Cyber Model-Based Engineering (MBE)

Ambrose Kam
Lockheed Martin Rotary Mission Systems (RMS)
Moorestown, NJ 08057
ambrose.kam@lmco.com

Michael Nance
Lockheed Martin Rotary Mission Systems (RMS)
Collegeville, PA
michael.h.nance@lmco.com

Carl Hein
XSIM LLC
Cherry Hill, NJ
chein@cxsim.com

Charles Johnson-Bey
Lockheed Martin Rotary Mission Systems (RMS)
Hanover, MD
charles.johnson-bey@lmco.com

Michael Stebnisky
XSIM LLC
Cherry Hill, NJ
mstebnis@cxsim.com

Matt Curreri
Lockheed Martin Rotary Mission Systems (RMS)
Moorestown, NJ
matthew.r.curreri@lmco.com

ABSTRACT

As systems continue to evolve due to complex mission needs, the inherent vulnerabilities are growing exponentially. This drives the need to identify and detect system vulnerabilities early on. Modeling & simulation have become a staple in the systems engineering process; and model-based engineering (MBE) has become a focal point within system architecture. Hence, it is critical to consider combining the two related activities in the context of cyber-security beginning from the design phase and throughout the lifecycle of the program. For many Department of Defense (DoD) programs, System Modeling Language (SysML) is used to generate system architecture artifacts. We believe cyber aspects need to be considered early in the systems engineering process, so security features are "baked in" starting from the requirements definition, rather than "bolted on" later in the deployment phase due to cost constraints at the beginning of the program. Our Lockheed Martin team has demonstrated that successful use of cyber MBE efforts can be a cost avoidance opportunity. Our approach ties traditional MBE methodology to cyber operations analysis. Through automation and machine learning, optimum cyber solutions are identified and integrated to the rest of the system appropriately to ensure all performance requirements are met. Ultimately, this will enhance the overall cyber system resiliency

ABOUT THE AUTHORS

Ambrose Kam is a Fellow in cyber in Lockheed Martin; with over 25 years experience in the Department of Defense (DoD) industry, he is currently leading teams of engineers and contractors to support cyber threat analysis and resiliency assessment through modeling and simulation. He regularly gives cyber lectures at public forums and conferences including, MIT, Georgia Tech and Military Operations Research Society (MORS). Ambrose received his Asian American Engineer of the Year (AAEOY) award in 2017 for his technical contributions, leadership and community services.

Charles Johnson-Bey is the Director of Cyber Innovations in Lockheed Martin Rotary & Mission Systems. He is the recipient of the 2018 Black Engineer of the Year Award (BEYA). He has spent his entire career solving complex engineering and technology problems. He's been a professor and a researcher, earned a doctorate in electrical engineering, worked at Motorola research labs and Corning's Research and Development Center, and is in a 15-year tenure at Lockheed Martin.

Michael Nance is a Senior Fellow for Lockheed Martin. He oversees engineering teams in the classified design, implementation, and testing of trusted ground, airborne, and space-based systems. He has over three decades of experience in senior leadership roles, including as a CISO, focused in Cyber and RF based secure information technologies, and is an expert in computer network infrastructure and cyber space operations. Dr. Nance is a Certified Information System Security Professional (CISSP) and an Information Systems Security Management and Architecture Professional (ISSMP / ISSAP). He received his Doctorate of Science (DSc) in Information Assurance from Capitol Technical University (Capitol College). He is active in STEM and in the information technology community, including with the InfraGard organization and various related councils. Additionally, he is a Board member of several organizations and universities, including serving as an Adjunct Professor on weekends at the University of Maryland University College. You can find him on various social media and broadcast networks and systems as a public speaker for Lockheed Martin especially within the Wounded Warrior community

Carl Hein is Chief Technology Officer at XSIM LLC, where he focuses on architecture and network modeling to facilitate analysis and distributed development. He has over 30 years of experience in modeling complex systems at multiple abstraction levels. He conducts research in the area of intelligent agent methods and simulation models.

Matt Curreri is a Lead System Engineer at Lockheed Martin with 30 years’ experience in engineering System & Software Engineer in both the commercial and Department of Defense (DoD) industry. He has lead teams of engineers in developing software for automation and system modeling designs. His current research efforts are in SysML modeling driving other technologies, including Cyber Analysis and Simulation and Automation Technologies. He published articles technical journals and several individual patents

Michael Stebnisky is Lead Developer at XSIM LLC, where he develops Systems Engineering related performance modeling and verification and validation simulations for Model Based System Engineering (MBSE) on DoD systems, including the Navy's AEGIS system. He develops simulation-based methods for multidimensional performance modeling, and methods for automating the modeling process.

Cyber Model-Based Engineering (MBE)

Ambrose Kam
Lockheed Martin Rotary Mission Systems (RMS)
Moorestown, NJ 08057
ambrose.kam@lmco.com

Michael Nance
Lockheed Martin Rotary Mission Systems (RMS)
Collegeville, PA
michael.h.nance@lmco.com

Carl Hein
XSIM LLC
Cherry Hill, NJ
chein@cxsim.com

Charles Johnson-Bey
Lockheed Martin Rotary Mission Systems (RMS)
Hanover, MD
charles.johnson-bey@lmco.com

Michael Stebnisky
XSIM LLC
Cherry Hill, NJ
mstebnis@cxsim.com

Matt Curreri
Lockheed Martin Rotary Mission Systems (RMS)
Moorestown, NJ
matthew.r.curreri@lmco.com

INTRODUCTION

Modeling and simulation (M&S) have long been considered a critical element within systems engineering. Up until recently, M&S has not been applied to the cyber security domain area. One concern is the maturity of the cyber security modeling tools to aide in the analyses of this multi-faceted problem. M&S techniques have been applied to the sensor, weapons, command & control and logistics & sustainment within Department of Defense industry; but these areas are typically not as dynamic, nor as complex as cyber where threats evolve in seconds or minutes, as opposed to years or decades. Additionally, as modern warfare is getting more and more network centric, cyber is becoming more critical to mission impacts. This paper discusses a new modeling & simulation framework that cyber security subject matter experts can leverage to better understand the impacts of cyber.

Model Based Engineering (MBE) methods can predict impacts of cyber security effects by describing a distributed dynamic system where its applications and/or functions, tasks, processes are drawn as interconnected elements. Each of these elements is represented as blocks within the SysML. This paper discusses a novel SysML modeling approach to apply Petri net methodology to a system architecture, where the interconnection between the blocks represents data needed by and/or produced by the blocks. The blocks can eventually be mapped to “places’ in a system or network with the MBE methodologies of SysML. Extracting XML from the SysML artifacts enables suitable network/cyber simulation tools to simulate messaging traffic required to run the system as well as to predict system impacts if specific message traffic is disrupted by embedded cyber events. This approach consistent with usage of the Department of Defense architecture framework (DoDAF) for system architectural analysis and capacity planning over the past couple of decades.

When developing a SysML model, one needs to assess the goal of the system model. What information must be provided to stakeholders. In some cases, SysML is used as a scratch pad or skeleton for discovering various aspects of a system without concerns of any deliverables. Often a system model is driven by specific goals to produce artifacts, such as internal and external customer design documents. Common outputs of SysML models are documents containing diagrams and supporting specifications. During the development of a SysML model, the model structure can vary greatly depending on the authors. However, it is recommended to consider at the outset the desired outputs, when developing the model structure within a consistent understood framework. Development decisions should be collected into a framework guideline document. We developed a framework guideline for SysML to support Cyber-security as well as other types of system concerns, called the *Jelly Framework*. In our case, this framework separates SysML artifacts into 3 groups of SysML artifacts:

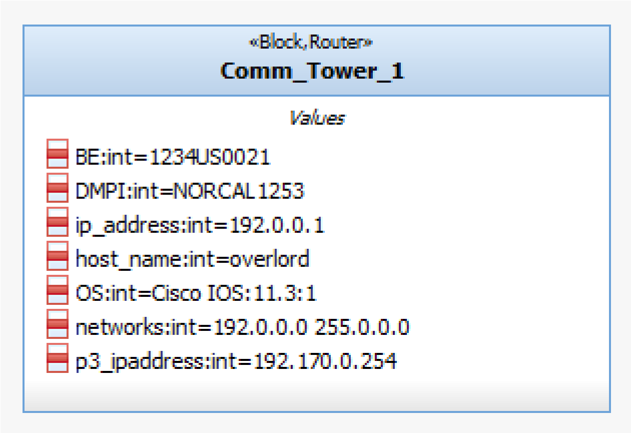
- Structural
- Behavior
- Requirements

The Structural group contains all components needed to describe the Cyber Environment. Two main diagrams are used for describing the cyber system modeling environment are: Block Definition Diagrams (BDD) and Internal Block Diagrams (IBD). The BDDs are used to define the system "Block" characteristics, its behaviors as well as the relationship between various blocks. The IBDs, on other hand, define how these Blocks are used in the specific context. Additionally, the IBDs also depict the system configurations.

To create a System Model for a Cyber Environment, the following steps were used. First, we have to define SysML Blocks. To do so, we use the Structural group of SysML (which includes BDDs and IBDs), and populate the Blocks with Nodes. A Node, in our cyber context, represents a piece of computer hardware. For example, a node could be some type of computer platform. In the cyber battle space, the types of platforms that we discuss in this paper are:

- **Sensors**: Radar Systems, Radar Antennas, etc.
- **Launchers**: Stationary Missile Launching platforms, Mobile Missile Launchers
- **Communications**: Routers, Hubs, etc.
- **Infrastructure Systems**: Power Stations, Sub Power Stations, etc.
- **Air Vehicles**: Fighter Jet, UAV, Drones, etc.
- **Surface Vessels**: Destroyer, Submarines, Commercial Freighters, Fishing Boats, etc.

Each of these platforms could be thought as computers with networking capabilities that could be vulnerable to cyber-attacks. To define these platforms in a SysML modeling tool, one would create these build blocks in the BDD. For this paper, we used the IBM Rhapsody tool for SysML modeling. For example, a Communication Tower node in a BDD system library as shown in Figure 1. For this example, one could name the Communication Tower, "Comm_Tower_1," and assigned network attributes associated with initial values to its block type definition (see Figure below). Please note that all examples are for illustration purposes. They do not represent any past, current or emerging systems.



«Block,Router»

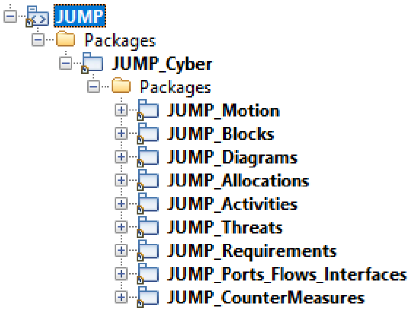
Comm_Tower_1

Values

BE:int=1234US0021
DMPI:int=NORCAL1253
ip_address:int=192.0.0.1
host_name:int=overlord
OS:int=Cisco IOS:11.3:1
networks:int=192.0.0.0 255.0.0.0
p3_ipaddress:int=192.170.0.254

Fig. 1. Defining SysML Blocks with Attributes and new Cyber Stereotypes

Notice at the top of the "Comm_Tower_1", there are word surrounded by "<<Block, Router>>". This is where the Stereotypes for a SysML element reside. Sims provides a set of SysML Stereotypes, which Block is one of them. We also can extend the SysML language by defining our own Stereotypes that provide additional clarification the propose of a SysML element. For this element, we have added an additional Stereotype "Router" which is housed in a SysML Profile call JUMP (Jelly Unified Modeling Profile). A SysML Profile is sort of library structure which can be imported into other models so to allow for sharing of these Cyber modeling Stereotypes (see Figure below).



- JUMP
  - Packages
    - JUMP_Cyber
      - Packages
        - JUMP_Motion
        - JUMP_Blocks
        - JUMP_Diagrams
        - JUMP_Allocations
        - JUMP_Activities
        - JUMP_Threats
        - JUMP_Requirements
        - JUMP_Ports_Flows_Interfaces
        - JUMP_CounterMeasures

Fig. 2. Jelly Unified Modeling Profile (JUMP) Profile Structure that contains the new Cyber Stereotypes and Types

Since SysML is object oriented with inheritance capability, the Comm_Tower_1 inherits the content of the VNSRouter. We can now apply the rest of the SysML Blocks to be used in our Cyber example to these established the inheritance relationship (shown with red lines) across the Type dependencies to formulate our Library of Network Nodes, as shown below:

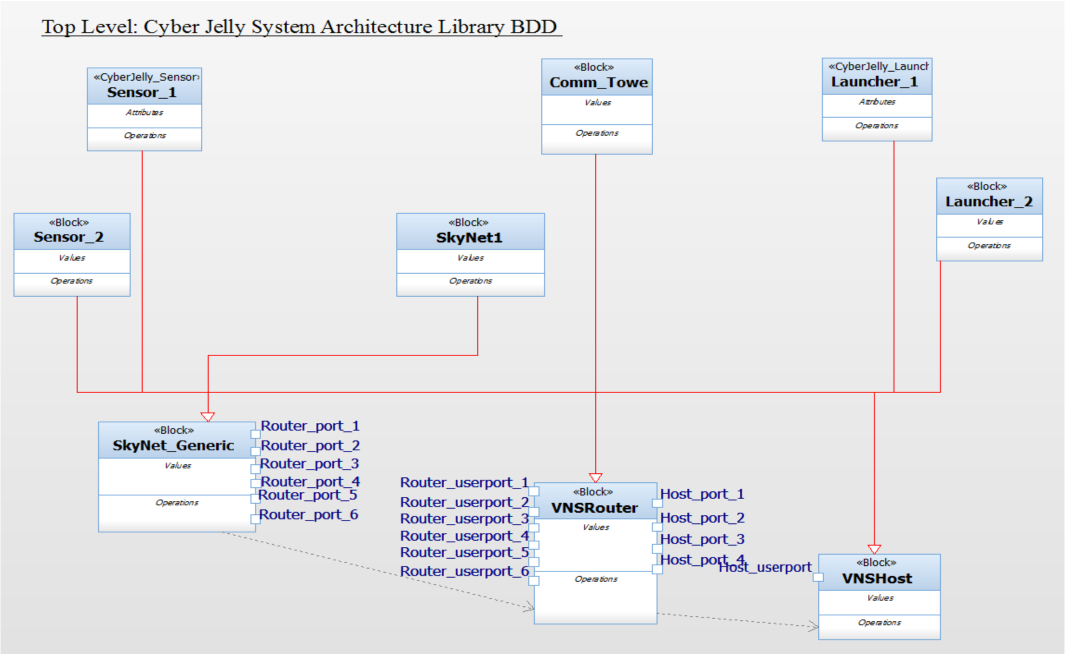


Fig. 3. Applying Types to SysML Blocks with Inheritance Relationship

Once you have established a Library of Nodes and their relationships among one another using the SysML BDD, one would then place some or all the SysML Block onto an IBD (Internal Block Diagram). The IBD is depiction of an instance of a Block in content or otherwise thought of as a configuration or an event of a System. When a SysML Block is applied to an IBD, the block is a considered at a Part of the usage. To obtain the Part from a SysML Block, with the Rhapsody SysML tool, you select the direct composition association.

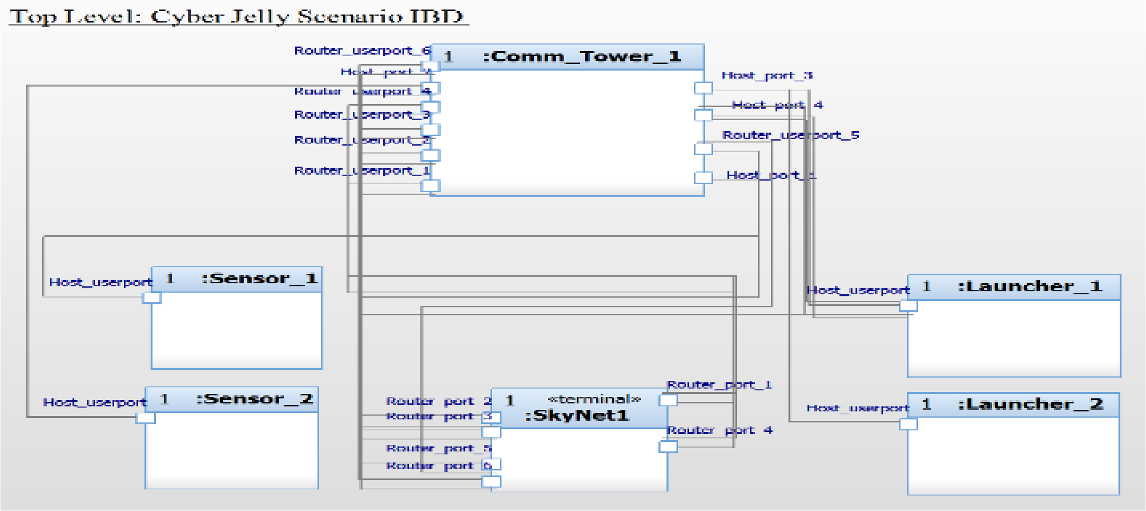


Fig. 4. A SysML Block in Context: IBD digram for a given Cyber Scenario example

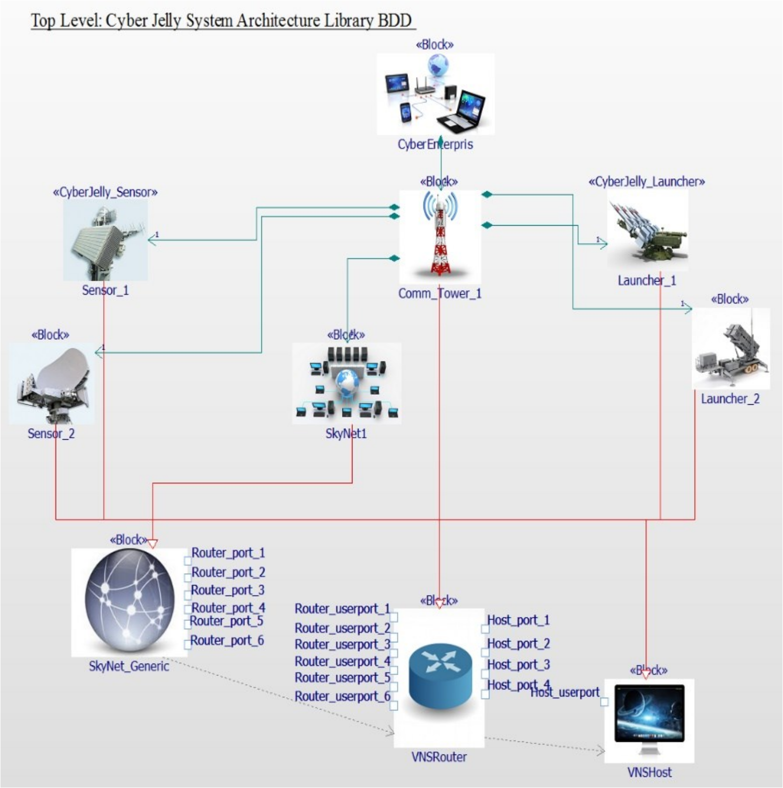


Fig. 5. BDD Cyber Network Node Library

Applying a touch of style to the IBD makes it more presentable and improves understanding for non-SysML users. In our example, images were applied as background, and parts and elements were added to construct a picture of a Cyber scenario, as shown in Figure 6. With this, we could tell a better story and explain the concept of operations (CONOPS) to the stakeholders. Essentially, a figure like Fig 6 could become our operational view, OV-1 within the DoDAF framework.

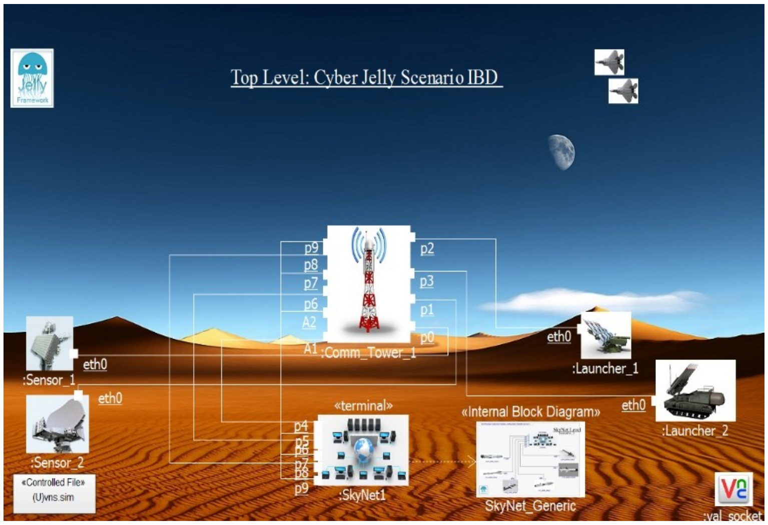


Fig. 6. A Touch of Style: Top-Level Cyber Scenario IBD

In addition to this CONOPS artifact, we are also representing the Cyber Architecture in a Logical representation with interactivity of behavior and message traffic using the SysML proxy pattern where the ports on the SysML blocks are type as Proxy Ports. These proxy ports are defined using SysML Interface Blocks (IB_Comm_Tower_1) that describe what is being transmitted amongst the various system artifacts. The connector that bind the SysML Blocks together via the proxy ports (p_Comm_Tower_1 and p_Launcher_2) have the messages define in the flows which contain items (Request and Report) that flow between the SysML Blocks (as shown, below).

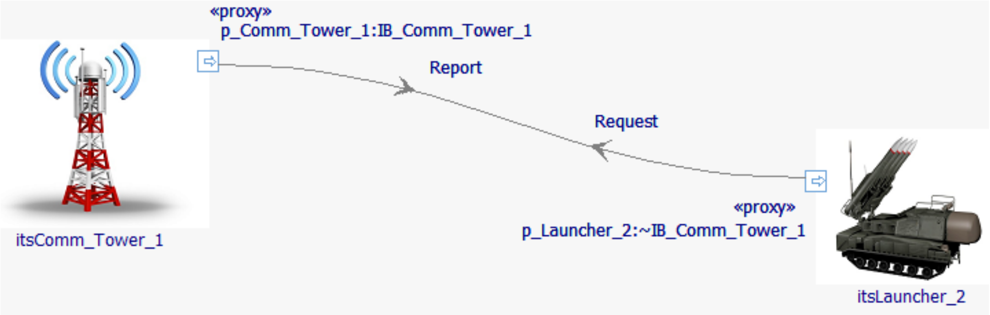
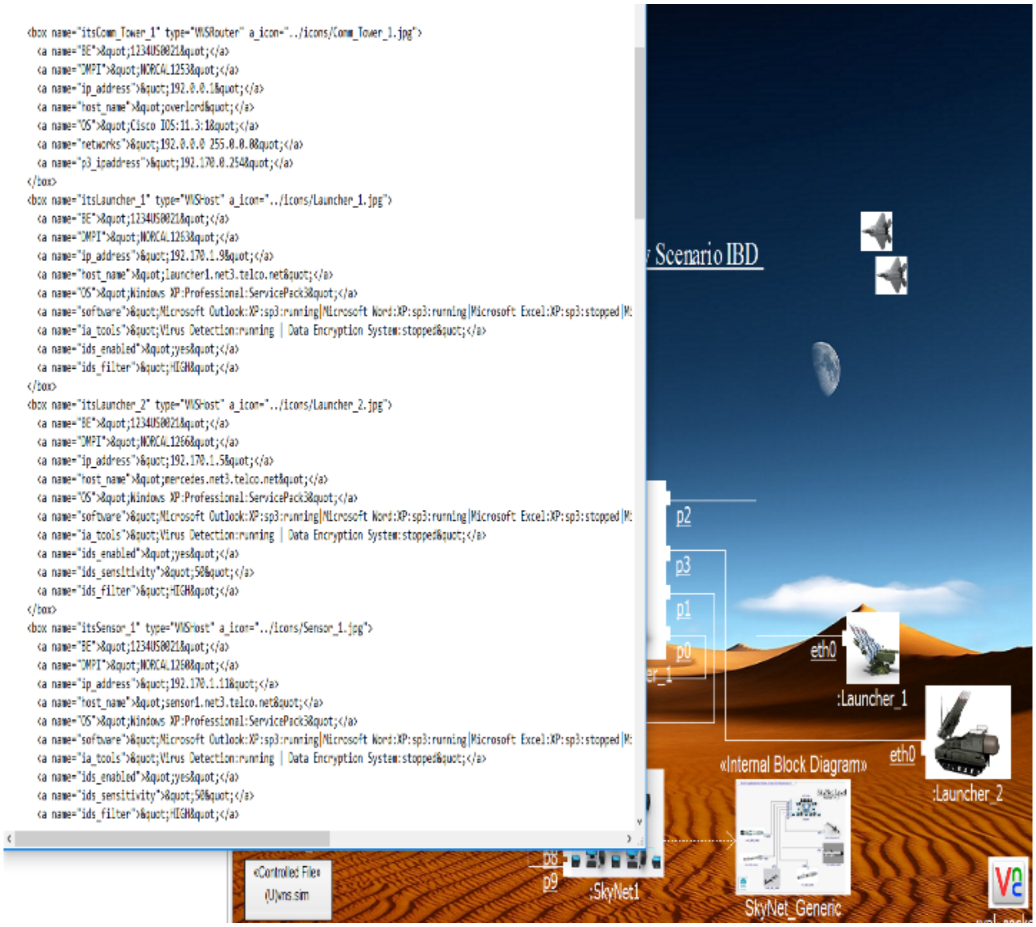


Fig. 7. Proxy Ports with connector that carries the flows of messages passed between SysML Blocks

Once the BDD is created with IBDs, the Rhapsody's Reporting Engine application called ReporterPLUS was deployed to read the IBD content using a customized ReporterPLUS script. The ReporterPLUS tool generates many different output formats and also can allow output customization. In our Cyber example, the input file format for the cyber simulation tool is XML. As a result, the team wrote script to ReporterPLUS to generate XML that the cyber simulation can understand. The sample XML output from the ReporterPLUS tool is shown in Figure 8 below. The convenience of this approach is that if you have another simulation tool that reads XML, you could easily bring in the metadata from a SysML environment and use them to drive a performance modeling tool.



```
<box name="itsComm_Tower_1" type="VNSRouter" a_icon="../icons/Comm_Tower_1.jpg">
  <a name="BE">&quot;1234US0021&quot;</a>
  <a name="DMPI">&quot;NORC4L1253&quot;</a>
  <a name="ip_address">&quot;192.0.0.1&quot;</a>
  <a name="host_name">&quot;overlord&quot;</a>
  <a name="OS">&quot;Cisco IOS:11.3:1&quot;</a>
  <a name="networks">&quot;192.0.0.0 255.0.0.0&quot;</a>
  <a name="p3_ipaddress">&quot;192.170.0.254&quot;</a>
</box>
<box name="itsLauncher_1" type="VNSHost" a_icon="../icons/Launcher_1.jpg">
  <a name="BE">&quot;1234US0021&quot;</a>
  <a name="DMPI">&quot;NORC4L1263&quot;</a>
  <a name="ip_address">&quot;192.170.1.9&quot;</a>
  <a name="host_name">&quot;launcher1.net3.telco.net&quot;</a>
  <a name="OS">&quot;Windows XP:Professional:ServicePack3&quot;</a>
  <a name="software">&quot;Microsoft Outlook:XP:sp3:running|Microsoft Word:XP:sp3:running|Microsoft Excel:XP:sp3:stopped|M:
  <a name="ia_tools">&quot;Virus Detection:running | Data Encryption System:stopped&quot;</a>
  <a name="ids_enabled">&quot;yes&quot;</a>
  <a name="ids_filter">&quot;HIGH&quot;</a>
</box>
<box name="itsLauncher_2" type="VNSHost" a_icon="../icons/Launcher_2.jpg">
  <a name="BE">&quot;1234US0021&quot;</a>
  <a name="DMPI">&quot;NORC4L1266&quot;</a>
  <a name="ip_address">&quot;192.170.1.5&quot;</a>
  <a name="host_name">&quot;mercedes.net3.telco.net&quot;</a>
  <a name="OS">&quot;Windows XP:Professional:ServicePack3&quot;</a>
  <a name="software">&quot;Microsoft Outlook:XP:sp3:running|Microsoft Word:XP:sp3:running|Microsoft Excel:XP:sp3:stopped|M:
  <a name="ia_tools">&quot;Virus Detection:running | Data Encryption System:stopped&quot;</a>
  <a name="ids_enabled">&quot;yes&quot;</a>
  <a name="ids_sensitivity">&quot;50&quot;</a>
  <a name="ids_filter">&quot;HIGH&quot;</a>
</box>
<box name="itsSensor_1" type="VNSHost" a_icon="../icons/Sensor_1.jpg">
  <a name="BE">&quot;1234US0021&quot;</a>
  <a name="DMPI">&quot;NORC4L1260&quot;</a>
  <a name="ip_address">&quot;192.170.1.11&quot;</a>
  <a name="host_name">&quot;sensor1.net3.telco.net&quot;</a>
  <a name="OS">&quot;Windows XP:Professional:ServicePack3&quot;</a>
  <a name="software">&quot;Microsoft Outlook:XP:sp3:running|Microsoft Word:XP:sp3:running|Microsoft Excel:XP:sp3:stopped|M:
  <a name="ia_tools">&quot;Virus Detection:running | Data Encryption System:stopped&quot;</a>
  <a name="ids_enabled">&quot;yes&quot;</a>
  <a name="ids_sensitivity">&quot;50&quot;</a>
  <a name="ids_filter">&quot;HIGH&quot;</a>
```

Fig. 8. Driving SysML into XML Based Simulation: XML file generated from SysML model

CYBER MODELING

Modeling and simulation (M&S) has been around for decades but applying it to cyber is a relatively new concept. Cyber simulation is becoming one of the relevant techniques for risk analysis or resiliency assessment. There are many cyber simulation tools available in the DoD or civilian industries. In our use case, we used Cyber Attack Network Simulation (CANS) simply because we have access to the source code, and is XML ready. CANS simulates the execution and effect of cyber incidents in a modeled network environment; the objective is to represent the behaviors of an intrusion and demonstrate the impacts on the mission system, hardware, and software applications. The adversary's effects on mission functionality is represented and tool provides an environment to determine remediation actions for the network defenders. As illustrated in Figure 9 below, attackers and the target network are modeled in a simulation framework from which performance metrics can be derived for cyber modeling, simulation and analysis (M&SA) studies.

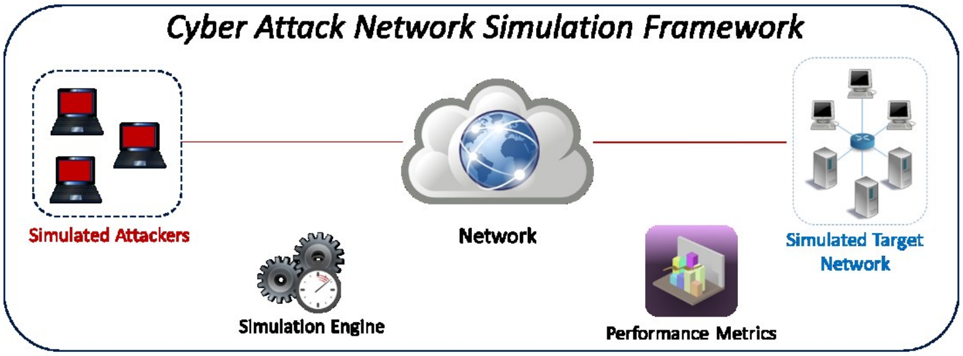


Fig. 9. CANS Software Architecture Overview

As evidenced in high profile hacking cases, cyber events "cascade" through a system - for example: a social engineering attack results in the installation of malware; the malware surreptitiously steals account credentials; the attacker uses the stolen credentials to impersonate a legitimate user then escalates privileges; the elevated privileges allow the attacker to install backdoor applications and command and control software, and so on. As the intruder(s) move through a network, capabilities are disabled, sensitive information is exfiltrated, and integrity of the system is compromised. A cyber simulation helps construct this "analysis of the possible" to ascertain impacts on a system or group of systems' ability to conduct mission operations.

A cyber simulation like CANS can be configured to support a number of cyber analysis use-cases, including – but not limited to – simulation analysis with or without an external combat simulator, cyber wargames, and cyber tabletop exercises. Systems engineers can conduct architectural risk assessments and identify gaps in security coverage that require controls or lockdowns. The cyber simulator can assist penetration testers and to train network/system administrators or other cyber defenders. Unlike "cyber range" methods for executing cyber exploits, software-based simulators of cyber attacks do not use any actual malware nor network reconnaissance or penetration tools and is therefore safe to use on any network or computer. As illustrated in Figure below, CANS is comprised of network models whose behavior is governed by a simulation engine, a datastore for sim configurations and cyber event types, and two user interface applications: a network visualizer and a Cyber Attack Launcher (CAL). The modeled network can be constructed from either an eXtensible Markup Language (XML) schema. Topology and network metadata from popular commercial off-the-shelf tools (COTS) like OPNET Modeler and Rhapsody or even network reconnaissance software like nmap can be imported to the cyber simulation environment via XML. To populate and validate the threat models, industry data such as metadata from the Common Attack Pattern Enumeration and Classification (CAPEC) database is used to generate cyber effects.

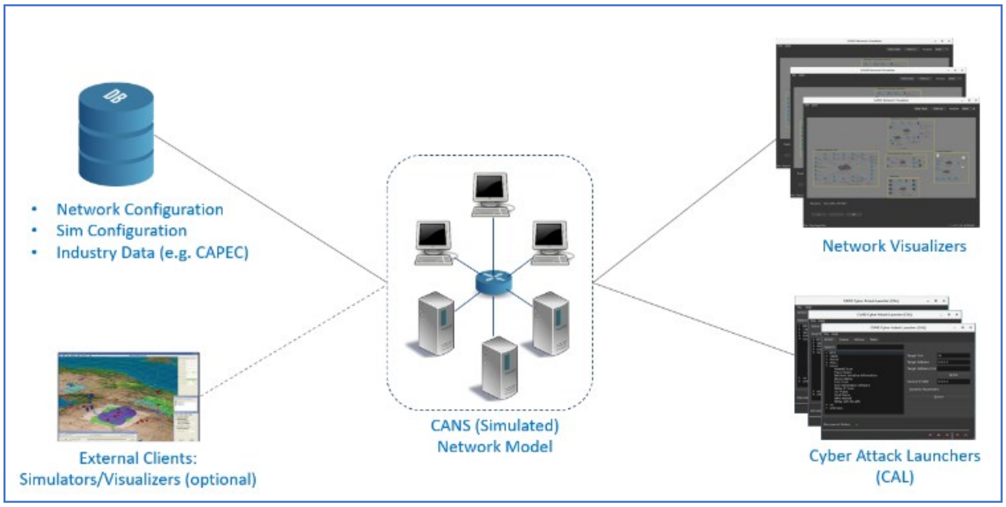

DB
• Network Configuration
• Sim Configuration
• Industry Data (e.g. CAPEC)
External Clients: Simulators/Visualizers (optional)
CANS (Simulated) Network Model
Network Visualizers
Cyber Attack Launchers (CAL)

Fig. 10. CANS Software Architecture & Component Decomposition

It is important to note, however, that a network model in the simulation environment can represent a number of potential configurations – e.g., a network of a single asset (for example, a satellite ground station) or a cluster of networks from multiple assets (ships, aircraft, etc.); figure 11 below illustrates how a cyber simulation network model can scale modularly.

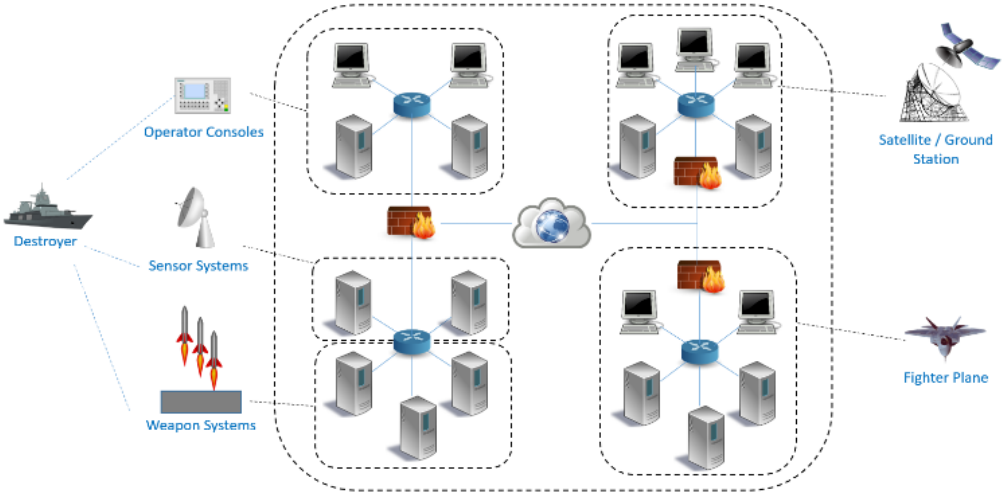


Fig. 11. Example of Network Models in the Cyber Simulation Environment

This modularity is exactly why the SysML MBE can be so useful. End user can easily add new elements or systems to a scenario. This can facilitate what-if analyses and analysis of alternatives (AoA) studies. Armed with these dynamic modeling capabilities, our cyber simulation environment can model a realistic operating scenario, and define both the attacks and the defensive measures. A visualizer can be used to depict the cyber effects on mission visually. Distributed Interactive Simulation (DIS) is an IEEE standard for different simulation tools to interoperate. Since our simulation environment is DIS-enabled, the output of a simulation run can be graphically displayed in a visualizer for playback or demonstration purposes. By leveraging this end-to-end environment, our cyber MBE framework can be used to analyze the security posture of existing or planned networks. Some of the metrics output include:

- # of intrusions (Successful, Undetected, Unobserved)
- # of information exploitations
- # impacts to various cyber precepts: e.g. CIA (Confidentiality, Integrity, Availability), AAA (Authentication, Authorization, Auditing)
- # of network nodes infected, compromised, controlled, crashed, etc.
- Node performance statistics (CPU, RAM, network usage, overload, etc.)
- Information on system operation, e.g.: % of system compromised, degraded, etc.
- Response* and recovery times*, dwell times* (interval between initial infection or intrusion to discovery and remediation)
- Metrics related to Cyber Resiliency[1]

The figure below shows a summary of an event sequence that starts with SysML architecture modeling and ends with analytical results and visual playback of cyber results in integrated cyber simulation environment. As noted in this paper earlier, once you have completed the SysML modeling (by defining a profile with IBD and BDD diagrams along with the topology information), you could perform the architectural trade studies necessary; this is to ensure the cyber is being considered early in the system design/development process. Once the architectural analyses are performed to meet the requirements, you can then generate and export the XML-based output files (ReporterPLUS for Rhapsody) to a cyber simulation tool; in our environment with CANS, appropriate attack vectors can be selected to determine their impacts on the infrastructure or system(s). The tool provides metrics for

[1] planned functionality

performance level analysis. At this point, you can choose a variety of defensive measures to explore their effectiveness relative to the chosen threats and attack vectors. Once the cyber risk analysis and cyber resiliency assessment are performed, you can choose to visualize this process, as shown below. Overall, this process of performing the cyber architectural modeling to simulation of Cyber Attacks is a rapid sequence of steps which can be automated (through Sikuli scripting) to produce an efficient cause-and-effect paradigm that allows the cyber analysts to experiment and experience multiple types of Cyber Attack scenarios.

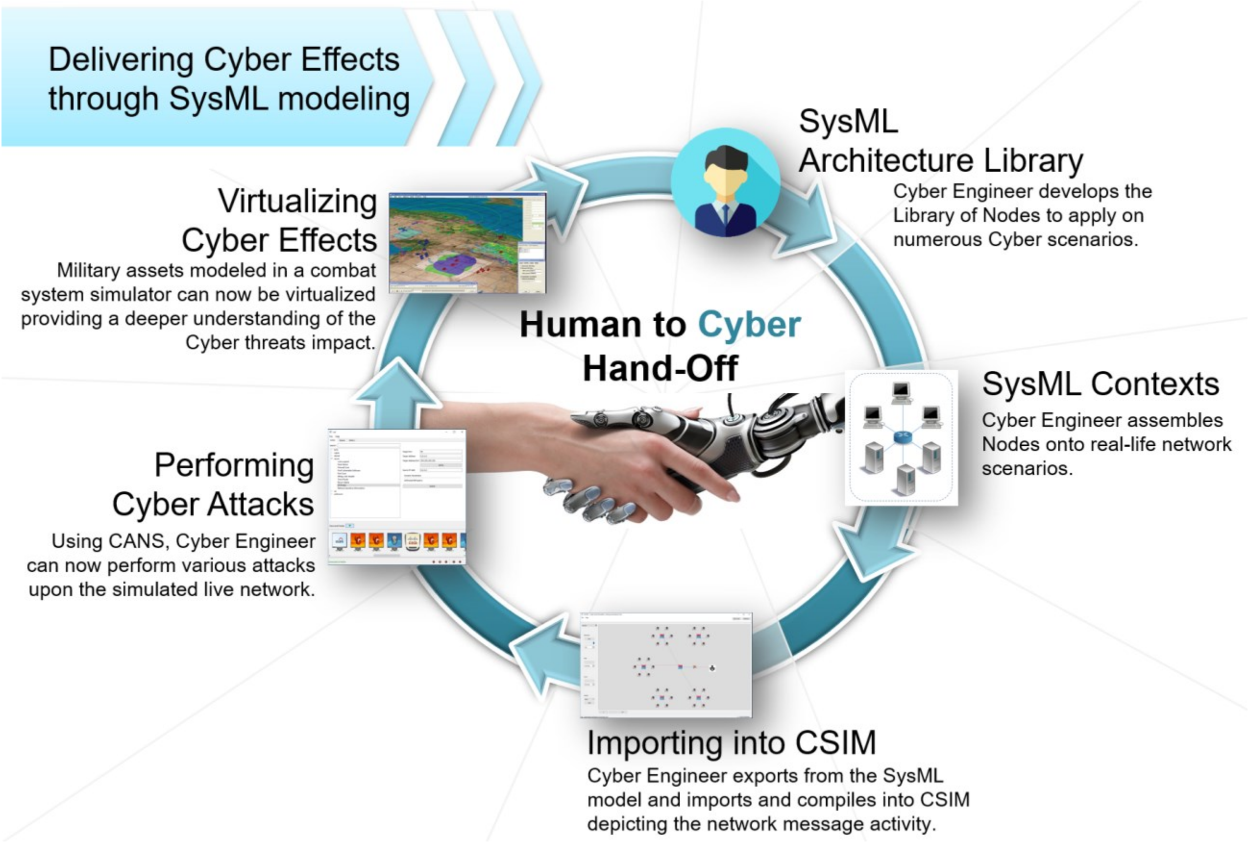

Delivering Cyber Effects through SysML modeling
SysML Architecture Library
Cyber Engineer develops the Library of Nodes to apply on numerous Cyber scenarios.
Virtualizing Cyber Effects
Military assets modeled in a combat system simulator can now be virtualized providing a deeper understanding of the Cyber threats impact.
Human to Cyber Hand-Off
SysML Contexts
Cyber Engineer assembles Nodes onto real-life network scenarios.
Performing Cyber Attacks
Using CANS, Cyber Engineer can now perform various attacks upon the simulated live network.
Importing into CSIM
Cyber Engineer exports from the SysML model and imports and compiles into CSIM depicting the network message activity.

Fig. 12. Human to Cyber Hand-Off: Summary of Architecutre Modeling / Cyber Simulation Sequence

FUTURE WORK

This paper covers current progress in modeling & simulation (M&S) to study/analyze existing and emerging cyber threats relative to a given system architecture. Significant advancements have been made to couple traditional SysML MBE techniques with a cyber simulation tool. This Cyber MBE marriage has proven to be useful in the DoD arena. Similar efforts can be applied to commercial systems as well so that cyber resiliency can be improved in the civilian world. For example, cyber resiliency should be analyzed before the DoD or civilian system is being planned and throughout development. At the system architecture and system definition phases, it is cost effective to model a system with SysML and explore different cyber defensive options relative to different operational scenarios. From the cost avoidance and cyber effectiveness standpoint, it is prudent to integrate cyber as part of the early system architecture development, rather than adopting a “bolted-on later” strategy. For future exploration, the team is looking at the applicability of Machine Learning (ML) and Deep Learning (DL) to this approach. The thought process is that the current what-if evaluation is very much an analyst-driven process. All the what-if analyses are being conducted based on existing and perceived threat scenarios. While this approach works, it is more of a trial-and error which may or may not provide the most optimal solution given the dynamic nature of cyber threats. To make this process more robust, automation techniques or autonomy need to be applied to the problem space. Machine Learning and Deep Learning have made significant impacts in medical, robotics and other fields; tools like TensorFlow and PyTorch are becoming better known as more users are discovering their use cases. Cyber MBE will benefit great from the technical advancement if features in the ML/DL can be improved through learning techniques such that optimum cyber mitigation solution(s) could be reached quickly.

SUMMARY

This paper provided a summary of an effort where SysML was successfully introduced into a cyber simulation environment. By doing so, it extended the utility of the cyber simulation so that it can be used to support architectural analysis studies that draw on cyber system solution performance. By fully embracing the MBE with SysML, the system development teams can easily add new parameters to the node and network models based on customer needs, and evaluate their impacts relative to cyber risk analysis and resiliency assessment. With this approach, network architecture and topology can be easily modified and updated without starting the modeling effort from scratch. Additionally, the simulation interface is now advanced to a point that it can be adapted to various visualization environments so that decision makers can have a heuristic view of cyber impacts (instead of making decisions based on intuition or assumptions without any solid foundation). The fact that cyber risks can be assessed early on in the design phase means that the cost-savings and cost-avoidance are significant. After all, system engineers understand that changes being made in the later phases incur a significant penalty in project costs and schedule. By managing complexity more effectively, this SysML approach also drives down technical and scheduling risks. All of these are critical in the cyberspace since threats are rapidly evolving, and attack vectors are increasing over time.

Our Cyber MBE effort has shown great promise, and the needs for cyber resilient systems have never been stronger—both in the DoD and civilian arenas. As cyber incidents are seemingly imminent as threats are outpacing defensive solutions, the key factor in enhancing system resiliency is mitigation responses and recovery. But, they can vary depending on countless factors, including the availability of network and system administrators and their respective skill levels, the time required to bring nodes and applications back up after a crash, and so forth. With so many events having indiscriminate outcomes, the need to construct statistical models coupled with architectural analysis to study the effects of cyber phenomena on systems becomes clear. And Cyber MBE can be an important part of the solution.

REFERENCES

[1] Barnum, S., *An Introduction to Attack Patterns as a Software Assurance Knowledge Resource,* OMG Software Assurance Workshop 2007

[2] Bodeau, D., Graubart, R.,*Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment* MITRE Technical Report MTR130432, Bedford, MA Nov 2013

[3] Committee on Technology for Future Naval Forces, *Becoming 21st Century Force, Modeling and Simulation,* Volume 9, U.S. Naval Studies Board National Research Council, 1997

[4] Department of Defense Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation* Secretary of the Navy Instruction (SECNAVINST) 5239.3B, *Department of the Navy (DoN) Information Assurance (IA) Policy*

[5] Jaquith,A, *Security Metrics: Replacing Fear*, Uncertainty, and Doubt. ISBN 9780321349989

[6] Powell, S.,*Cyber Effects Prediction, Black Hat Briefing, DC, 2010*

[7] Ostermiller, Voula, *TI12 Network Modeling Report for BL9.C2*, Lockheed Martin MST, Nov, 2014

[8] Security Technical Implementation Guide - Application Security and Development, Defense Information Systems Agency (DISA), 23 January 2014

[9] Sergio Herrero-Lopez, S., Williams, J., Sanchez, A., *Large-Scale Simulator for Global Data Infrastructure Optimization*, 2011 IEEE International Conference on Cluster Computing, MIT, 2011

[10] Simmons, C., et. al., *AVOIDIT: A Cyber Attack Taxonomy,* Dept. of Computer Science, University of Memphis, IEEE Mag, Apr, 2010

[11] Uma, M., Padmavathi, G., *A Survey on Various Cyber Attacks and Their Classification,* International Journal of Network Security, Vol.15, No.5, PP.390-396, Sept. 2013