Future Look – Effective Cybersecurity Using Modeling & Simulation

Paul Gustavson,
SimVentions
Fredericksburg , VA
PaulGustavson@SimVentions.com

Steve Reeder
SimVentions
Fredericksburg , VA
CharlesReeder@SimVentions.com

ABSTRACT

Cybersecurity Engineering operates within the new domain of Cyberspace, and is focused on the security aspects of systems to ensure the design, architecture, and development are robust enough to deal with diverse disruptions once deployed. Disruptions might include a malicious attack, a security breach, infrastructure degradation due to natural disaster, an insider threat, or a physical act of terrorism.

The opportunity exists to leverage Modeling and Simulation (M&S) in a novel way to represent and assess security vulnerabilities, and engineer and test security enhancements without compromising operational integrity. Namely, it provides an efficient and expedient means to facilitate Cybersecurity Engineering. It is a game changer.

This paper explores the benefit and approach to develop and use threat models and penetration (pen) test models upon representations of weapon systems (current or future). Virtual systems, simulations and stimulators representing these systems can be distributed via networks. Models and adjunct simulations reflecting cyber threats, malicious effects, and pen injections can be used in the context of this distributed environment to assess and validate system designs and architectures without compromising integrity.

M&S provides a means to evaluate potential threats before they're exposed and in the wild, and promotes security engineering early in the development process. It offers a means to bolster system integrity creating greater confidence of systems before they are deployed or updated.

This paper discusses the important elements of security engineering that can be supported using M&S, and offers four steps to begin to leverage M&S in a new and novel way.

ABOUT THE AUTHORS

Paul Gustavson, is a cofounder and CTO of SimVentions. Paul leads in identifying and contributing to the company's capability and influencing the strategic vision. His experienced includes simulation systems, software applications, Naval surface system components and tools, and DoD and international standards. Supports the DoD M&S Coordination Office (M&S CO) and is active within the Simulation Interoperability Standards Organization (SISO). Author of *Leaders Press On*, and contributing author of *Engineering Principles of Combat Modeling and Distributed Simulation* and *C++Builder 6 Developer's Guide*.

Steve Reeder, Cyber Defense Lead, Nuclear Aircraft Carriers, responsible to develop defense in depth solutions and certification and accreditations artifacts. His experience includes, operating system development, critical real time control systems, offensive and defensive Cyber capabilities, Test and Evaluation (T&E); Government agent for Verification, Validation, and Accreditation (VV&A) of M&S solutions.

Future Look – Effective Cybersecurity Using Modeling & Simulation

Paul Gustavson,
SimVentions
Fredericksburg , VA
PaulGustavson@SimVentions.com

Steve Reeder
SimVentions
Fredericksburg , VA
CharlesReeder@SimVentions.com

INTRODUCTION

The SimVentions customer base is predominately comprised of Military and Government Agencies, hence the discussion pertaining to Cybersecurity and Modeling and Simulation (M&S) clearly has a DoD tone. The paper addresses the domain of Cyberspace and how Cyber is inculcated into all the traditional domains. Threat agents are discussed briefly as well as today's evolving hacker communities. Traditional networks, Industrial Systems and Mobile Communications are introduced as well as some integration points among them. The effects of the integration among networks, industrial systems and mobile on Cybersecurity engineering tasks is that modeling and simulating must now be extended to address a much larger and more dynamic Cyber threat attack surface. This paper identifies eight key hypotheses to support "effective cybersecurity using modeling and simulation."

We also discuss how to apply M&S in a simple yet novel way to represent cyberwarfare so that we can test and train proactively. This includes leveraging the use of existing systems represented as either simulations or live system using a notional virtual hypervisor environment. As an example, we will identify several SimVentions offerings; Informedb (Enterprise Architectures support) and EMBR (Modeling and Simulation support) to show how the solution space can be represented.

CRITICAL COMPONENTS

This first section explores the six major components that need to be understood and considered in order to establish proactive cybersecurity M&S tool. As we examine these components, we will identify the key hypotheses that should be represented or supported.

The Cyberspace Domain

Cybersecurity engineering is a field of practice that brings together aspects of systems engineering, operational security, software engineering, and acquisition to aid in developing secure systems.

Cybersecurity engineering differs from other engineering disciplines in that it operates within "Cyberspace". For the military, Cyberspace is a new and global domain. It physically resides within the other domains of air, land, maritime, and space. Where Cyberspace differs from the other domains is that it is an environment created to exploit information, disrupt human interaction, affect intercommunication, or impair system performance.

This domain co-exists within the electromagnetic spectrum, telecommunications, systems of systems and networks of networks. Because Cyberspace is man-made, it is only through continued attention and maintenance that Cyberspace persists. Effective use of Cyberspace occurs through the unified efforts of integrating military forces and their actions to create a force that operates as a whole and synchronizes actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time.

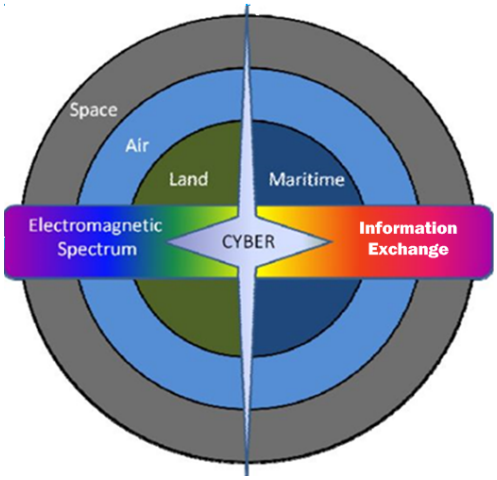

Figure 1. Air Force Doctrine Document 3-12, 15Jul10

As illustrated in Figure 1, Cyber touches five recognized dimensions of today's military: Land, Sea, Air, Space and Information. And, because the battlespace is seen as an integrated whole, Cybersecurity Engineering is also conducted within these five global operational dimensions and choreographed via the Information dimension. This dimension includes the electromagnetic spectrum medium.

What know from experience that every system has some unknown vulnerability – including DoD Weapon Systems. And threat actors of all types will seek diligently to identify and exploit the vulnerability of the software and hardware of these systems. The simulations that represent these DoD systems should reflect to varying degrees this vulnerability. This identifies our first key hypothesis.

Hypothesis #1 – Every System has a Weakness

There are new threats, and patterns that are introduced without warning. It's unreasonable to think that every system can be built without any vulnerabilities, or that preventive software or hardware will stop every threat. We must assume that every system is exploitable and has weaknesses. After all, that's the assumption being made by rouge players in the cyberspace domain. We should assume the same, that includes program managers, architects, engineers, developers, and users not just cybersecurity professionals. Doing so, will allow us to begin to think even more proactively.

If we know our enemy – their tactics – and know ourselves – our strengths and weaknesses – we can greatly reduce our risk. Consider the sage advice of Sun Tzu.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles.
If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself, you will succumb in every battle."

Those words written in the 5th century BC are profound and ring true today as it relates to cybersecurity. The opportunity before us is to do all that we can to know ourselves and know our enemy. Cybersecurity shouldn't be an afterthought – it should be forethought. With this belief in mind, we pose a question. ***How can a meaningful environment be constructed representative of the five dimensions that provides a means to know ourselves and know our enemy without risk or compromise?*** This paper provides a framework for that decision bounding process.

The Value of Modeling and Simulation

Embracing Sun Tzo's philosophy, we began with a declaration. There is no greater tool to create greater cybersecurity awareness than the use of modeling and simulation. Quite simply, M&S offers a means to know ourselves and know our enemy. If Sun Tzu was alive today, he'd use it. And when it comes to effective cybersecurity there may be no greater tool that's underutilized.

Hypothesis #2 – M&S offers the best tool to evaluate the impact of cyber threats and system weaknesses

Cybersecurity is all about the engineering and testing of systems functionality to protect the system(s) commensurate with the value of both the systems and data for the users, owners and stakeholders. Cybersecurity is rarely accomplished in isolation. All systems are designed to operate within an architecture of some form or another. The Cyberspace domain can be depicted as 3 "architectural like" layers (Physical, Logical and Social), and within these layers are the components of Cyberspace (Geographic, Physical Network, Logical Network, Persona, and Cyber Persona). This is illustrated in Figure 3. Each of these layers are important represent within an M&S environment.

The **Physical Layer** aspect is where Cyberspace components tie to the other domains. These are the things that are "touchable" items within Cyberspace. These are things such as the hardware, and infrastructure (wired, wireless, and optical) and physical connectors (wires, cables, radio frequency/electromagnetic spectrum, routers, servers, Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), programmable logic controller (PLC) and various computers).

The **Logical Layer** is technical in nature and consists of the logical connections between network nodes. Nodes are defined as any device connected to an IP addressable network.

The **Social Layer** is the human and the cognitive aspect of Cyberspace. First, the Persona Components are how people and groups are addressed in Cyberspace (e.g. e-mail address, IP address, cellphone number, Twitter tags, work-role and others). The Cyber Persona is the actual person operating in Cyberspace. People operating in Cyberspace can have many Persona Components but the Cyber Persona is the link to the actual person(s). When rogue individuals and/or enemy organizations from the "Social Layer" perpetrate malicious attacks, three things must be present; (1) Motive, (2) Opportunity, and (3) Means.

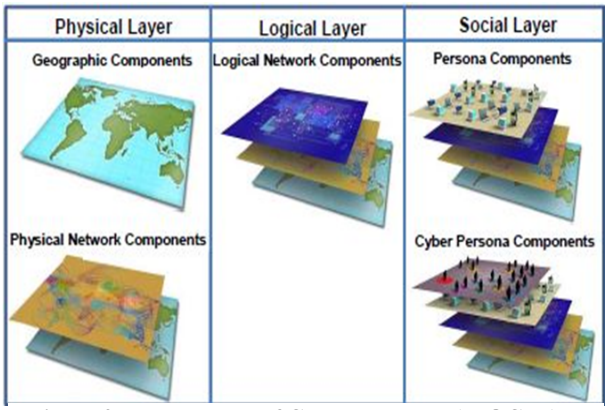

Figure 2. Three layers of Cyberspace, TRADOC PAM

(1) Motive: This is the "who and why" of the attacker.
(2) Opportunity: This is the "where and when" of the attack.
(3) Means: Support the "why" of the attack.

Hypothesis #3 – M&S needs to represent / support each Cyberspace domain layer (Physical, Logical, and Social)

The Common Cyber-Threats

While the motivation of threat actors may be difficult to determine, their most probable attack tools, methods and vectors can be estimated, modeled and simulated with basic "Script Kiddie" commercially available or even free tools. The types of attacks against IT systems can be loosely grouped into the following:

- **Remote Attack** (e.g. exploits against services such as DNS, NetBios and/or other remote services),
- **Client Side Attacks** (e.g. aimed at Java, Flash, etc.),
- **Blind Side Attacks**, (e.g. all the exploits at once from the attackers tool kit(s) at the target system),
- **Fuzzing Attack** (e.g. bring a network or service down by flooding it with larger amounts of traffic than it can handle),
- **Denial-of-Service Attack** (e.g. SYN flood attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic),
- **Man-in-the-Middle Attack** where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Hypothesis #4 – Every type of cyber-attack is the representation of a Pattern, which can be modeled and cataloged in M&S

Many of these attacks and attempted exploits can be conducted by well known "Script Kiddie" tools. Well known attacks can then be modeled and simulated easily and most likely thwarted by commercially available Security Information and Event Management (SIEM) solutions. **However, astute Security Engineers need to be aware of the overt and convert aspect of the ever-growing "exploit development community".**

Just stopping "Script Kiddie" attacks isn't enough. For example, one of the oldest overt organizations is ZDI. Their market niche is known as "Bug Bounties" and ZDI is just the tip of the iceberg. Bug Bounty is a cooperative relationship with the intent of identifying and correcting application vulnerabilities. **The objective is to close vulnerabilities before they are exploited in the commercial market place, which is equivalent to our need within DoD.** Identifying software vulnerabilities has become a lucrative business with its own marketplace and Cyber-Actors with differing motivations and some with questionable ethics. Bug Bounty groups them by the color of a hat (white, gray, or black).

- **The White Market** - facilitates hacking contests and direct vendor communication to provide for responsible disclosure of the vulnerabilities (like ZDI).
- **The Gray Market** - is made up of legitimate companies that operate in the legal gray zone within the zero-day market and sell the exploits to governments and law enforcement agencies across the globe.
- **The Black Market** - is where software flaws are sold to the highest bidder to rogue actors that are willing and able to employ those exploits against Cyber targets.

Hypothesis #5 – The M&S community offers an effective venue for the White Market and thereby reduces the impact of the Black Market

The take away is that standard commercial network defense tools will stop many Cyber-threats, but not all. M&S provides the next logical space to be proactive in defending cyber-threats.

The Exploitation of Industrial Systems

Common attack vectors against Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA) are; vulnerabilities in the protocols, attacks through back doors, holes in the network perimeter, database attacks, communication hijacking and man-in-the-middle attacks, Cinderella attack on the time provision and synchronization. The functions of ICS components are to maintain and keep the infrastructure up and operating. These systems support the electrical power grid, pipelines (water, sewage, fuels, etc.) cell towers and data centers.

Hypothesis #6 – M&S provides a mechanism to represent Industrial Systems and the related Patterns of attack that might occur

The Vulnerability of Mobile Communication and IoT Devices

Mobile devices (e.g. radio based systems) must also be included as a target of the Cyber-Attack landscape and includes Military Link networks, deployable satellite based networks and the fastest growing category…. Smartphones and personal digital assistants. These devices give users access to many applications. However, smartphone security has not kept pace with traditional computer security. Technical security measures, such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and mobile phone operating systems are not updated as frequently as those on network supported computers. Wireless threats are loosely grouped into:

- **Access Control Attacks** – attempts to penetrate a network by evading WLAN access control measures such as Access Point MAC filters and Wi-Fi port access controls.
- **Integrity Attacks** - occur when the attacker send forged control, management, or data frames over a wireless network to perform another type of attack.
- **Confidentiality Attacks** – attempt to intercept confidential information sent over wireless associations.
- **Authentication Attacks** - occur when the attacker steals the identity of Wi-Fi client, their personal information, login credentials, etc., to gain access to network resources.

From a Security Engineering prospective the Internet of Things (IoT) must included. Currently an estimated 15 billion physical objects use the Internet to exchange data — That number is expected to reach 50 billion by 2020. IoT by its own definition is more than just cellphones but also includes smart watches to heart-monitoring implants and home automation. At the most basic level the IoT concept is that objects are linked to the Internet to enable the sharing of data and services to provide collaboration to accomplish a meaningful business and/or personal task. The impact of this to the Security Engineer is that the aperture of risk exposure has been radically increased. For the Cyber Engineer, defenses must be factored in for one of the weakest devices in the Cyber Environment terms of security. It should be assumed that mobile devices will be interacting with every asset that make up the critical components of the infrastructure.

Hypothesis #7 – M&S provides a mechanism to represent Mobile Devices and IoT and the related Patterns of attack that might occur

The Enterprise Architecture

The ultimate task of the Cyber Engineer is to render individual systems, networks, families-of-systems and systems-of-systems "Cyber Secure". The Cyber Engineer and supporting team must be able to re-create targeted aspects of the operational architecture to understand how and when to best leverage M&S capabilities. This task of re-creating specific aspects of the operational environment also demands the selection of an appropriate Enterprise Architecture Methodology. Hence the need for usable and robust Architectural products.

The disciplined approach for Enterprise Architectures has been around for about 30 years. The field of study was created to address two major problems: (1) System complexity: organizations were spending increasing amounts of capitol on IT and, (2) Poor business alignment: ***However, The Cyber Engineer must realize that architecture artifacts were developed to address linking architecture capability to business needs and largely do not address linking architecture capability to operational cyber defense requirements.***

In today's commercial sector, architecture approaches address different business niche requirements. We propose that architectures must also be adaptable beyond just aligning IT to business needs and to be extended to address Cyber's ever evolving Defense in Depth requirements.

Architectures must be the foundation for linking the "As Is" state of operational Cyber defense performance needs to the "To Be" state. Architectures are the living baseline for measuring and assessing impacts needed for Cyber defense. Additionally the architecture provides the baseline for determing when and where M&S can be applied.

Hypothesis #8: Both "As Is" and "To Be" Architectures can be represented and rendered using M&S

BRINGING IT ALL TOGETHER

In the abstract, we stated that there are four steps to configuring the modeling and simulation environment. Now that the critical components have been defined including eight key hypotheses statements, the next aspect is to examine how to bring it all together within the M&S space. First, however, let's review the hypotheses we have identified to support effective cybersecurity using M&S.

1. Every System has a Weakness
2. The best tool to evaluate the impact of cyber threats and systems weaknesses is M&S
3. M&S needs to represent / support each Cyberspace domain layer (Physical, Logical, and Social)
4. Every type of cyber-attack (i.e., threat) is the representation of a Pattern, which can be modeled and cataloged in M&S
5. M&S offers an effective venue for the White Market and thereby reduces the impact of the Black Market
6. M&S provides a mechanism to represent Industrial Systems and the related Patterns of attack (i.e., threats) that might occur among these systems
7. M&S provides a mechanism to represent Mobile Devices and IoT, and the related Patterns of attack (i.e., threats) that might occur among these devices
8. Both "As Is" and "To Be" Architectures can be (and should be) represented and rendered using M&S

These hypotheses provide the ground rules. It identifies specifically, what assumptions we can make and what capability is needed. The remaining of this section explores each of the four steps to support the vision.

Step One – Introduce Threat Systems into M&S Domains

By employing the combined use of both models and simulations – and they are different -- we can effectively represent the Cyber-Attack kill chain within Cyber-Warfare. The first step is to introduce a threat system into an M&S Domain. This M&S domain may be a real-time simulation network configured systems represented by a simulation, or it might be a Live Virtual Constructive (LVC) environment represented by a virtualized DoD system, or it could simply be a set of architecture models representing a DoD Weapon System that can be evaluated internally using Monte Carlos analysis.

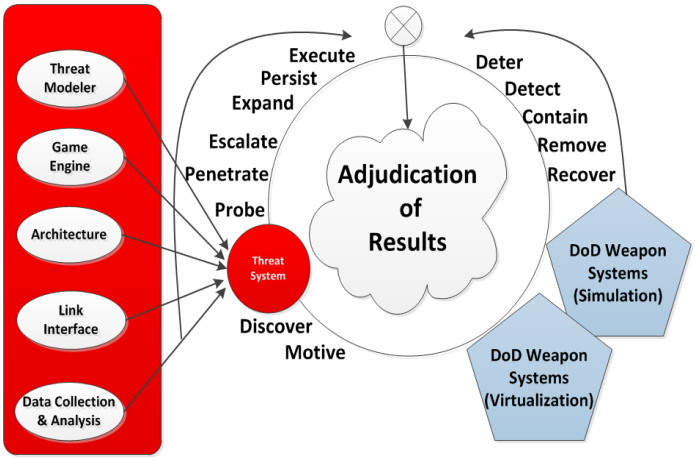

Figure 3. Gaming Theory Cyber Attack Model

For the purposes of this discussion, we will assume we are connecting into an environment featuring an existing simulation or a real system (or system component) that has been virtualized.

Our initial focus for Step One is primarily on a new component called a Threat System, which is made up of five components: (1) Threat Modeler, (2) Game Engine, (3) Architecture, (4) Link Interface, (5) Data Collection and Analysis. The Threat System represents an inconspicuous system on the network covertly trying to attempt entry into a DoD Weapon System, or affect its operation. Let's explore each of the Threat Systems components.

The Threat Modeler

The Threat Modeler provides a framework for modeling the threats that are appropriate for the targeted environment(s). It uses the concept of Patterns, much like what can be described by the SISO Base Object Model (BOM), to represent such threats. Using BOMs in this way, we can map to distributed architectures like HLA to dynamically inject new FOM modules within an environment. The BOM standard supports Hypotheses 4, 6, and 7.

A scenario for our Threat Modeler might be the representation of a "Man-in-the-Middle Attack". In this example, the attacker our system is representing might try to relate or alter the communication between two systems on a network that are attempting to communicate with each other. It may impersonate the federate. A BOM would have been created to represent variation of this type of threat, and during a live execution of simulations in play, the object model can be instantiated as either part of a threat scenario (see Game Board), or initiated manually.

The full type of threats that could be modeled as a BOM within the Threat Modeler include but are not limited to the following:

- Remote Attacks
- Client Side Attacks *
- Blind Side Attacks *
- Fuzzing Attack
- Denial-of-Service Attacks
- Man-in-the-Middle Attack *
- Access Control Attacks
- Integrity Attacks *
- Confidentiality Attacks
- Authentication Attacks

**Represents the predominate set of models (i.e., patterns) that would most often be represented*

The Game Engine

The Game Engine would support the attacker's scenario based upon the motivation and desired outcome – it provides a game board in combination leveraging the threats from the Threat Modeler. Employing the BOM type mechanism patterns we represent the game boards, and marries up the scenario models to the models of a threat.

Using the scenario we identified earlier, we might have a game board crated that identifies within it, threat models (others BOMs) it may use based on various Triggers. BOMs, as modeling framework, allows actions to be represented based on trigger events or messages. Because all data on a network has the potential to be absorbed by other systems, it is possible for a federation to be spoofed (imitated). The game board provides a mechanism to reflect the actions that might take place to support the federate impersonation. Every BOM offers a capability to reflect extensions and variations for any action or reaction that might occur. The potential exists is to have a myriad of game boards, which leverage and use the threat patterns described previously.

The Architecture Modeler

The Architecture Modeler component provides a way to reflect details of the system and system components that are in play (i.e., the system represented as a simulation) that we are interested in probing for the testing (e.g. white, grey or black box). For example, the Attack System via the game engine may be attempting to penetrate a weapon system that is reflected within the simulation network. This attempt and effort to infiltrate and strategize is coordinated via the building of a map of the known architecture – especially what can be known about that system. This essentially is what a cyber adversary would attempt to learn anyhow, so why provide that capability as a component.

The architecture elements of a system can be documented (captured) using the class constructs of the BOM, which would then be mapped with a conceptual model description of that system. This conceptual model describes how a system behaves (or we think it behaves), whereas the *classes* describe how the architecture is defined. One mechanism to dynamically build architecture models is to import the object and interaction classes that the simulation – as a federate in an HLA environment for example – uses. Namely take hold of what it publishes on the network. These FOM object and interaction classes provide a framework for build architecture BOMs at the class level. During execution of the simulation (or virtualized system), any incoming information regarding the object updates and interactions of that weapon system that are generated, can be used to dynamically build a representation of that architecture. Granted, this architecture would lack the internal workings of the system, but it does expose enough of the system, and the patterns of its behavior, to create a map of the published and exposed layers of a system. It's not an x-ray scan of a system, but it is close, and we can use that scan as a map to mark areas of vulnerability. As threats are applied and used against an architecture, the map can be marked with virtual pushpins indicating what we've tried to penetrate, and what response resulted.

What we ultimately care about an Architecture is the "cause and effect" that a threat may have upon it. This Architecture component could also be used in a faster than real-time application using Monte Carlo analysis as a means to determine system vulnerability and behavior in response to threats.

A game board, may be leveraged by the Architecture Modeler as an external system; then monitored by watching the network traffic. Eventually enough information is gathered to know the patterns and portray that system if the criteria on the Game Board warrants a "Man-in-the-Middle" Attack. Ideally, the Architectural Modeler should not only be able to play offense in a White Hat scenario, but also provide the analysis to improve the system defense.

The Link Interface

The Link Interface provides the capability for the threat system to integrate within a distributed network such as HLA, DIS, or DDS, and is needed to represent the attack vector based on the parameters established from the kill chain. In other words, it sends "cause" objects and events into the environment, and receives "affect" objects and events from the systems at play. (Note: this Link Interface serves to support the adjunct connection needed for Step Two described in the next section).

In our scenario related to the "Man-in-the-Middle" attack, we need a mechanism to gather network data in make sense of it. This where the Link Interface comes into play. Additionally, the Link Interface can also be separate component, such as tool like SimVentions Dexter tool that is used to integrate (i.e., bridge) disparate systems together.

The Data Collection and Analysis Component

The Data Collection and Analysis Component will provide the feedback to the execution of the Cyber-Attack kill chain. It will give us a means to evaluate cyberwarfare in an M&S environment that represents a real-world scenario. This is an important component to Step Three.

The Architecture Modeler provides a way to scan and learn the idiosyncrasies and behavior of other systems. What is important is the gathering of that data to support after action review. Such analysis provides a means to improve system defense against cyber threats.

Step Two – Evaluate Impact on DoD Weapon Systems using M&S

The evaluation of a cyber-attack, in our scenario, is not limited to just the view from the attacker. The opportunity exists also to counter defend, and gain a view from the weapon system, or any other system that is trying to perform its job. Therefore, the next step is to evaluate the impact of a cyber threat on a DoD system. In this realm, we move from the offensive posture of Step One with a Threat System, to the defensive side of a DoD system. This is depicted on the right-hand side of Figure 3. The targeted DoD systems will either employ defensive measures to mitigate attacks or try to operate as normal. In either case, we want to determine the operational performance impact after a threat or attack. These DoD systems, as described earlier, are either represented as a Simulation or interfaced as live equipment through Virtualization such as a hypervisor environment.

Both representations will support both Red and Blue actors by capturing the results for real-time and post event analysis. It is critical both offensive and defensive interactions are monitored for cause and effect. Also through utilizing virtualization technology we can manage multiple operating systems (or multiple instances of the same operating system) on a single computer system. Then, through a hypervisor instance, we can include physical system for analysis. Virtualization allows processor, memory, and other resources to quickly be reinstalled when damaged and returned to a normal operational state.

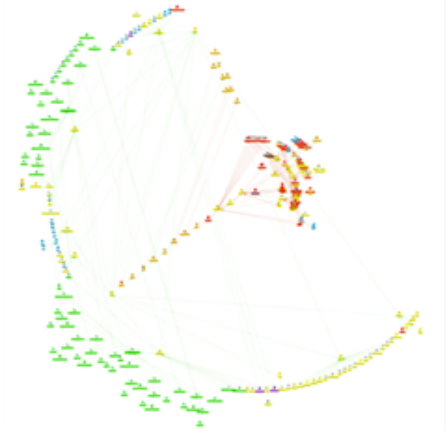

Figure 4. Network Connection View

The important factor to understand for Step Two is to recognize that these systems are likely ready to be used today – either as simulations or virtualization – and have little to no Cyber-defensive representations in the simulation space. Therefore, what we need is an adjunct to such systems that can model various defensive postures. Using the same architecture as the Attack System, we can instantiate this adjunct system to run in parallel with a DoD system (simulation, stimulator or virtualization). In this way, we can begin to evaluate how a system can be more resilient in a cyber rich environment

Cyber Warfare is conducted within Cyberspace. It is the newest and most complicated threat to National Security. To counter this leading threat, the DoD needs to understand their architectures to determine the best means to protect networks, communication lines, combat systems, and command and control elements. The same Threat Attacker module (described in Step one) using the same scenario, can be used conversely as an adjunct to support an existing system. In this adjunct role, the Threat Attacker module can arbitrate on the behalf of the simulation (or system) as it relates to cyber threat. Namely, it will evaluate incoming threats, and, using its own game board specific to the system it is supporting, to respond accordingly. In this mode, it might monitor, to learn the behavior of the attack system building its own Architecture Model of the threat system, or in another mode it might coordinate a defensive posture to thwart an attack.

It can also be used to determine the level of impact and the ensuing system degradation that occurs for the system its supporting. In this way, the cyber sim vulnerability representation doesn't need to be modeled by the system, but it can be carried out by the adjunct. The benefit is minimal code modification to an existing system. It offers a "do no harm approach". The adjunct, in this role, simply needs to deselect the type of message (objects and interactions) that the system would normally sends or receives. The adjunct, essentially, limits the bounds of the system.

Step Three – Use an M&S Catalog for Threats, Game Boards, and Architectures

The third step is to consider leveraging and use of an M&S Catalog (or equivalent) to capture and access various threats, game boards, and architectures. The Attack System, and its converse instantiation as an Adjunct tool to support DoD systems would use the catalog (or equivalent) to access such models.

Presently, the fastest method for standing up capabilities is to simply reuse or repurpose existing M&S suites. A primary source is the Defense Modeling & Simulation Coordination Office. They provide access to thousands of M&S based assets. These assets also include models of Threats, Game Boards, and the Architectures representing operational simulation systems. And the assets can be leveraged either at design-time, real-time, or after action.

The M&S Catalog currently can be searched by topic powered by IBM's Watson Enterprise Discovery search engine and includes Federated sites outside of the Catalog. The Catalog supports the visibility component of the net centric data strategy and provides an avenue for M&S organizations to make resources available for reuse.

The Enterprise Metacard Builder Resource (EMBR) tool complements the Catalog and was developed to offer organizations local control and management of their M&S assets; assets are then be published to the Defense M&S Catalog. The Enterprise Metacard Builder Resource (EMBR) is a free, GOTS tool to help your team collect, organize, and share Defense M&S information and resources, making the managing and sharing of assets easier.

Step Four – Use Analysis Tools to Evaluate Architecture Stability

Cyber engineers need the ability to visualize enterprise network architectures across individual platforms, classes of platforms, and theater based battle groups. They need to be able to plan virtual cyber testing, develop plans for commonality and technical refresh as well as performing strategic planning to counter potential network intrusions. The fourth step is to leverage the use of analysis tools that connect related data.

One mechanism to support this Enterprise Architecture need is a tool called lnformedb Enterprise, which has been developed by SimVentions. This tool allows a group to define their own schema and collect data into an extensible model to build an accurate representation of the programs static and dynamic relationships. The lnformedb Enterprise has application to many functional domains beyond systems engineering including cyber security, cyber architecture, configuration management, system load-out planning, model validation, and many other uses. Cyber engineers presently use this capability to:

- Visualize network architectures
- Perform alternative routing pathways
- Develop technical refresh timelines
- Perform configuration management and audit IT systems
- Generate required certification and accreditation artifacts such as HW/SW lists and connectivity views

Cost savings are found in the development and generation of artifacts currently built by hand in PowerPoint, Excel, and other standalone office products. Advanced query functions and dynamic views of architecture data can transform previous one-dimensional views into three-dimensional. For example: with the correct schema and data attributes in place a user can quickly identify IT systems connected to the network sorted by equipment type, functional use and location. Displaying interconnected systems can also be viewed at multiple levels of abstraction.

SUMMARY

Our Military is facing a Cyber based enemy with capabilities that range from simple "Script Kiddie" attacks to those of Nation-State's caliber. Cyberspace is growing more complex with ever increasing interconnectedness. The opportunity exists to leverage Modeling and Simulation (M&S) in a novel and proactive way to represent and assess security vulnerabilities, and engineer and test security enhancements without compromising operational integrity. Specifically, M&S must be exploited for both modeling the threats and realistically modeling the operational

environment to be defended. This paper has presented four steps to provide this capability using M&S. It includes the following:

1. Introduce Threat Systems into M&S Domains
2. Evaluate Impact on DoD Weapon Systems using M&S
3. Use an M&S Catalog for Accessing New Threats, Game Boards, and Architectures
4. Use Analysis Tools to Evaluate Architecture Stability

Consider again the need for such a solution. Cyber threats are now a primary concern. DoD must have the ability to evaluate the impact of cyber threats among existing fielded and future systems in order to improve and modify the baseline defense capabilities – and to know the enemy. The union of Cyber-based architectures, M&S capabilities combined with live, virtual, and constructive simulations and/or tactical system components hosted in a hypervisor environment provides an effective tool to prepare for and respond to evolving Cyber Threats.

REFERENCES

[1]Field Manual 3-38 Cyber Electromagnetic Activities, Feb 2014, page 1-4, https://fas.org/irp/doddir/army/fm3-38.pdf, accessed January 2017

[2]DoD Standard Practice Documentation of Verification, Validation, And Accreditation (VV&A) For Models And Simulations, MIL-STD-3022 w/Change 1

[3]EC-Council, Ethical Hacking and Countermeasures v7., Module XV

Harris, Shon All in One, CISSP Exam Guide, Fifth Edition, copy right 2010, page 889

[4]Hewlett Packard Enterprise Security Research, Cyber Risk Report 2016

[5]https://ics.sans.org/blog/2016/12/20/how-do-you-say-ground-hog-day-in-ukrainian/ , accessed January 2017

[6]https://mscatalog.msco.mil/ , accessed January 2017

[7]https://msdn.microsoft.com/en-us/library/bb466232.aspx , accessed January 2017

Jaswal, Nipun Mastering Metasploit, Second Edition, page 222

[8]National Institute of Standards and Technology. Guidelines on Cell Phone and PDA Security (SP 800-124).

[9]Weidman, Georgia, Penetration Testing, A Hands-On Introduction to Hacking, 2014, page vii

[10]www.cert.org/cybersecurity-engineering/, accessed January 2017

[11]www.cisco.com/c/en/us/solutions/internet-of-things/overview.html, accessed January 2017

[12]www.mcafee.com/us/products/siem/index.aspx, accessed January 2017

[13]www.rafayhackingarticles.net/2010/03/free-hacking-tools-for-every-hacker.html, accessed January 2017

[14]www.rh.gatech.edu/features/preventing-click , accessed January 2017

[15]www.securityweek.com/top-3-threats-industrial-control-systems, accessed January 2017

[16]www.webopedia.com/TERM/T/TCP_IP.html, accessed January 2017