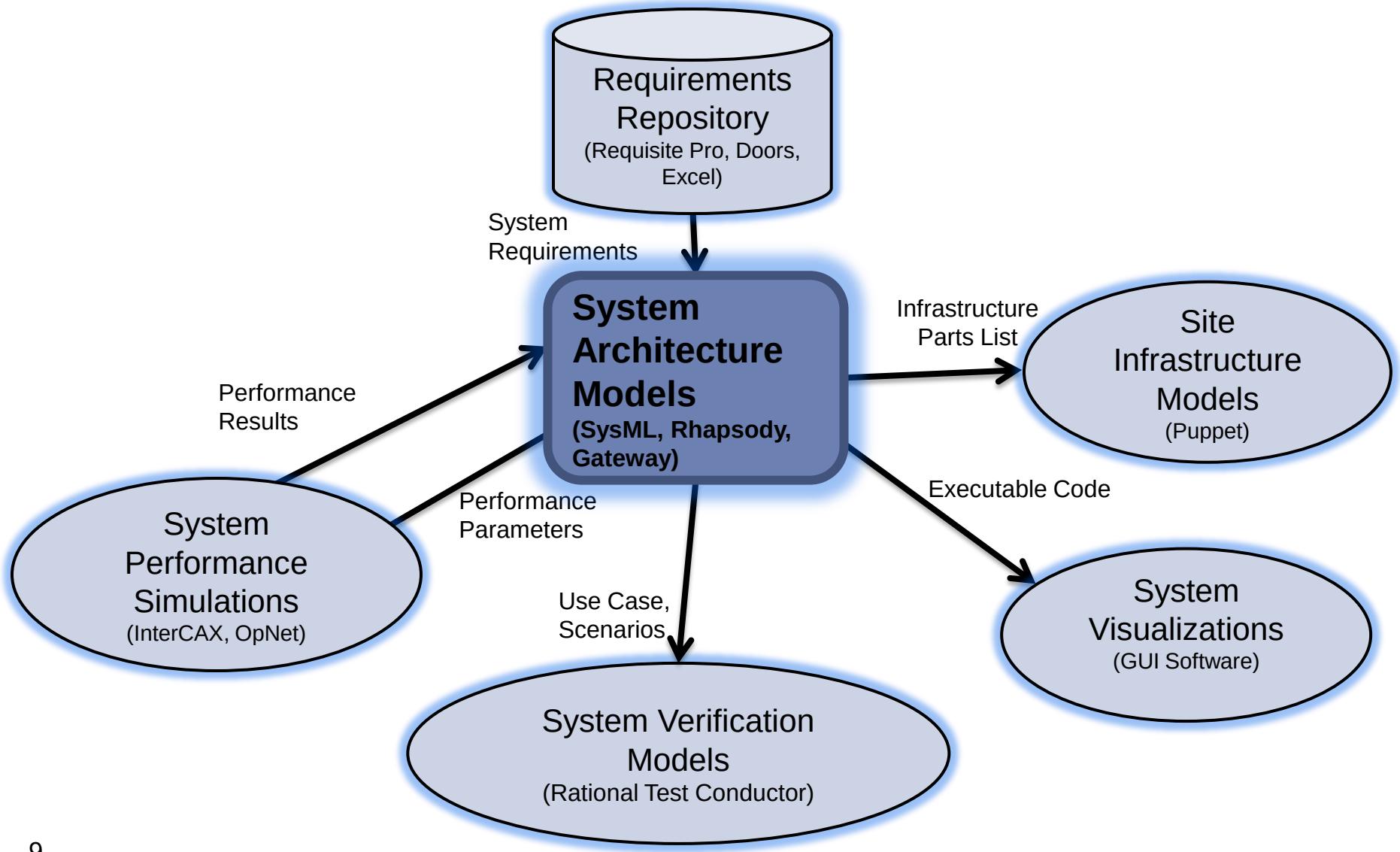
NORTHROP GRUMMAN

- SysML can be grouped into four functional areas
  - Each group is implemented using the shown SysML diagrams
  - The groups also interact with each other to provide a cohesive architectural model



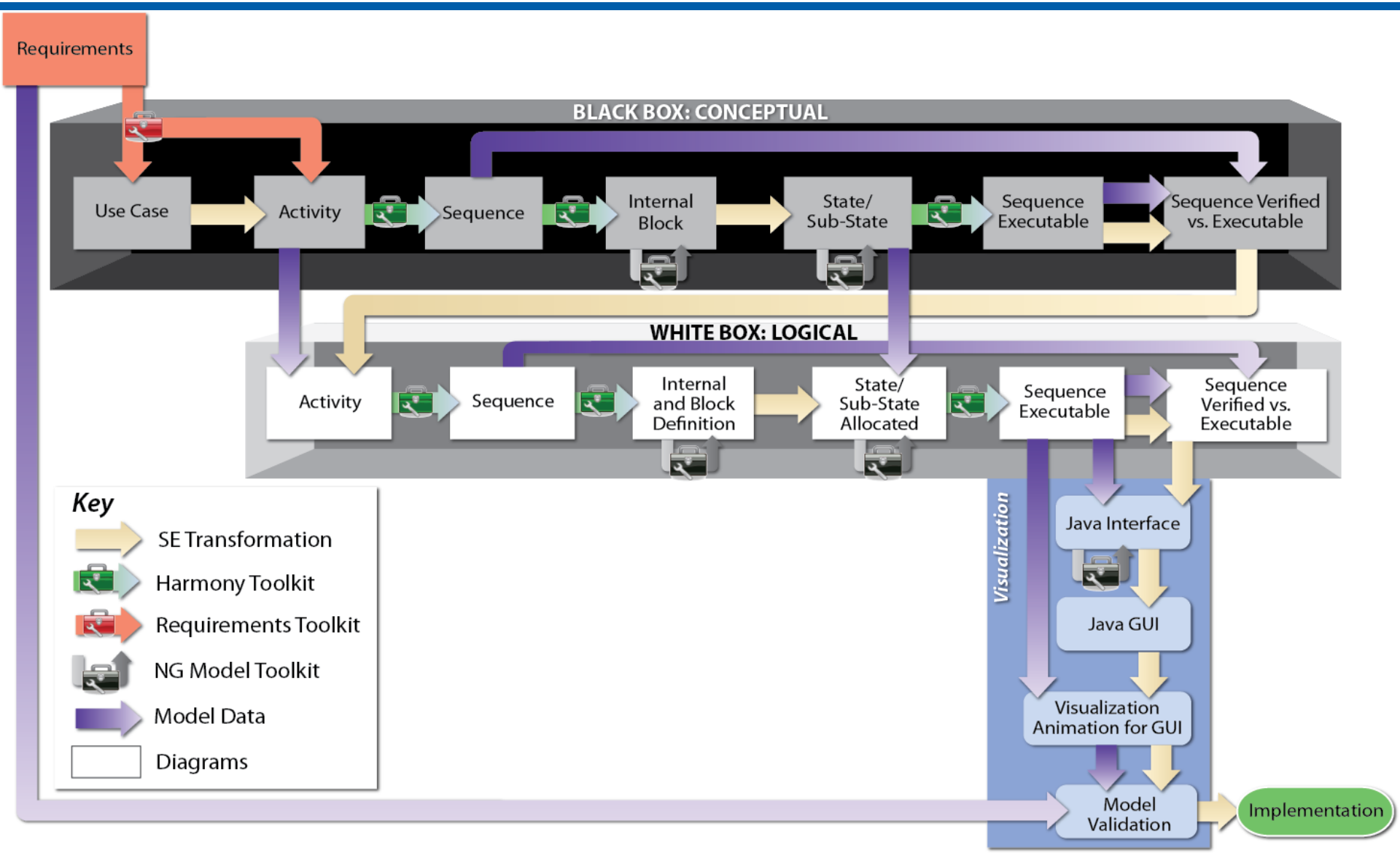
Model Based Systems Engineering Framework

NORTHROP GRUMMAN



MBSE Process Using SysML Rhapsody and Harmony

NORTHROP GRUMMAN



Application of Modeling

NORTHROP GRUMMAN

Modeling artifacts can support the development of:

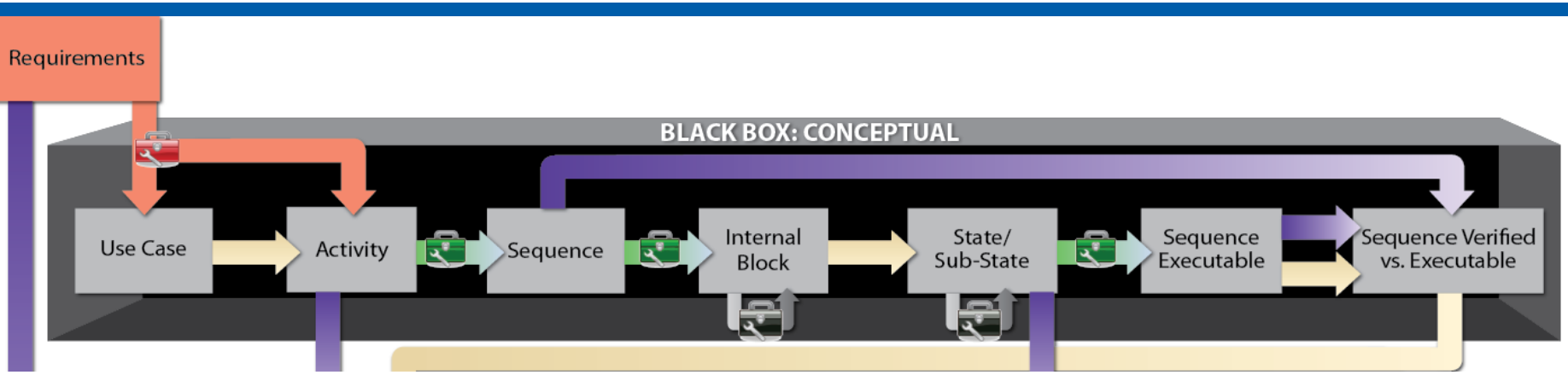
- Concept of Operations specification (CONOP)
- System Capabilities Validation
- Architecture Design
- System Data use and flow
- Component Specifications
  - Software
  - Hardware
- Inputs to OpNet performance modeler
  - Architecture
  - Scenarios
- Software
  - Activities
  - Messages
  - Data
- Hardware
  - Parts list
  - Interconnect diagram
- System Interface Verification
- Test Plans

Demo Problem Description

NORTHROP GRUMMAN

- Data Exfiltration Using Botnet Demo
  - Hacker wants to gain access to User data on his system and have it sent back
  - Hacker created a Botnet consisting of multiple Drones (use of un-secure computers) that are used to attack the User
  - On each Drone the hacker uses a Command and Control Computer to remotely install Malware
  - User protection consists of a Firewall and Analyst to evaluate questionable messages
  - If Firewall or Analyst determine message sent is an attack then the message is blocked from accessing the Users system
  - If Malware command gets through (unrecognized signature) the Firewall and Analyst then the Malware downloads data from the Users system to the Hacker

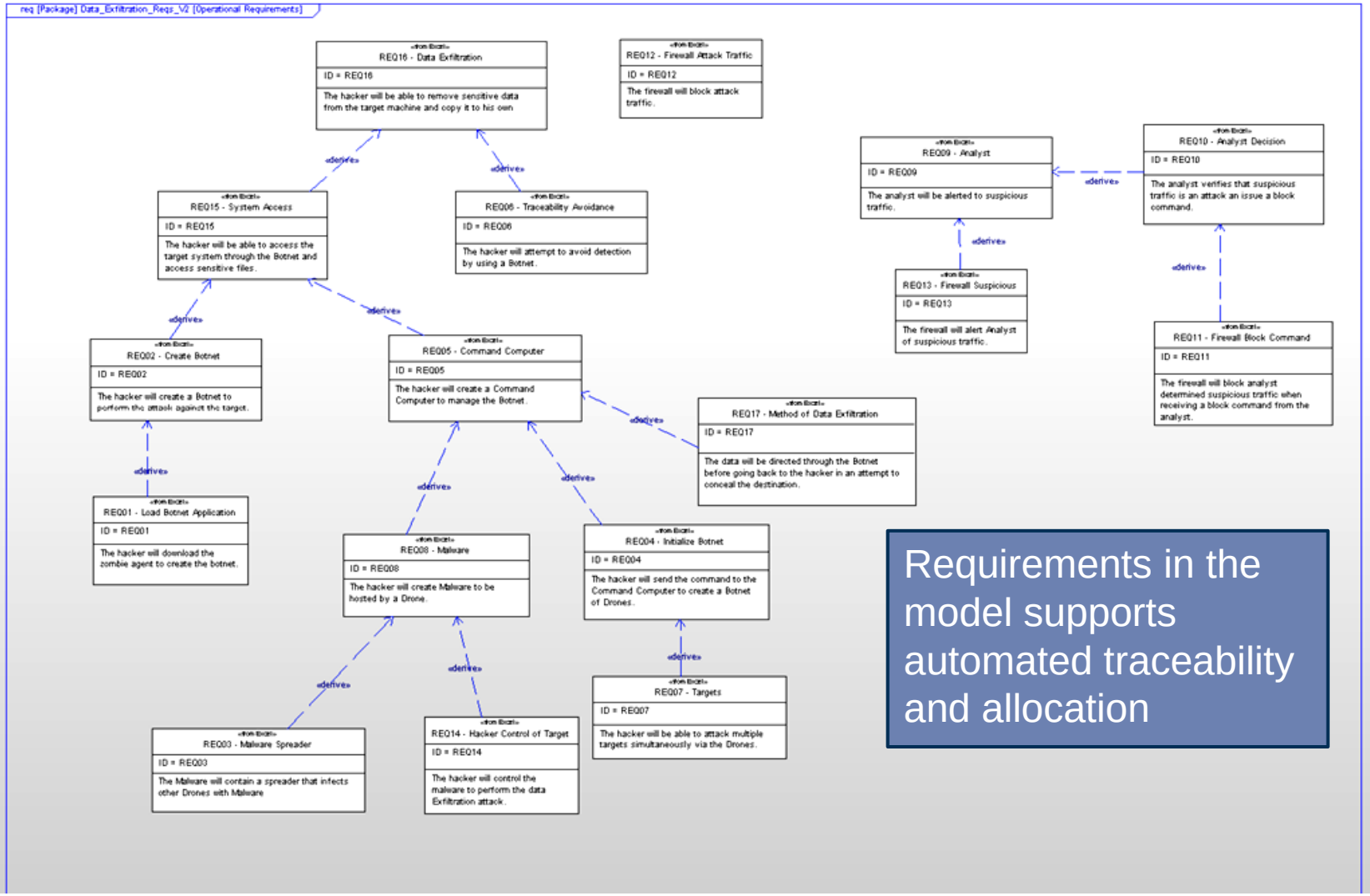
Conceptual Model - Black Box



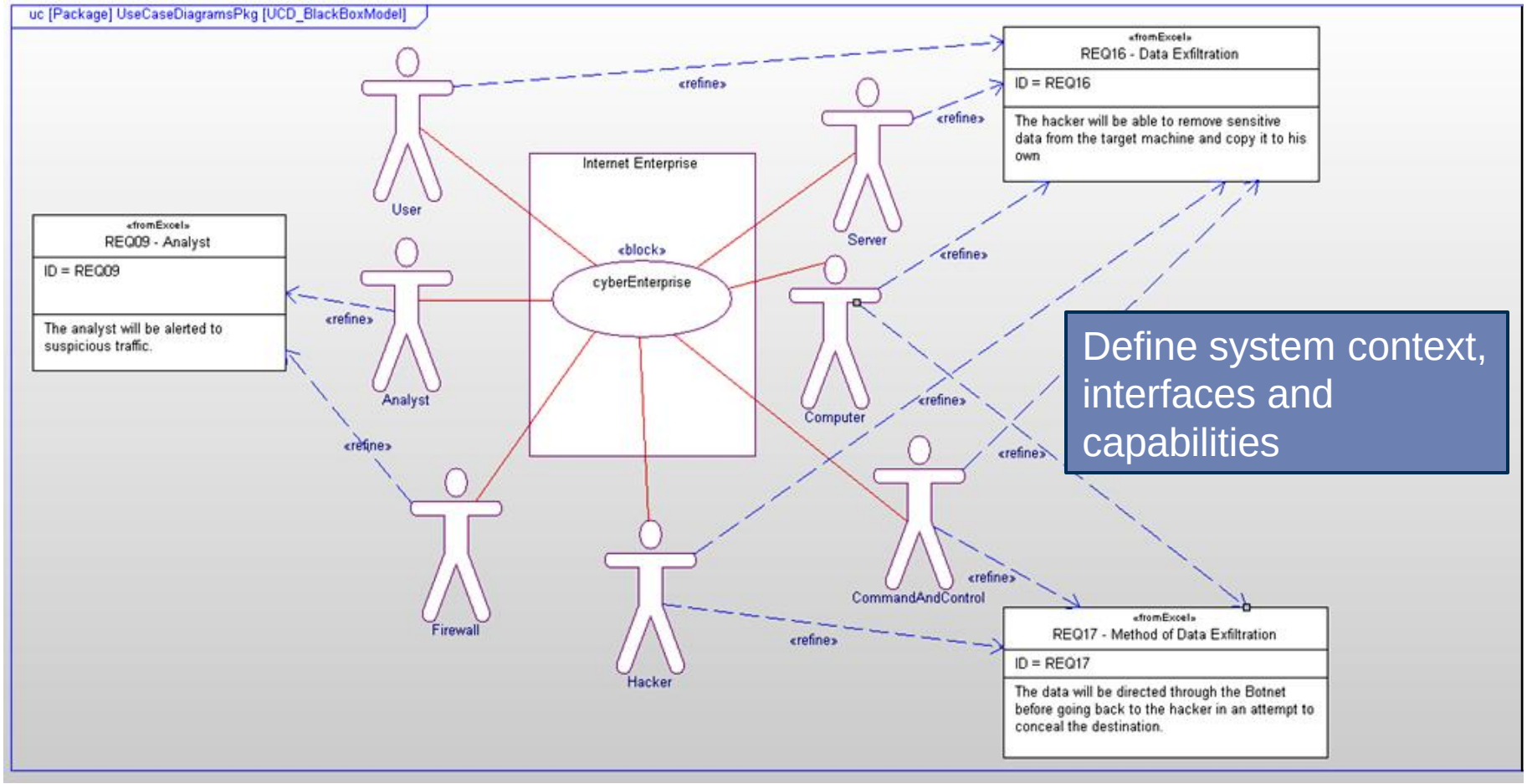
System Requirements- Black Box Diagrams

- Use Case
- Activity – Scenario
- Sequence
- Internal Block
- State
- Sub-State
- Sequence – Executable
- State – Executable
- Sequence – Verified vs. Executable

System Requirements

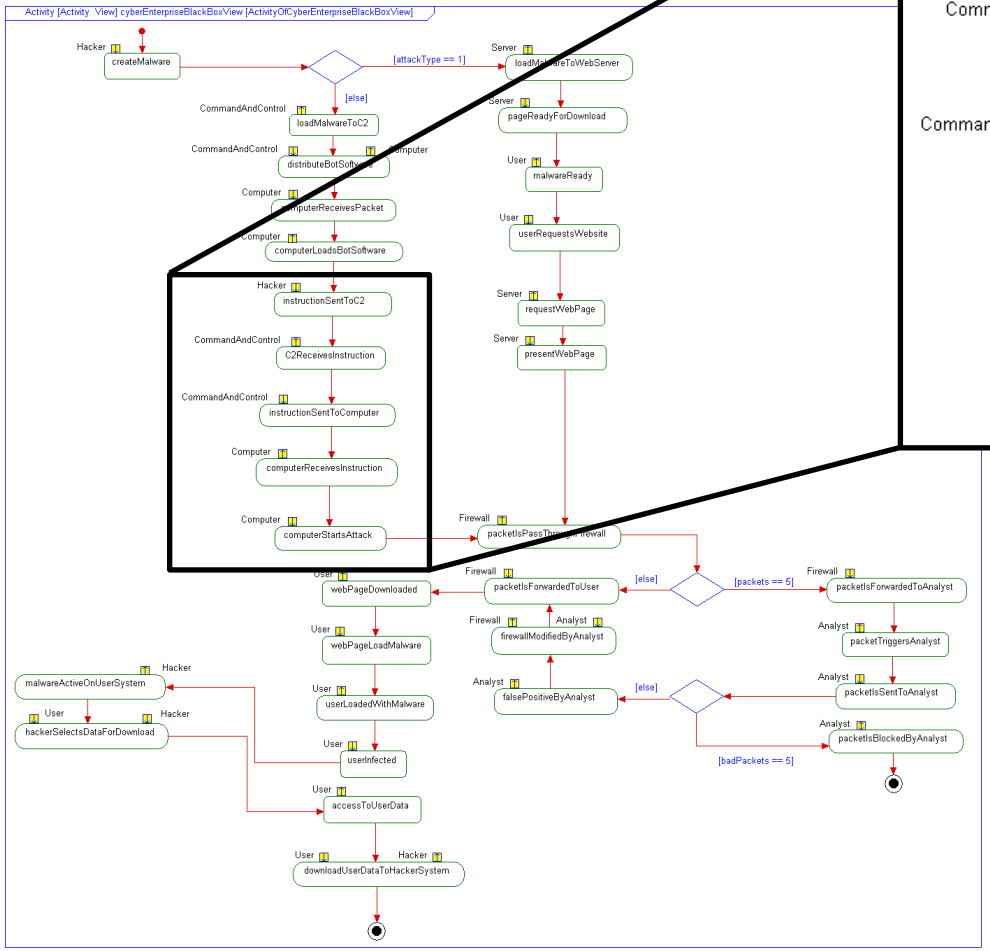


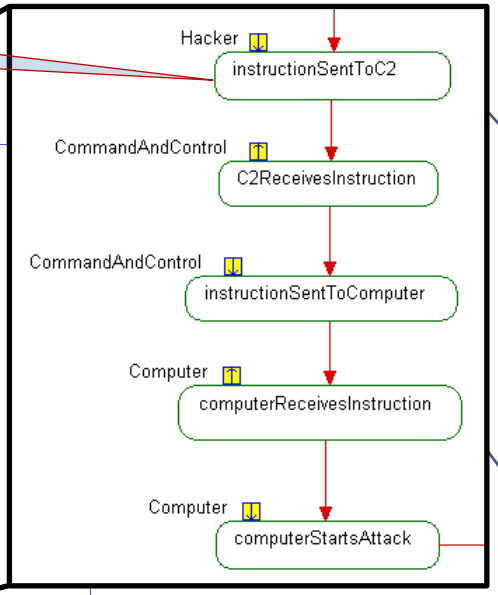
BB Use Case



BB Activity - Scenario

This activity will be highlighted throughout this presentation





<<refine>>

«fromExcel»
REQ04 - Initialize Botnet

ID = REQ04

The hacker will send the command to the Command Computer to create a Botnet of Drones.

<<refine>>

«fromExcel»
REQ06 - Traceability Avoidance

ID = REQ06

The hacker will attempt to avoid detection by using a Botnet.

Engineer define actions required to perform scenario operations

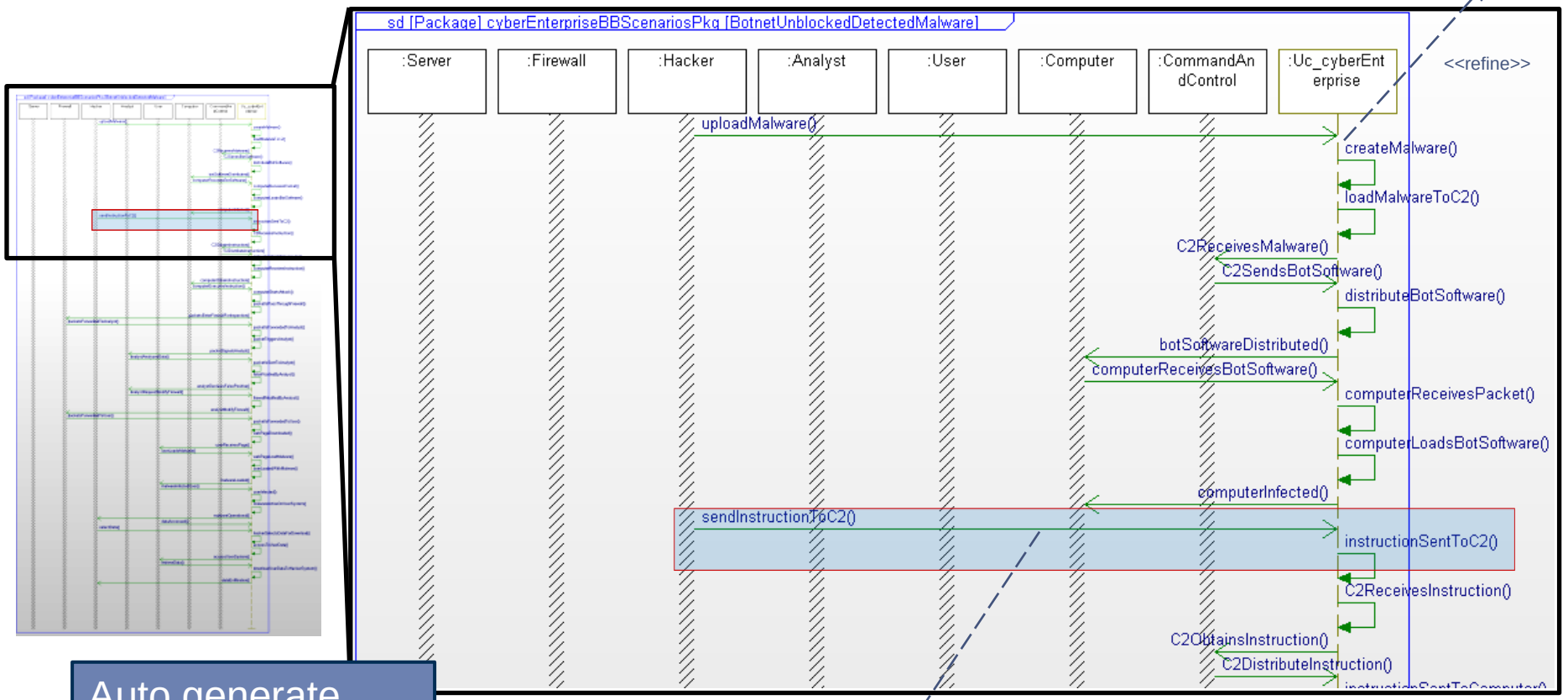
BB Sequence

NORTHROP GRUMMAN

«fromExcel»
REQ08 - Malware

ID = REQ08

The hacker will create Malware to be hosted by a Drone.



Auto generate sequences from Activity diagram

«fromExcel»
REQ04 - Initialize Botnet

ID = REQ04

The hacker will send the command to the Command Computer to create a Botnet of Drones.

<<refine>>

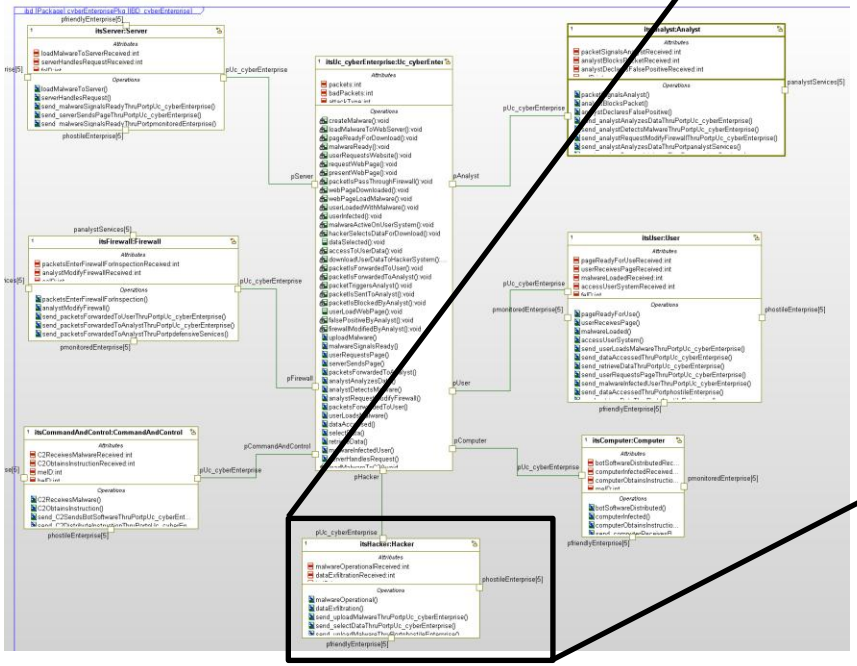
BB Internal Block

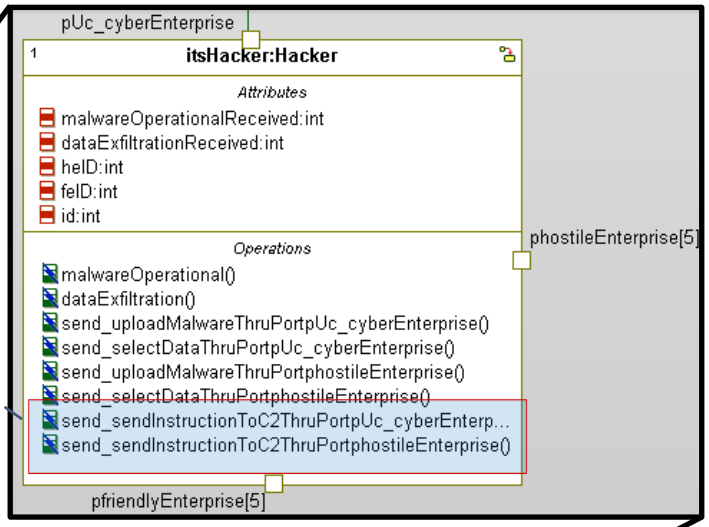
«fromExcel»
REQ04 - Initialize Botnet

ID = REQ04

The hacker will send the command to the Command Computer to create a Botnet of Drones.

<<refine>>





Auto allocate messages and operations to components

BB State

Cyber Enterprise State

«fromExcel»
REQ02 - Create Botnet

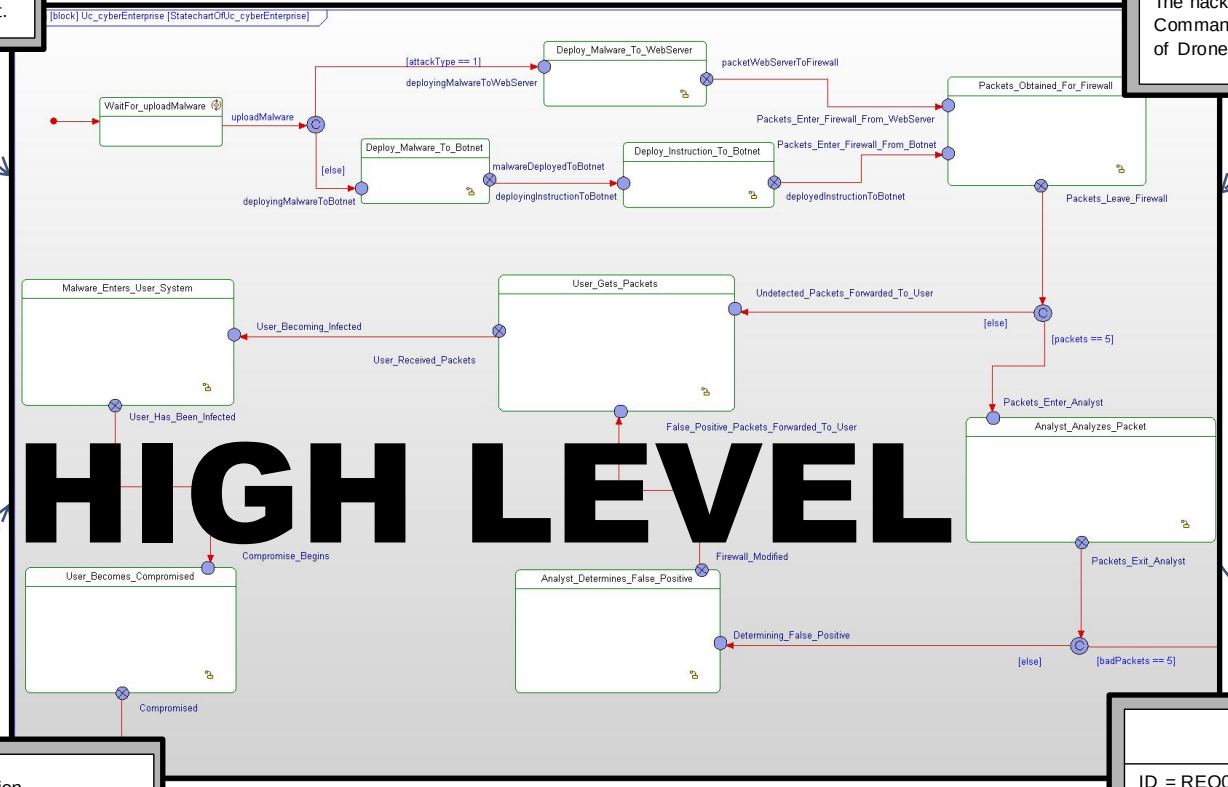
ID = REQ02

The hacker will create a Botnet to perform the attack against the target.

«fromExcel»
REQ04 - Initialize Botnet

ID = REQ04

The hacker will send the command to the Command Computer to create a Botnet of Drones.



<<refine>>

<<refine>>

<<refine>>

<<refine>>

«fromExcel»
REQ16 - Data Exfiltration

ID = REQ16

The hacker will be able to remove sensitive data from the target machine and copy it to his own

«fromExcel»
REQ09 - Analyst

ID = REQ09

The analyst will be alerted to suspicious traffic.

This is the state model of the activities defined to satisfy the requirements

BB Sub-State

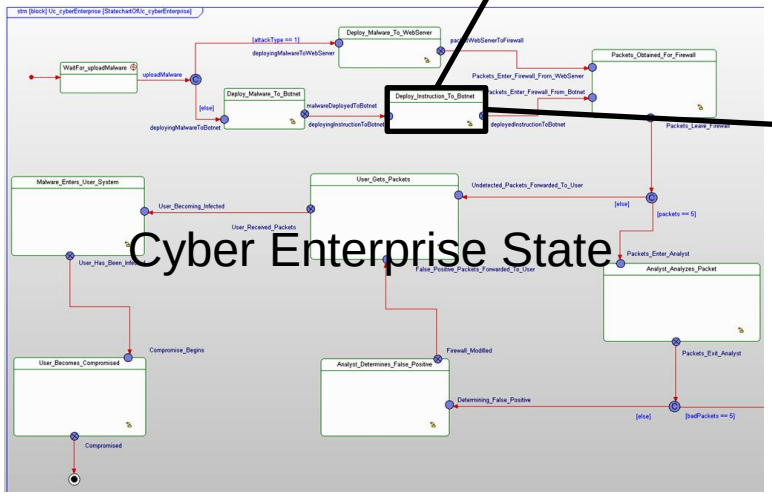
«fromExcel»
REQ04 - Initialize Botnet

ID = REQ04

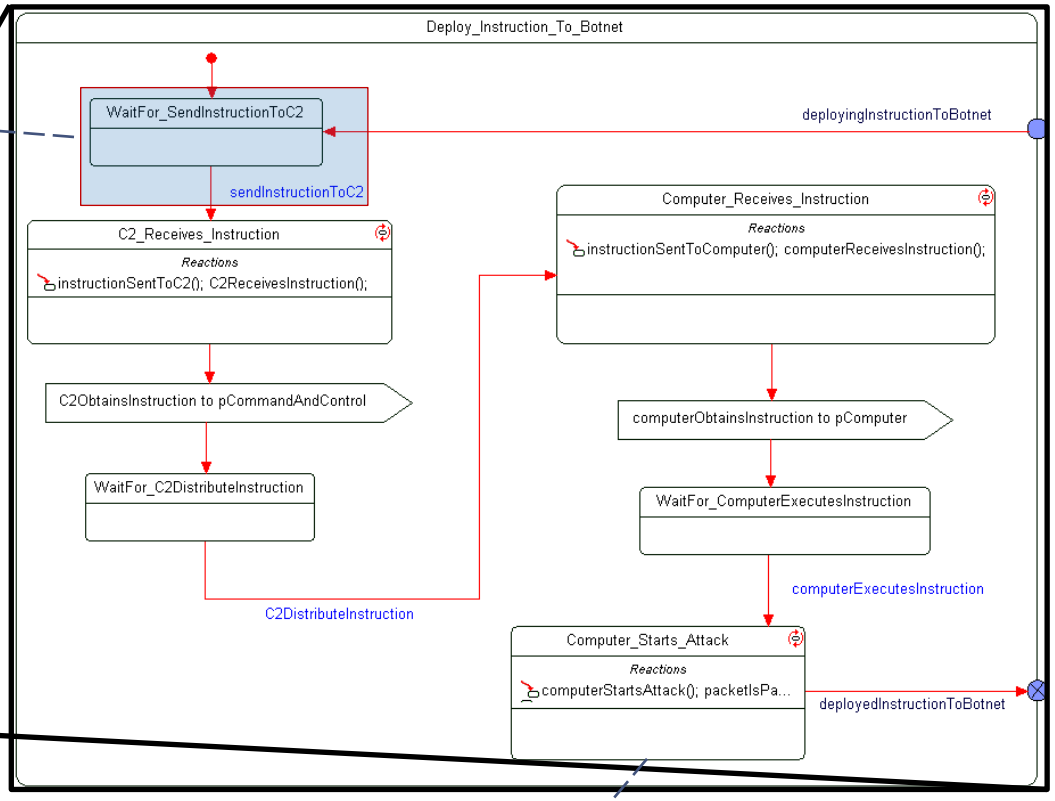
The hacker will send the command to the Command Computer to create a Botnet of Drones.

<<refine>>

Develop the behavior of systems via the executable model that is driven by the states



Cyber Enterprise State



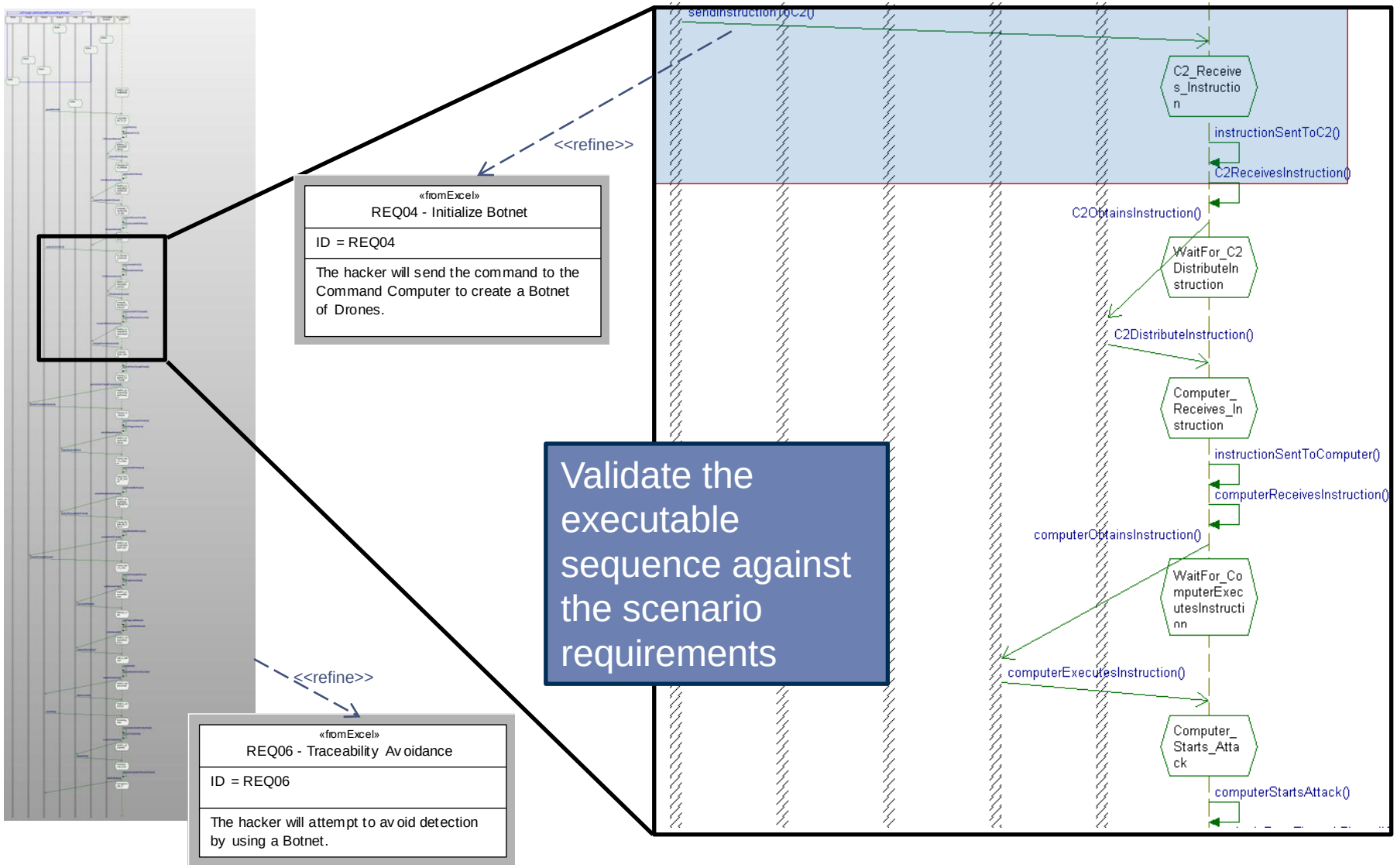
<<refine>>

«fromExcel»
REQ07 - Targets

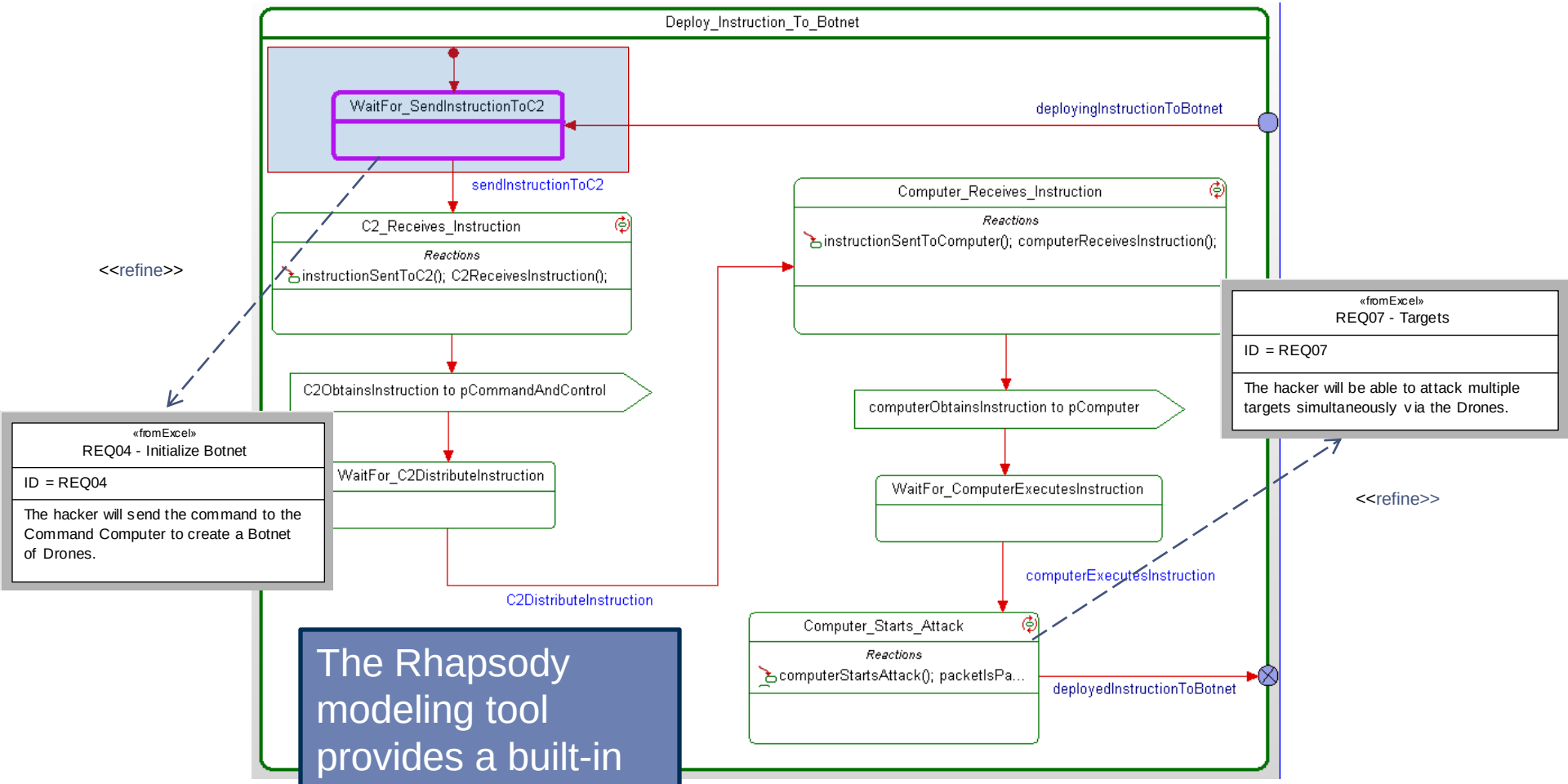
ID = REQ07

The hacker will be able to attack multiple targets simultaneously via the Drones.

BB Sequence - Executable

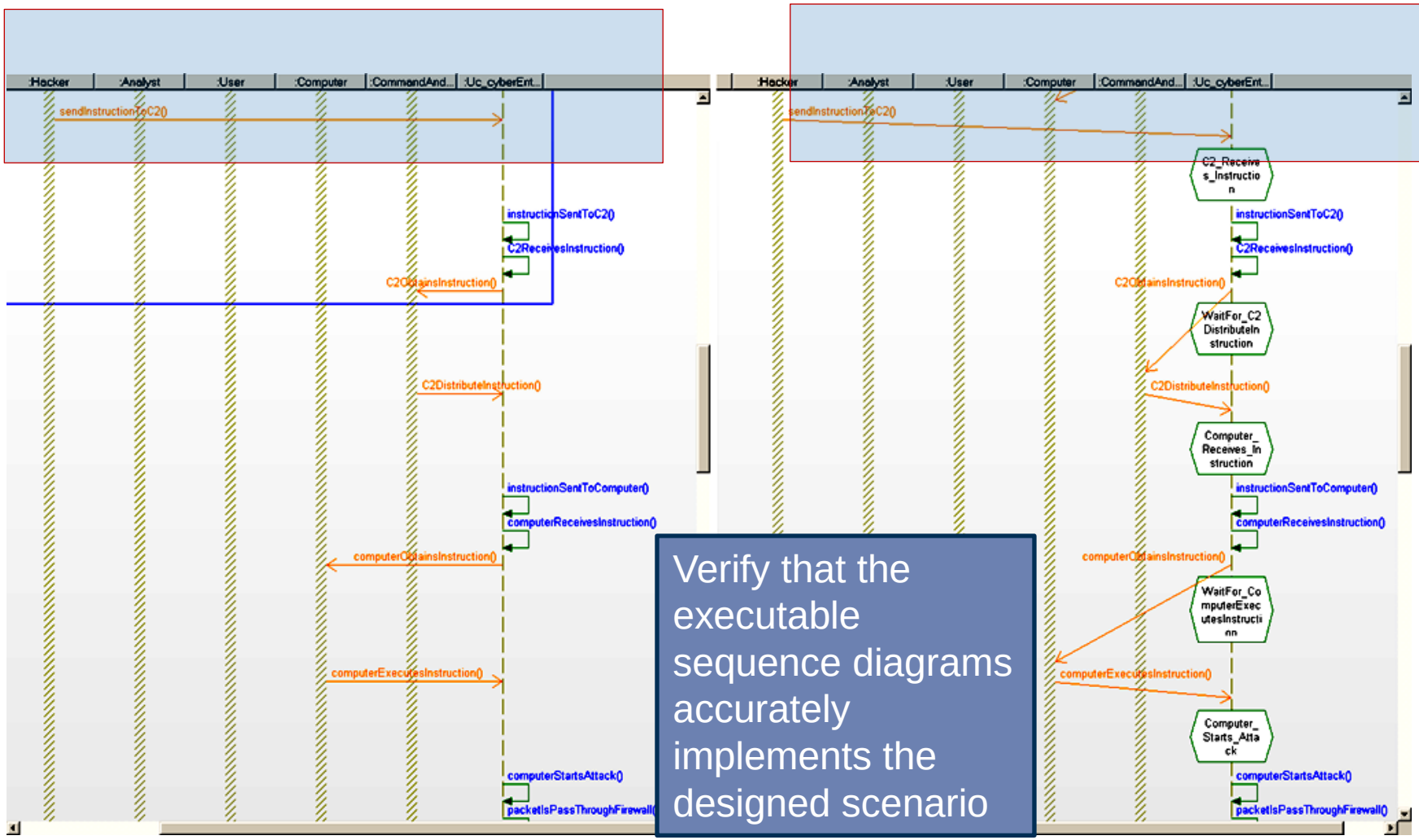


BB State – Executable - Visualized



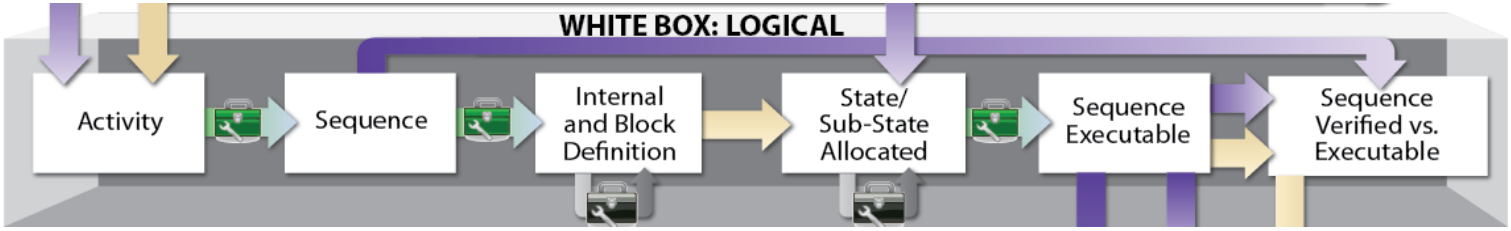
The Rhapsody modeling tool provides a built-in visualization of each state as the model is executed

BB Sequence Verified Versus Executable



Verify that the executable sequence diagrams accurately implements the designed scenario

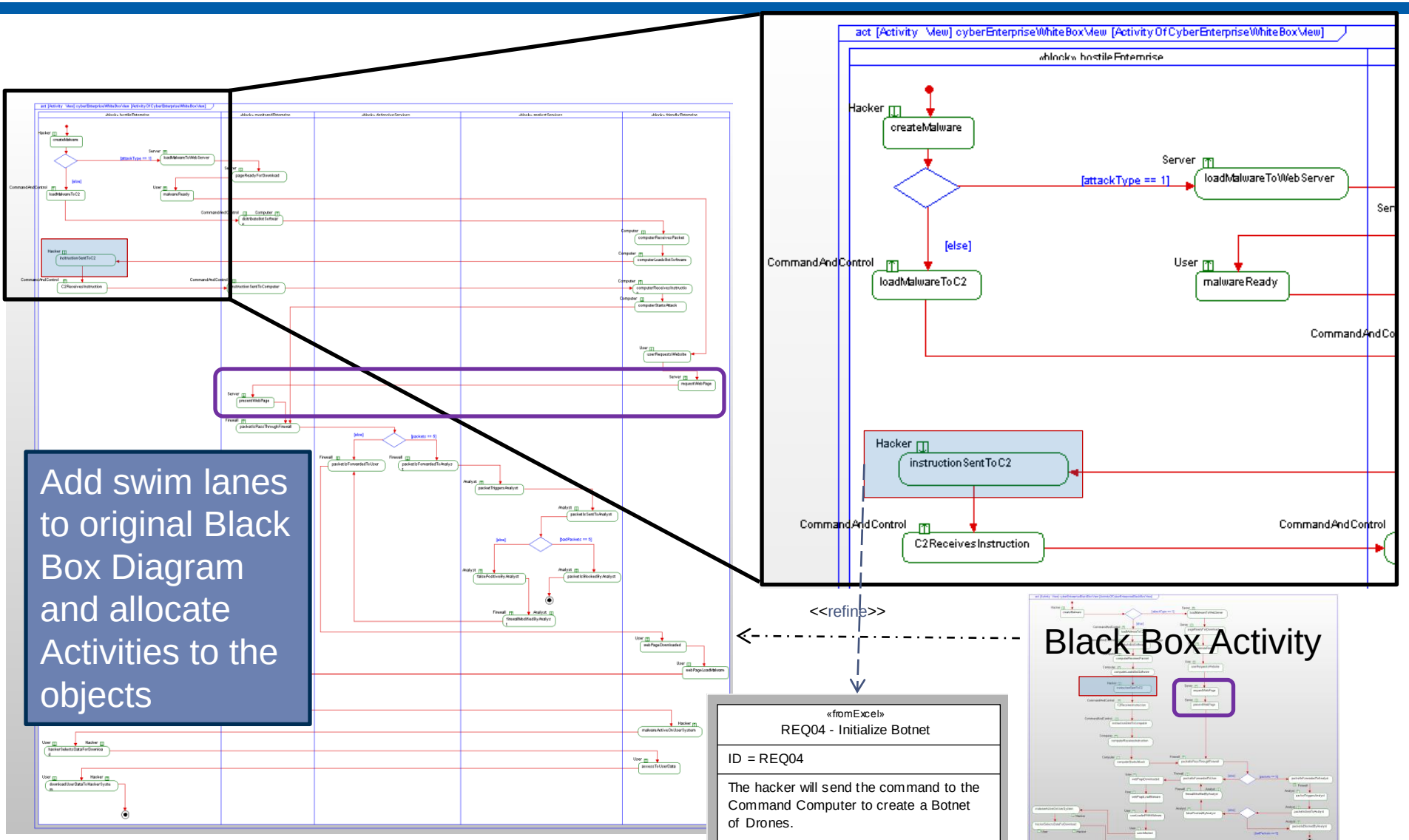
Logical Model – White Box



- White Box Diagrams
  - Activity – Swim Lanes
  - Sequence – Logical
  - Internal Block – Physical
  - Block Definition – Physical
  - State – Allocated
  - Sub-State – Allocated
  - Sequence – Executable
  - State – Executable
  - Sequence – Verified vs. Executable

WB Activity – Swim Lanes

NORTHROP GRUMMAN



WB Sequence

Presents the five objects that execute the use case functionality

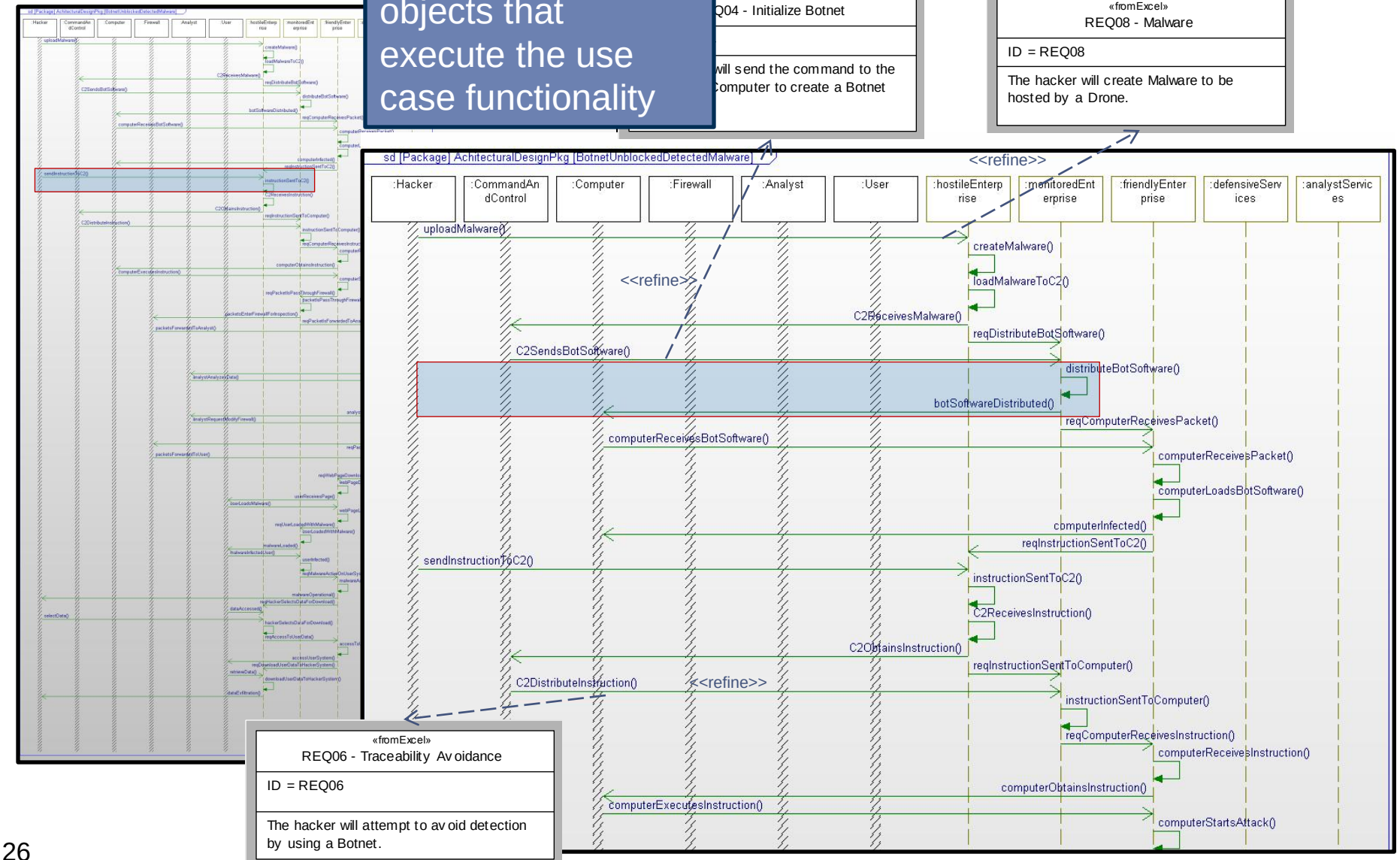
«fromExcel»
Q04 - Initialize Botnet

will send the command to the Computer to create a Botnet

«fromExcel»
REQ08 - Malware

ID = REQ08

The hacker will create Malware to be hosted by a Drone.

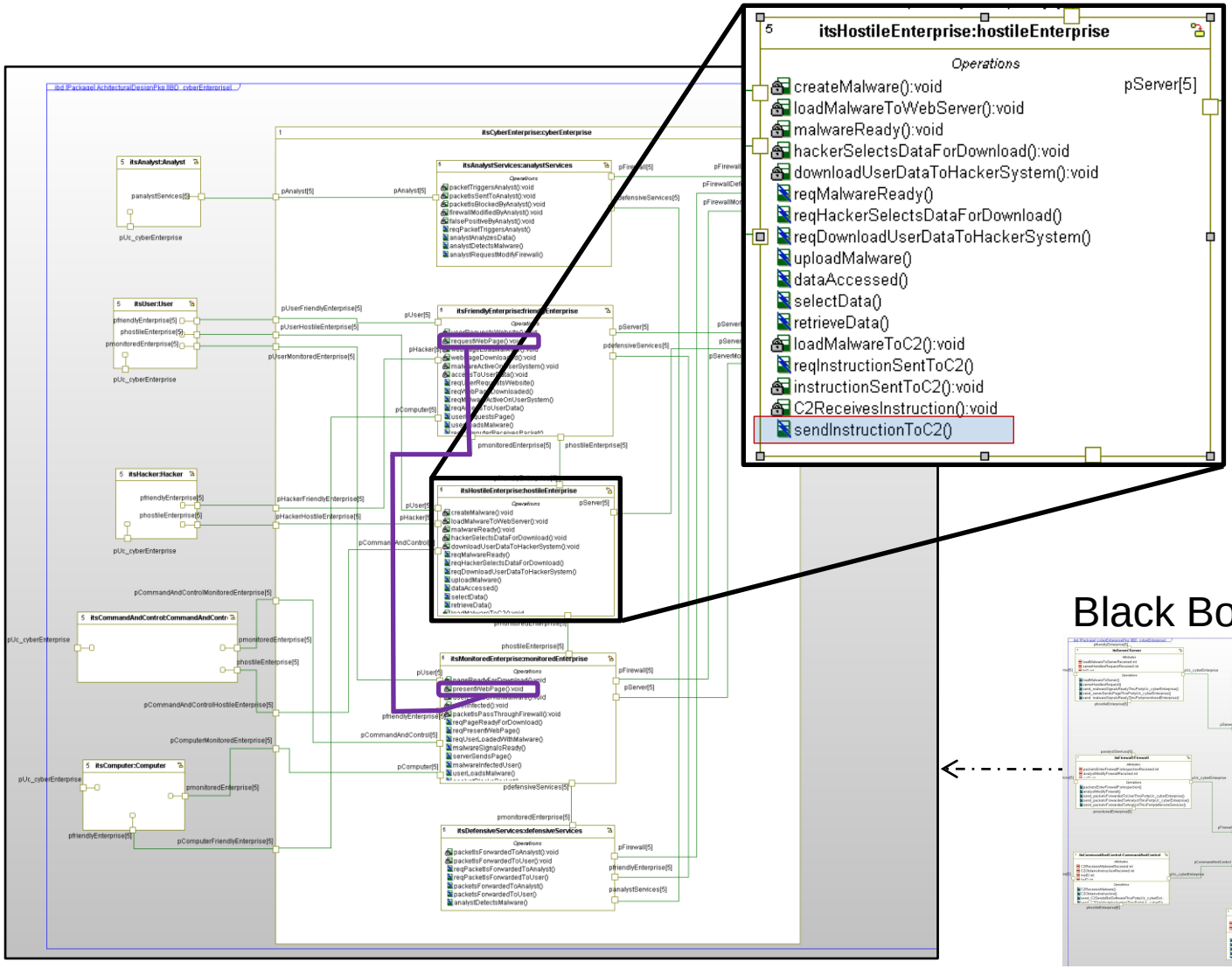


«fromExcel»
REQ06 - Traceability Avoidance

ID = REQ06

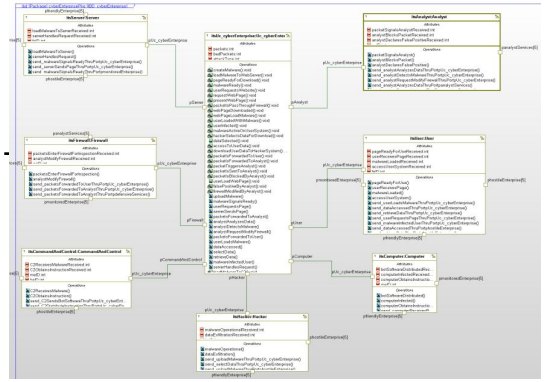
The hacker will attempt to avoid detection by using a Botnet.

WB Internal Block

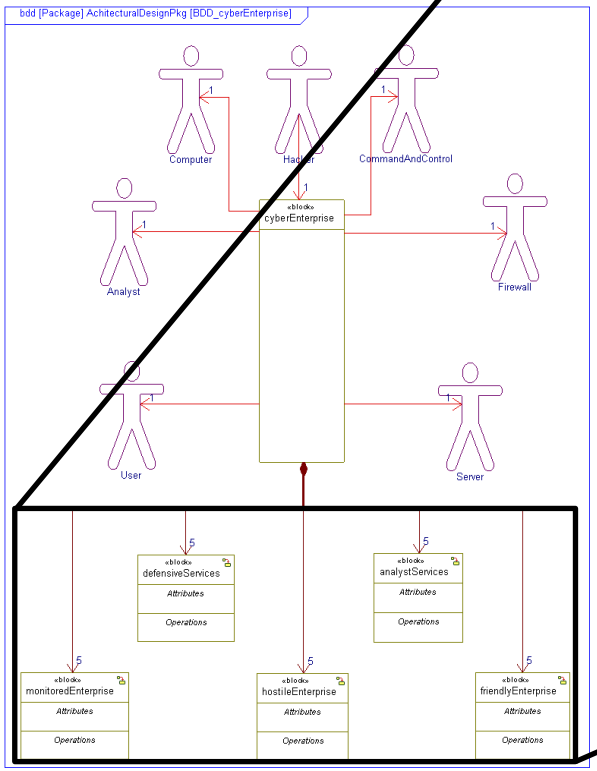


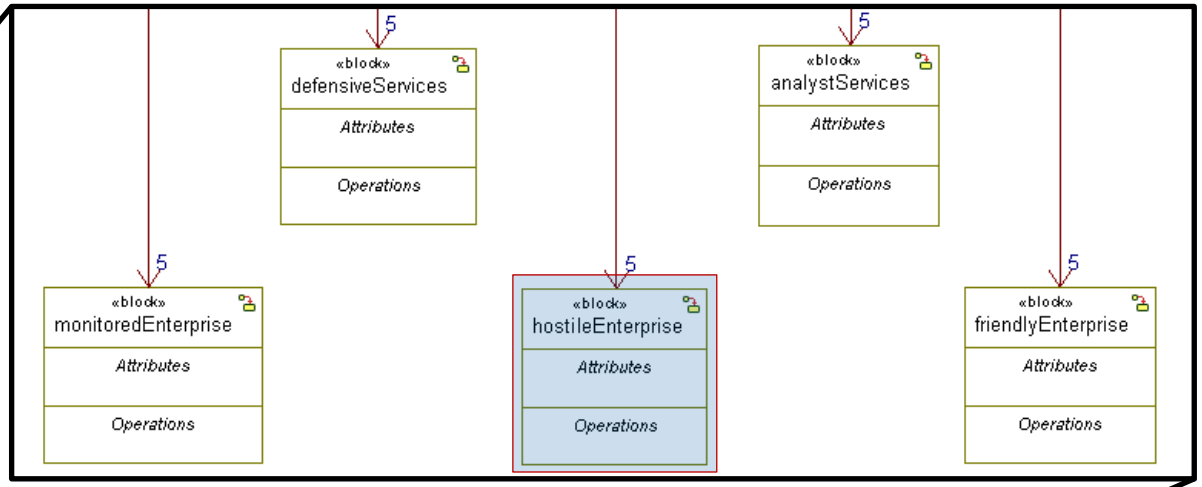
Objects are shown with Operations and Messages automatically allocated from the White Box Activity/Sequence diagrams

Black Box Internal Block



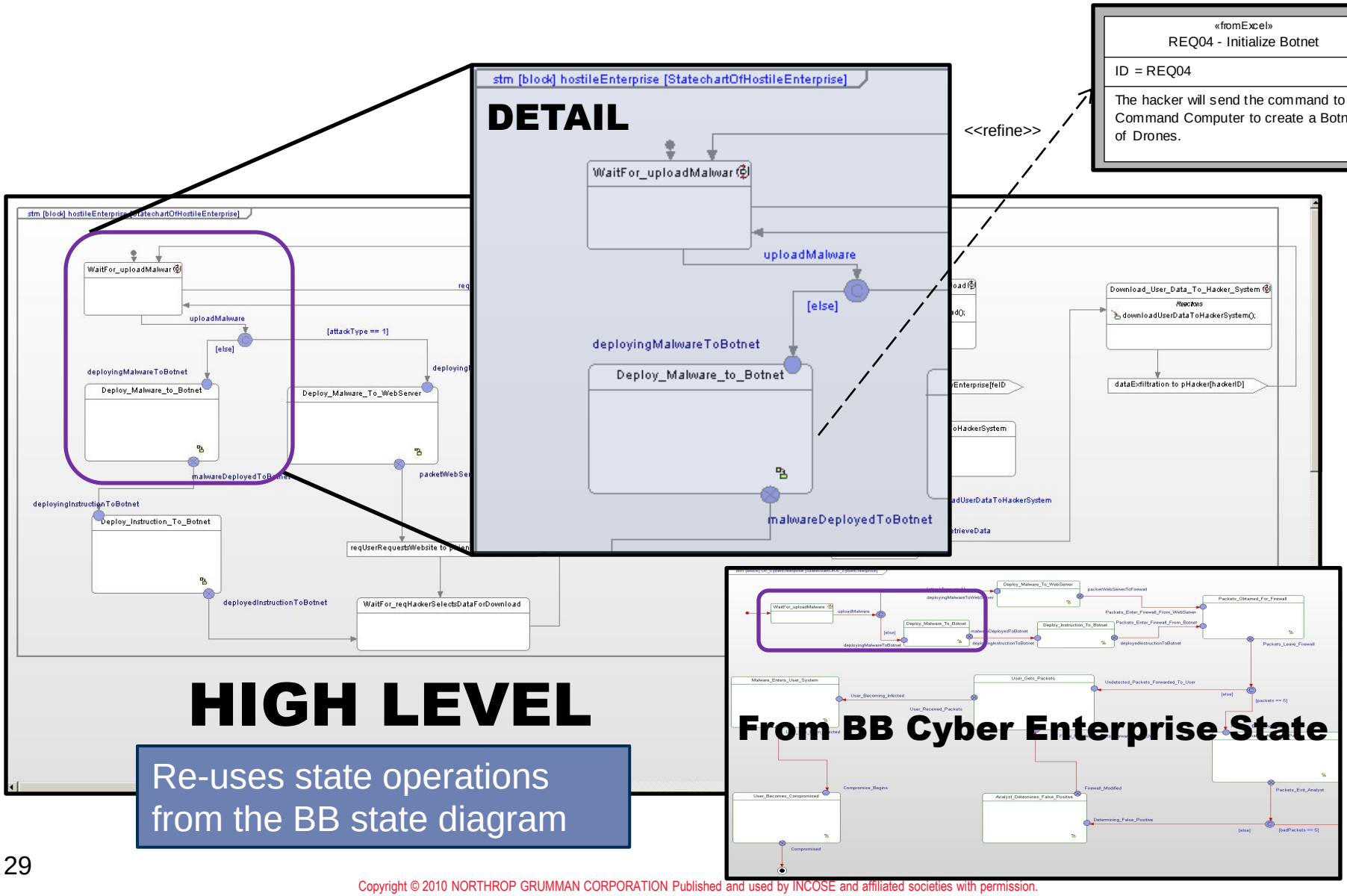
WB Block Definition



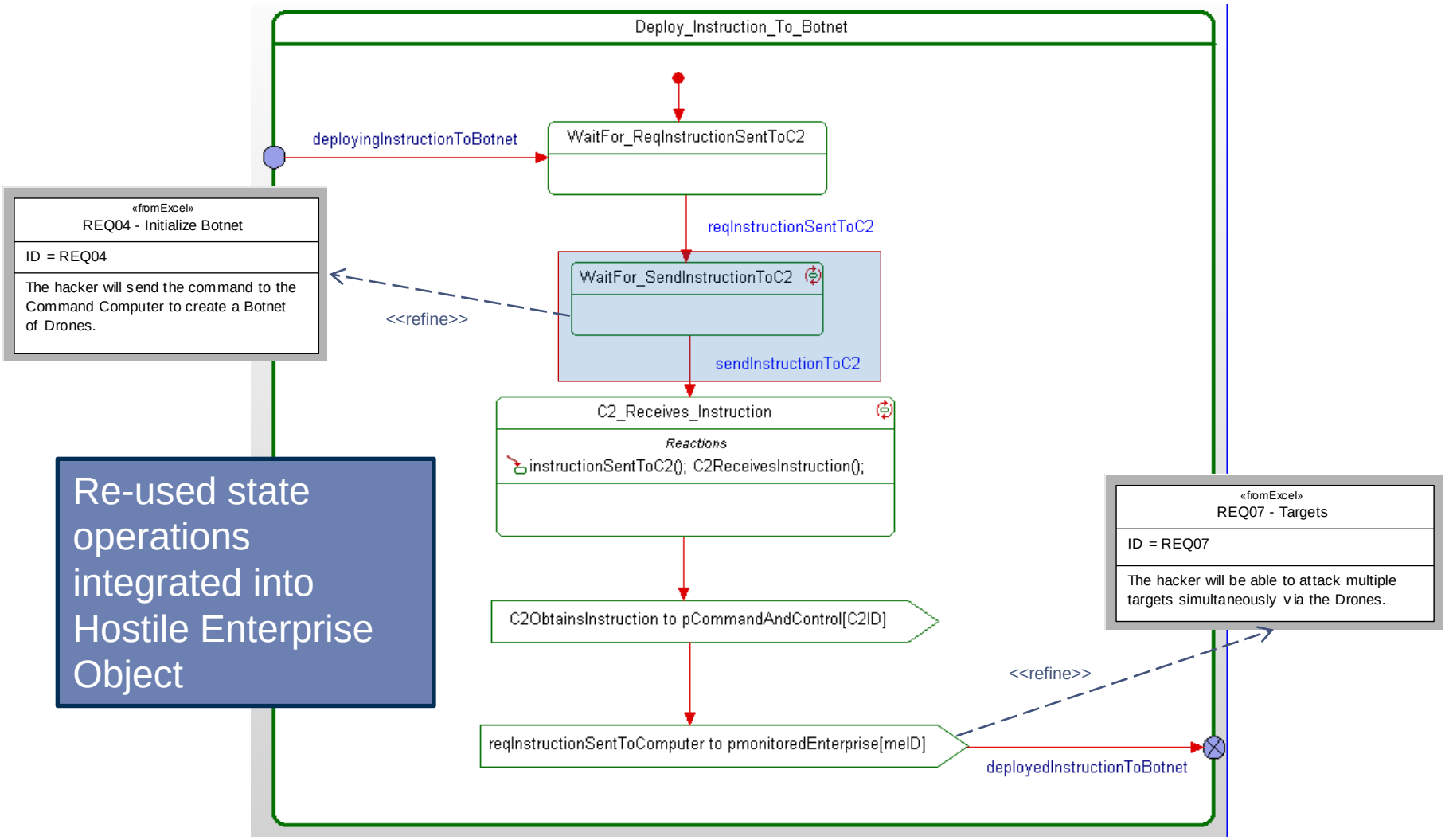


System Objects are Logical but can be allocated to Physical devices

WB State - Allocated

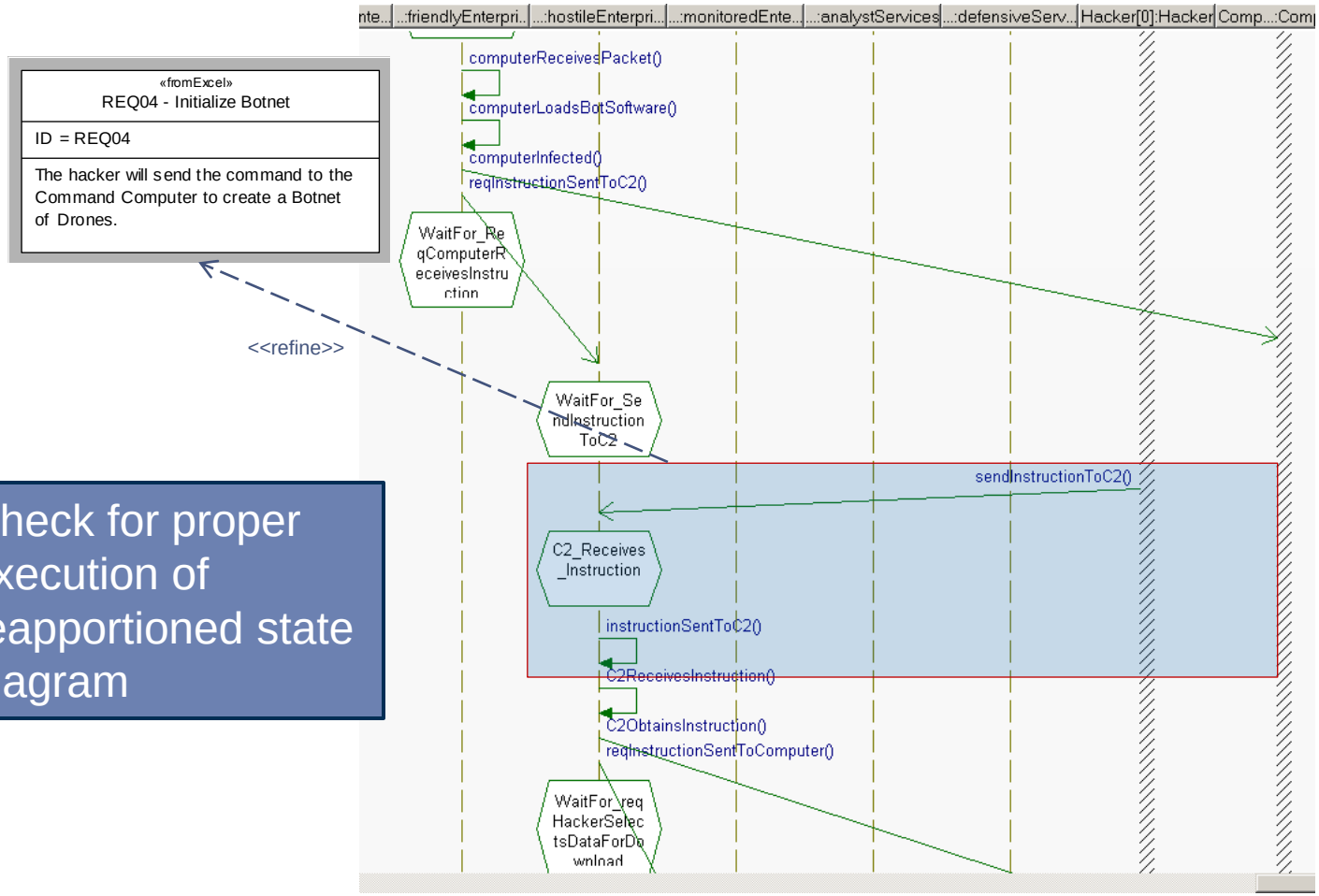


WB Sub-State - Allocated



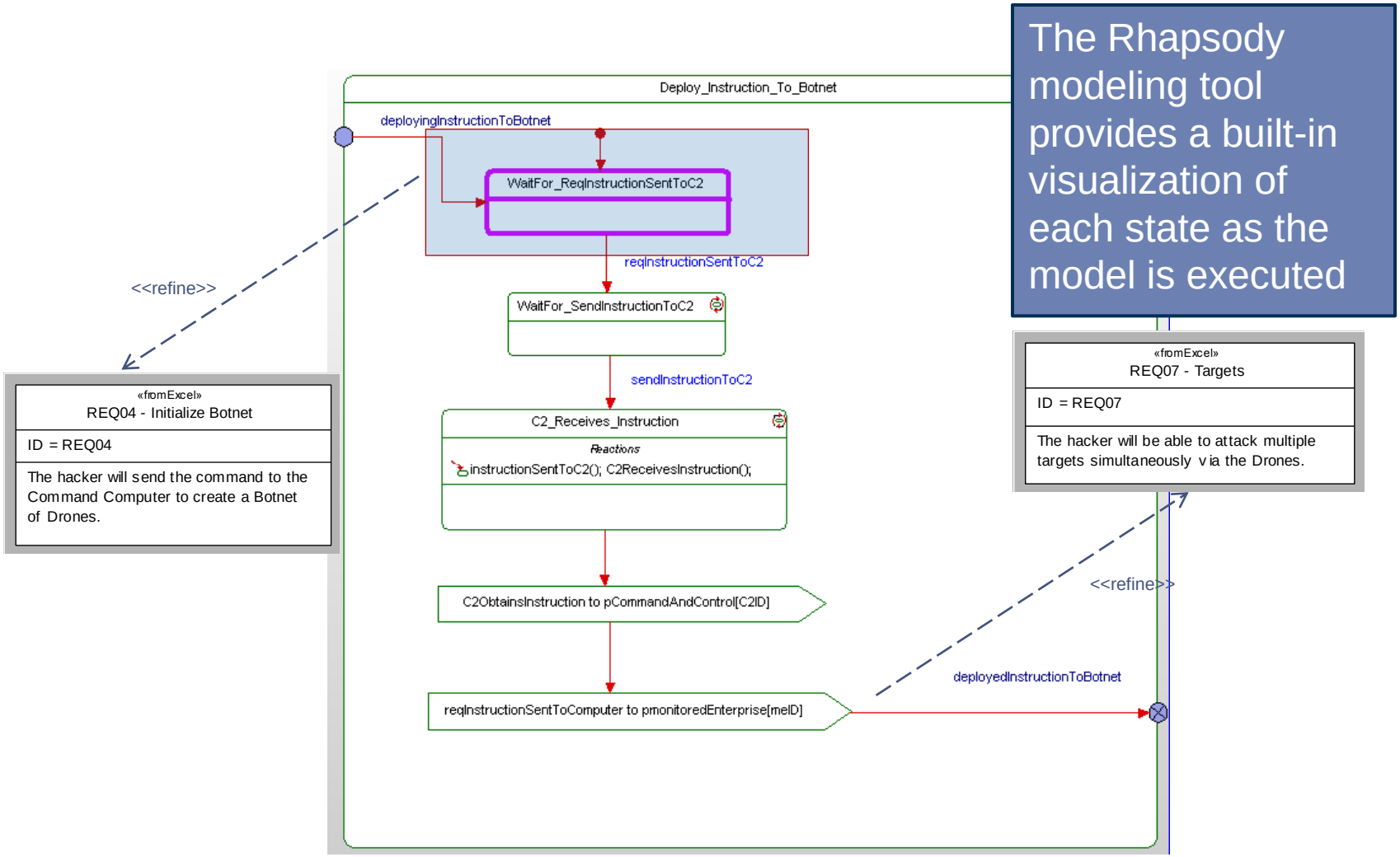
Re-used state operations integrated into Hostile Enterprise Object

WB Sequence - Executable

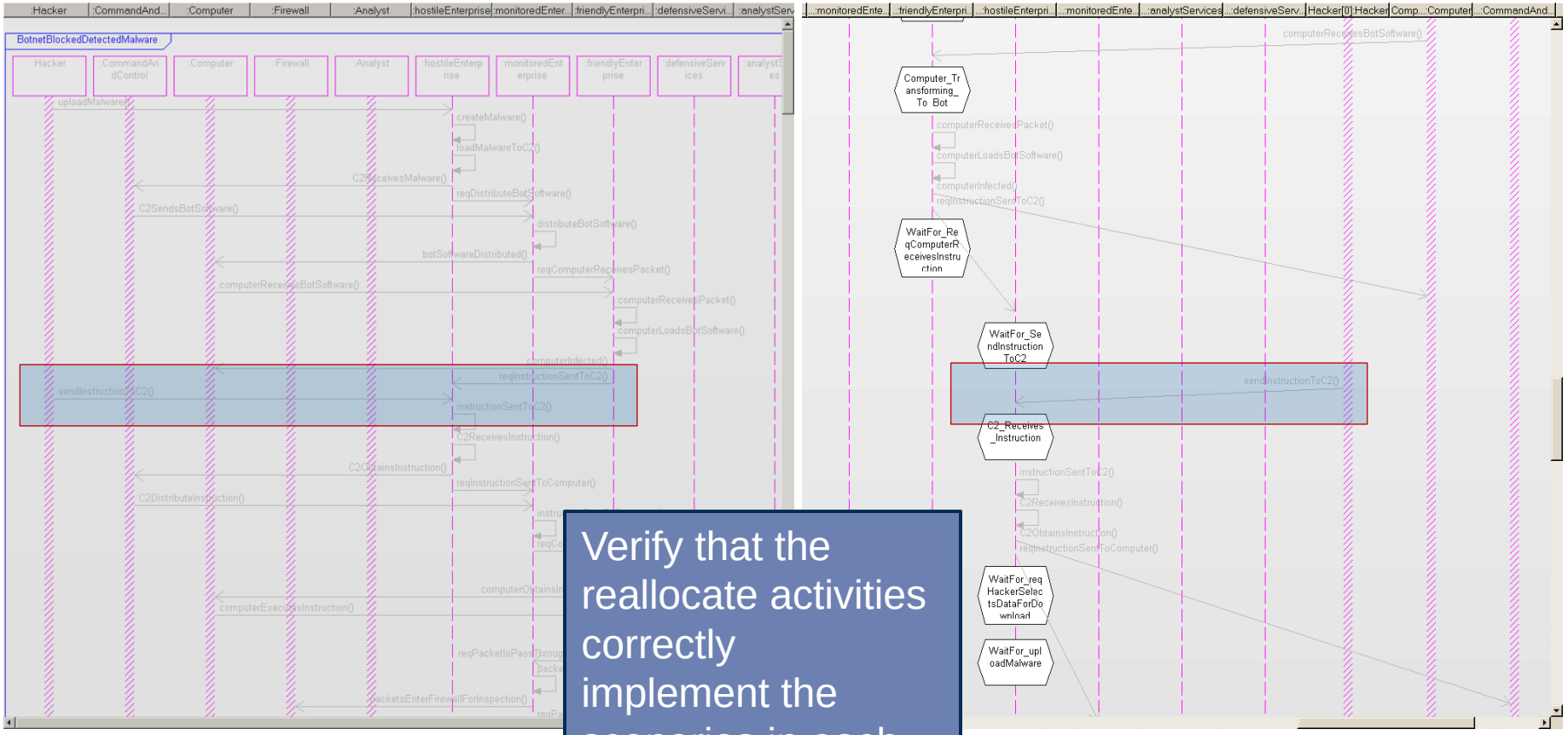


Check for proper execution of reapportioned state diagram

WB State – Executable - Visual



WB Sequence – Verified vs. Executable



Verify that the reallocate activities correctly implement the scenarios in each object

Visualization

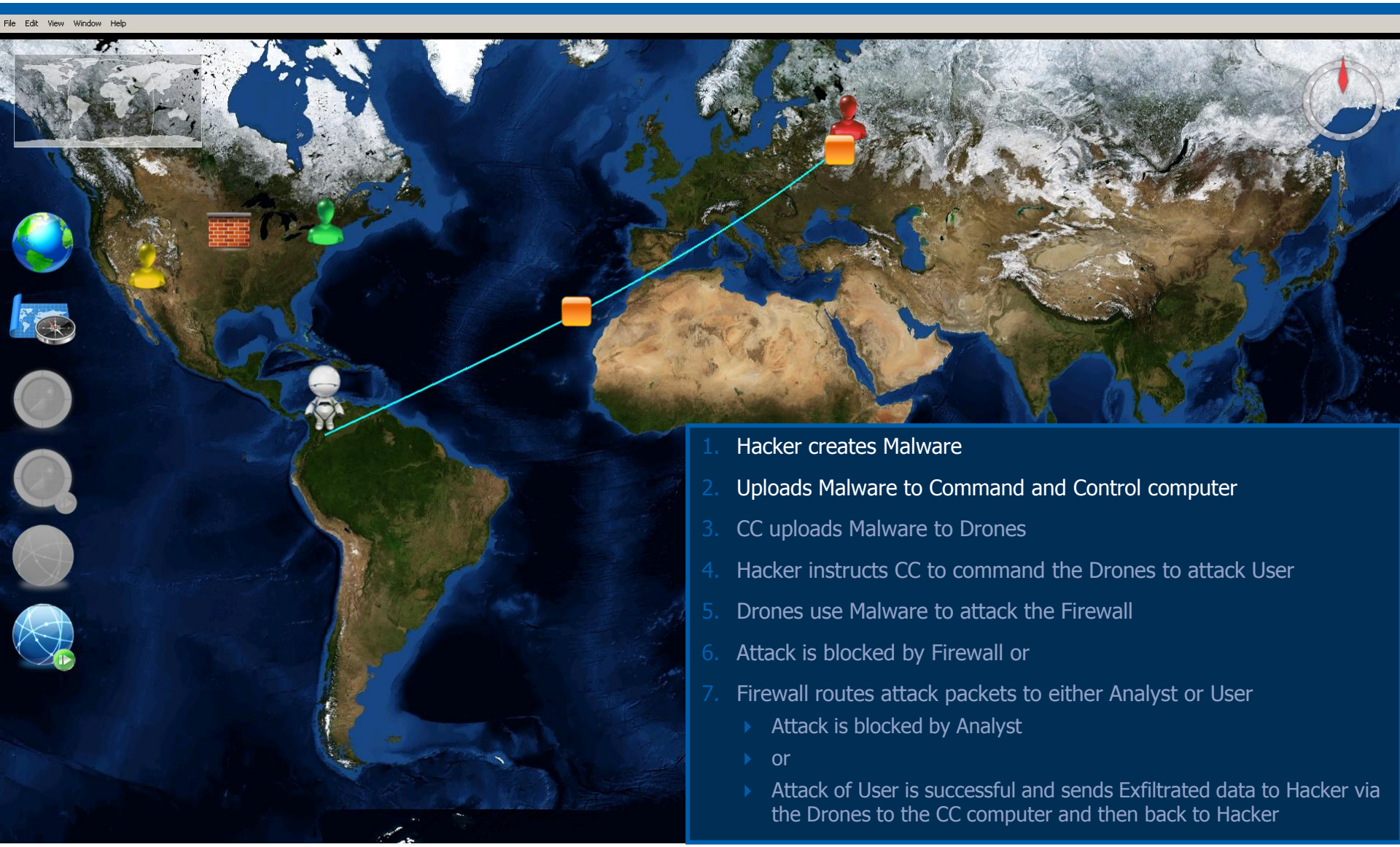
NORTHROP GRUMMAN

- Purpose
  - Verification of Requirements
    - Models provides a mechanism to verify that Requirements are implemented in the design
  - Validation of Design
    - The model visualization allows the Stakeholder to Validate that the systems performs that capabilities that were intended
- Demonstration
  - Visualization of Executable Demo on World Map
    - A high level animation is shown on the world map to present visually how attacks are directed and detected

NORTHROP GRUMMAN

Demo

Hacker Uploading Malware to Command and Control



1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Command and Control Uploads Malware to Drones

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Drones Use Malware to Attack Firewall

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Firewall Blocks Packet

NORTHROP GRUMMAN

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Firewall Routes Attack Packets to Analyst

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Analyst Blocks Packet

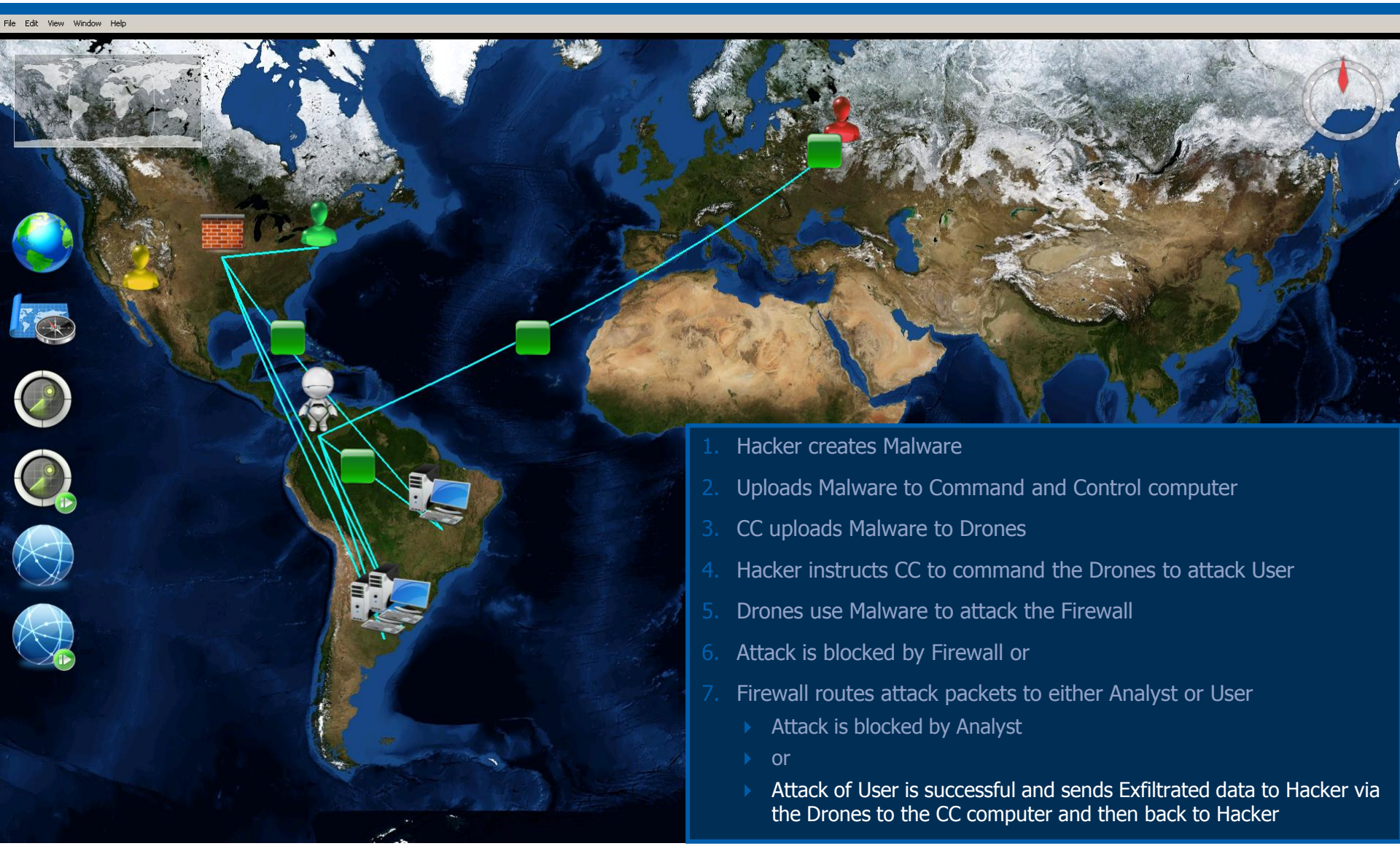
1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Firewall Routes Attack Packets to User

NORTHROP GRUMMAN

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Successful Data Exfiltration to Hacker



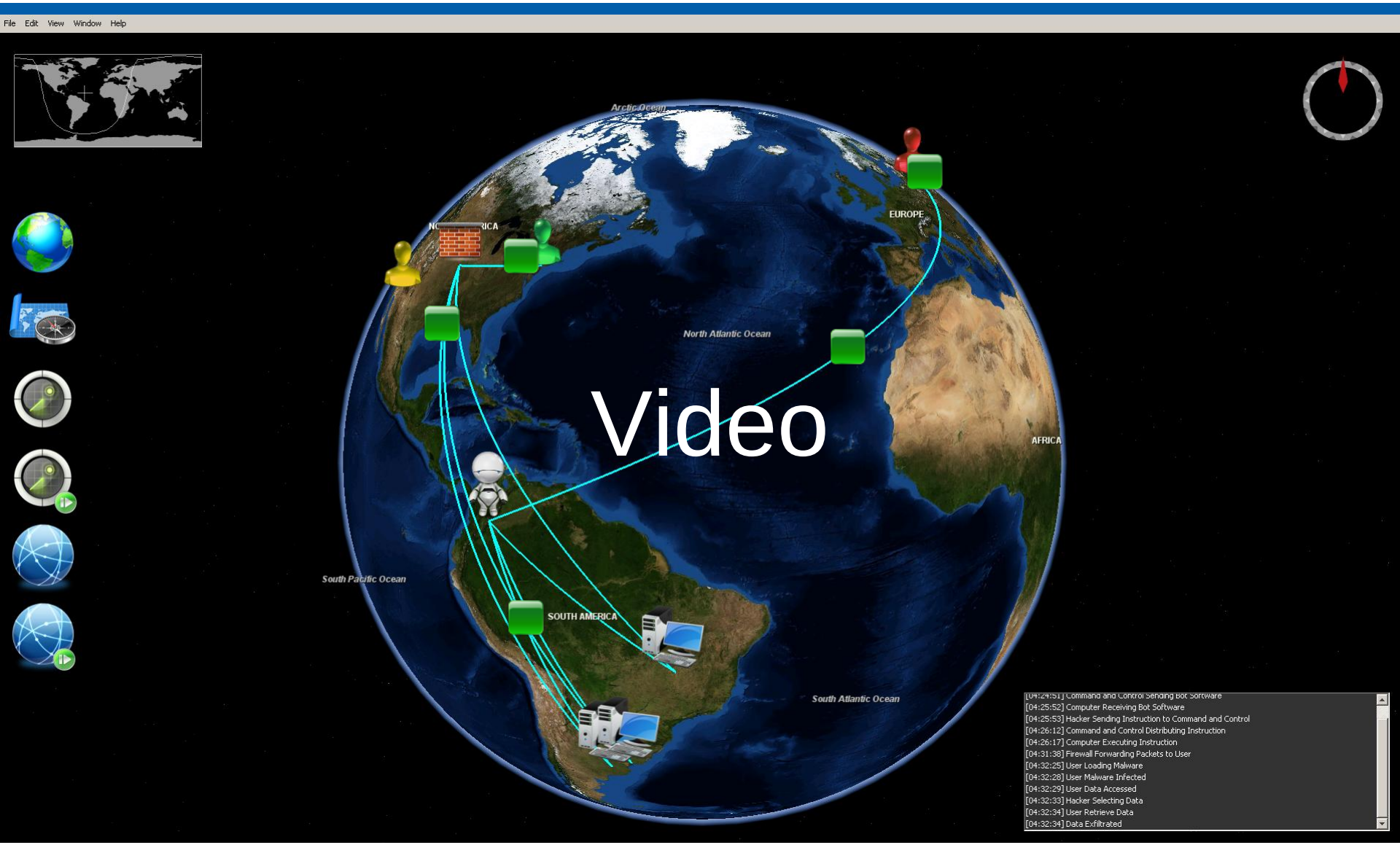
1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Conclusions

NORTHROP GRUMMAN

- The Model Based System Engineering capability:
  - Reduce design and specification errors that have to be corrected at greater cost during the system development
  - Reduced manually induced design errors since the tool has the capability to automatically create diagrams from data entered into the previous diagram
  - Provides for modeling of the requirements in the architecture of the system for an integrated view of the system
  - The simulation of the architecture and its visualization provided a more accurate view for the Stakeholders to determine that the design meets the needs their needs

Data Exfiltration Using a Botnet Model Simulation



NORTHROP GRUMMAN

Questions

Gundars Osvalds
Senior Principal Enterprise Architect
Northrop Grumman
gundars.osvalds@ngc.com


NORTHROP GRUMMAN