M&S JOURNAL

A DoD MODELING & SIMULATION COORDINATION OFFICE PUBLICATION | SUMMER 2013

Cyber Warfare is no Computer Game

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
M&S Journal, Summer 2013	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Modeling and Simulation Coordination Office,4800 Mark Center Drive, Ste. 16E08-08,Alexandria,VA,22350**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
M&S Journal, Summer Edition 2013,Volume 8 Issue 2

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**57**	

FROM THE EXECUTIVE EDITOR

While the cover of this issue is a fanciful representation of cyber warfare, we are all aware that this is a serious topic. Computer virus infections, hacking, and large-scale network disruptions are common. Dr. Norbert Wiener, the MIT mathematics professor who first coined the term “cyber” in 1948, noted, “Progress imposes not only new possibilities for the future but new restrictions.” The Department of Defense (DoD) relies on information technology possibilities; now DoD must also face the restrictions. This issue’s articles illustrate the support M&S provides to understand both the possibilities and the restrictions of cyber warfare.

Dr. Steven King, in his guest editorial, sets the stage for the use of M&S in cyber warfare. Dr. Mark Gallagher and Dr. Michael Horta describe the Cyber Joint Munitions Effectiveness Manual (JMEM) and the need for mission planners to project and understand the effects of cyber warfare. Mr. Ryan Norman and Mr. Christopher Davis present the Cyber Operations Research and Network Analysis (CORONA) project that provides an enterprise framework for reconfigurable cyberspace test and experimentation. Mr. Scott Musman et al., provide insight into a military unit’s ability to conduct its mission during a cyber attack in terms of continuing the mission, knowing those aspects of the mission impacted, and recognizing the cyber attack when it occurs. Ms. Stephanie Harwell and Mr. Christopher Gore describe simulators that advance technical skills to “train as you fight” in the cyber arena.

Since many DoD capabilities depend on computers, networks, and communications, cyber attacks threaten national security. DoD can use M&S to understand and mitigate these threats as well as to enhance its cyber capabilities. As indicated in these articles, we hope you will find that DoD is making great strides in addressing both.

GARY W. ALLEN, PHD
Associate Director M&S Data
Modeling and Simulation Coordination Office (M&SCO)

Table of Contents

Guest Editorial: Cyber

GUEST EDITOR

Steven E. King, Ph.D.
Deputy Director, Cyber Technologies
Information Systems & Cyber Security Directorate Research Directorate
Office of the Assistant Secretary of Defense (Research & Engineering)

THE GROWTH OF COMPUTERS AND INTERNET USE SINCE THE 1990's HAS BEEN STAGGERING. DURING THIS TIME OUR NATION HAS GONE FROM SIMPLE DIAL-UP ACCESS THAT ALLOWED FILE SHARING TO THE UBIQUITOUS BROADBAND ENVIRONMENT OF TODAY THAT ADDRESSES ALL ASPECTS OF OUR LIVES FROM PRIVATE TO PUBLIC. THE INTERNATIONAL SCOPE OF ACCESS IS ON A SCALE WE COULD NOT HAVE IMAGINED 20 YEARS AGO. WITH THESE TECHNICAL ADVANCES COME RELATED THREATS. INITIALLY THESE THREATS WERE FEW AND COULD ONLY BE COMMITTED BY HIGHLY SKILLED PERSONS. THE OPPORTUNITIES TO CAUSE HARM WERE LIMITED AS THE ON-LINE ENVIRONMENT WAS ALSO LIMITED. HOWEVER, AS THE CAPABILITIES HAVE EXPANDED SO HAVE THE THREATS. THE EXPANSION HAS GROWN TO THE POINT WHERE IT HAS GONE PAST THE PRANKS OF INDIVIDUALS TO A WIDE RANGE OF CYBER-CRIMINAL ACTIVITY. THE CURRENT SPECTRUM OF THREATS INCLUDES CYBER-ESPIONAGE, THE MASSIVE LOSS OF INTELLECTUAL PROPERTY, BOTH FROM BUSINESSES AND GOVERNMENT, AND THE POTENTIAL DAMAGE TO OUR CRITICAL INFRASTRUCTURES FROM STATE SPONSORED CYBER ACTIVITIES.

The term "Cyber" covers a broad spectrum with the possibilities and threats of that spectrum well described in the following quote from the Department of Defense Cyberspace Policy Report from 2011: "Cyberspace is a critical enabler to Department of Defense (DoD) military, intelligence, business and, potentially, civil support operations. While the development and integration of cyber technologies have created many high leverage opportunities for DoD, our increasing reliance upon cyberspace also creates vulnerabilities for both DoD and the Nation."

Steven E. King, Ph.D.

The Cyberspace Policy Report is only one of the related strategic planning documents that highlight the need for continued developments in cyber science and technology. Recognition of the problem space, however, requires focus on critical areas of priority research. To that end the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) has established overarching themes to guide future research efforts. These key themes are briefly defined as:

- **Assuring Effective Missions** – developing tools and techniques that enable efficient models of blue, grey, and red behavior for both cyber and kinetic environments, in order to determine the correct course of action in the cyber domain.
- **Agile Operations** – developing mechanisms that enable dynamically changing cyber assets to be marshaled and directed toward an objective, in order to create and/or maintain a defensive or operational advantage.
- **Resilient Infrastructures** – developing integrated architectures that are optimized for the ability to absorb shock and the speed of recovery to a known secure state.

■ **Foundations of Trust –** developing measures of trustworthiness for components within the cyber infrastructure, and to large systems where components and participants have varying degrees of trustworthiness.

Taken together one can readily see this is a broad landscape to cover and will require the best DoD has as a team effort. Today we envision a significant part of that effort is the need for work in modeling, simulation, and experimentation, as well as the DoD research needed in the embedded, mobile, and tactical cyber domains. The idea of providing focus also applies to the efforts of the modeling and simulation (M&S) communities to best support DoD. At this point DoD needs to develop M&S capabilities that are able to simulate the cyber environment in which the DoD operates in sufficient fidelity to represent the current and future cyber threats and the operation of cyber defenses. Such capabilities enable a more robust assessment and validation of cyber technology development. DoD also needs real time cyber M&S of operational systems and networks at scale to improve situational awareness, analyze cyber mission threats and execute the course of action analysis to enable missions in a degraded cyber environment.

In order to work toward this goal the ASD(R&E) Cyber Modeling and Simulation Campaign (CMSC) is an initial study to inventory and characterize the tools and capabilities available to support cyber M&S, to reach out to the community in order to identify specific M&S research and integration challenges, and to identify the needs for cyber and cyber-kinetic exercises. This effort will establish a plan to develop cyber M&S tools and techniques that enable analytical modeling and multi-scale simulation of complex cyber systems. The CMSC will explore M&S tools and techniques that will drive innovation in research, aid in integrated experimentation, improve new technology transition to operations, and simulate the cyber environment with sufficient fidelity to integrate cyber M&S with the traditional M&S environment related to the kinetic domain.

Partnered with the M&S challenge is a second thrust area, the Cyber Measurement Campaign (CMC). The CMC invests in new analytical methodologies, models, and experimental data sets to establish metrics to measure a system's current security posture, and apply these scientific principles to promising technologies in order to determine their effectiveness against adversary actions. The CMC has conducted an inventory and assessment of cyber experimentation and test range technology that provide for the conduct of controlled, repeatable experiments. These testbeds and ranges need to be scalable and with sufficient realism to assess the effectiveness of new cyber tactics, procedures and technologies.

What I have outlined here reflects only the beginning of what will prove to be a long-term commitment to providing for national security. By way of contributing to that greater effort the DoD *M&S Journal* provides a way to educate the M&S Communities and highlight products and concepts that address the challenges outlined. I invite all readers to take advantage of what is presented.

Author's Biography

Steven E. King, Ph.D.

Dr. King is the Deputy Director for Cyber Technology in the Information Systems and Cyber Security Directorate of ASD(R&E). His responsibilities include coordination of the DoD S&T investments in Cyber Security, Information Assurance (IA), Biometrics, and Computer Network Operations, interagency S&T coordination/collaboration and chair of the DoD Cyber S&T Working Group. He has led efforts to create major new Cyber Security S&T Initiatives within DoD including a large expansion of OSD cyber security Small Business Innovation Research projects, two new ASD(R&E) Program Elements and major new funding at DARPA. Dr. King led the Cyber Priority Steering Council as it developed a roadmap for cyber research in DoD. He has led studies as part of the Guidance for the Development of the Force (GDF) and the National Military Strategy for Cyber Operations Implementation Plan which resulted in new research initiatives on Cyber Conflict Defense. He represents the DoD research community in numerous interagency forums.

Dr. King was trained as a research physicist specializing in basic and applied nuclear radiation detection, nuclear environmental studies and nuclear spectroscopy. He earned a B.S. degree and a Ph.D. degree in nuclear physics both from Duke University. His career included stints as a senior scientist at Technicare in medical imaging, as a research physicist at the Naval Research Laboratory, and as a program manager within the U.S.-Russian Joint Commission under Vice President Gore and Prime Minister Chernomyrdin. Dr. King was the first Director of the Defense Venture Catalyst Initiative (DeVenCI) which was created to explore ways to engage the Venture Capital community to identify and enable rapid insertion of emerging technology into DoD. He is the recipient of the DoD Exceptional Civilian Service Award and the DoD CIO Information Assurance Award. He has published 37 refereed papers and edited/sponsored several books on DoD information security research.

Cyber Joint Munitions Effectiveness Manual (JMEM)

AUTHORS

Dr. Mark A. Gallagher
Studies and Analyses, Assessments, and Lessons Learned
Headquarters, United States Air Force (AF/A9)
Washington, DC 20330-1570
Mark.Gallagher@pentagon.af.mil

Dr. Michael Horta
USCYBERCOM/J38
Offensive Cyber Operations
9800 Savage Road
Fort Meade, MD 20755
mchorta@cybercom.mil

KEYWORDS

Cyber analysis and planning, cyberspace operations, computer network attack, computer network defense, cyber analytics, Joint Munitions Effectiveness Manual (JMEM), information operations

ABSTRACT

THIS ARTICLE SUMMARIZES A TEN-YEAR EFFORT TO DEVELOP CYBER PLANNING TOOLS EQUIVALENT TO CONVENTIONAL OR NUCLEAR WEAPON PLANNING MODELS AND DATA. CYBER OPERATIONS REQUIRE MORE DETAILED DATA BECAUSE OF THE PRECISE TECHNICAL NATURE OF THESE ACTIVITIES; HOWEVER, SECURITY CLASSIFICATIONS, WHICH HINDER AN ADVERSARY'S ABILITY TO EASILY REMOVE VULNERABILITIES AND PROTECT INTELLIGENCE SOURCES, MAKE OBTAINING EFFECTIVENESS DATA DIFFICULT. WHILE SOME ARGUE THAT SIMILAR PLANNING DATA IS NOT APPROPRIATE FOR CYBER, WE CONTEND THAT, LIKE THE CONVENTIONAL WEAPONS, SOME SITUATIONS REQUIRE PLANNING EFFECTIVENESS CALCULATIONS. WE CONCLUDE BY PROPOSING A SCHEME WHERE HIGHLY CLASSIFIED AND PRECISE TESTS ARE CONDUCTED; HOWEVER, ONLY AGGREGATE DATA THAT DOES NOT REVEAL HOW THE CYBER EFFECT IS ACHIEVED COULD BE PROVIDED TO OPERATIONAL PLANNERS.

INTRODUCTION

What models and data does the military need to plan and execute cyber operations? What analytical capability is needed to support resourcing decisions for cyber operations? Many individuals answer these questions with analogies to what has worked well for conventional weapon systems. Others contend that cyber activities are so vastly different from kinetic operations that the approach for kinetic systems cannot even be adapted. Some even claim that the cyber domain is so dynamic that models and data are irrelevant. In this article, we address these questions along with the various viewpoints by summarizing a ten-year effort to adapt the best of kinetic modeling to better support cyber operations—Cyber JMEM. Our answers are "it depends" upon the type of cyber operations; our discussion concludes with proposals on when and how models and data can be helpful for cyber planning and operations.

In this introduction, we examine the joint planning system with particular focus on the joint targeting cycle. In the subsequent three sections in this article, we examine its application in kinetic, information operations, and cyber. First, we review planning and operations data used for kinetic systems, particularly the development and use of JMEM. This discussion will include both conventional and nuclear weapons along with aircraft penetration effectiveness. Our second section summarizes the Information

Operations (IO) JMEM, which includes the cyber modeling initiatives. The third section examines the successes and challenges of extending the approach for kinetic systems to cyber operations.

Joint Publication 3-13 [6] defines IO as:

> *the integrated employment, during military operations, of IRCs in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.*

Prior to the Secretary of Defense Memorandum [5] on 25 January 2011, IO was defined as the five pillars of computer network operations, electronic warfare, psychological operations, operational security, and military deception. The new definitions categorize these actions as information-related capabilities (IRCs) within IO. Since IO is now a process, rather than capabilities, we need to revise the IO JMEM name. Our goal remains to produce, accredit, and distribute effectiveness models and associated data for IRCs for planning, operations, analyses, and resourcing. We contend that providing evaluation techniques, which are similar and compatible to JMEM for conventional weapons, is a key step in employing IRCs. Ultimately, we strive to institutionalize IRCs through their integration with kinetic means.

For the United States military, joint operations planning is the process by which combatant commanders transform national strategic objectives into assigned military actions. Using predominantly "military art," the commander determines the military objectives while considering the operational environment, which includes the conditions, circumstances, and influences that affect the employment of capabilities. As the process proceeds, the commander and subordinates make more specific decisions. When military planners evaluate the ability to achieve effects against adversary systems, they apply the Joint Targeting Cycle, as defined in Joint Publication 3-60 [7]. This process guides the commander in selecting and employing capabilities against targets and then assessing the resulting effects.

Targeting is the bridge between military intelligence and operations. The Joint Targeting Cycle is a six step process that facilitates that interface between these two communities. The intelligence process identifies potential targets. including their functions and vulnerabilities, through the target development step. Operations provide the military means to affect the target in the capability analysis step. The Joint Targeting Cycle combines that data to provide recommendations to the commander on the ability of various attack strategies to achieve the desired effects.

A system may be thought of as comprised of components and linking arcs connecting those components. A system is a potential target if affecting its function would contribute to achieving the desired end state directly or indirectly. Each component and link has characteristics, some of which are vulnerabilities that can be exploited by military means. For example, the components of an airport consists of a runway, aircraft parking, fuel tanks, and repair facilities. The airport's function of generating aircraft sorties may be degraded by destroying the runway, aircraft, or fuel tanks. Each component and link has different vulnerabilities to attack. They contribute differently to system operation. Also each subsystem may be repaired or its loss mitigated in various manners. Hence, different attacks vary the extent and duration of their effect on the system's function.

Military objectives are usually offensive: degrading or destroying an adversary's system. However, military objectives can also be defensive, such as protecting the function of our allies' systems. Objectives for humanitarian operations frequently include maintaining particular systems' performance. In reliability modeling, assessing the impact of actions on system performance or on system degradation are mathematically equivalent [4]. Military planners tend to think in terms of the reliability of our weapon systems, and the degrading effects that those weapons inflict on the adversary system. Planners need to be careful and consistent to predict the system of systems likelihood of outcomes.

When military planners evaluate potential impacts on particular adversary systems, military science, with its inherent models and data, joins military art in supporting the necessary decisions. The process employs the Joint Targeting Cycle [7] with its six steps:

1. End State and Commander's Objectives
2. Target Development and Prioritization
3. Capabilities Analysis

4. Commander's Decision and Force Assignment
5. Mission Planning and Force Execution
6. Assessment

This iterative cycle begins with the commander specifying the desired "end state" or conditions that should be achieved. The target development examines the components of systems that the military can affect to achieve the desired end state. Capabilities analysis examines various military systems' abilities to exploit target vulnerabilities to achieve the desired effect. In the fourth step, the commander chooses particular military units to strike targets, and those actions are executed in the fifth step. Assessment is the process of collecting intelligence and determining if the desired effect was achieved. The cycle repeats because the assessment may cause the commander to modify the objectives for the subsequent cycle. While the general flow is followed, in reality, information produced at any step may result in returning to any of the previous steps.

Not surprisingly, the central component of the Joint Targeting Cycle is the definition of "target." Joint Publication 3-60 defines a target as *an entity or object considered for possible engagement or action*. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3370.01 [2] describes five target types: facility, individual, virtual, equipment, and organization. Every target has characteristics that affect the opposing military's ability to detect, locate, identify, affect, and assess it. The military's capabilities to exploit a target's vulnerabilities are a primary concern in determining if the desired effects can be achieved. For the last half of the 20th century, the United States military has used JMEM models based on empirical data in the Joint Targeting Cycle, particularly to support target development (Step 2), and capability analysis (Step 3), and to a lesser extent, assessment (Step 6). Therefore, we explain target development and capability analysis in more detail.

Target development is the systematic examination of potential target systems to determine the functional impact and its duration necessary to achieve the commander's objectives. Military planners, including intelligence targeteers, examine system components and the associated links to assess their impact on the overall targeted system performance and their potential vulnerabilities. Considerable data has been collected to support this process. The intelligence community classifies fixed installations by category codes that define their function and general features. They have also collected vulnerability information, such as the target buildings' type(s) of construction. The JMEM provides typical conventional weapon effectiveness against various elements. The military planners select as potential targets those targeted system components with vulnerabilities, which if exploited, will contribute to achieving the commander's objectives. Target vetting ensures the fidelity of the intelligence and analysis used to develop the target(s). For major adversary systems, the national intelligence community may assist in verifying targeting intelligence. Target validation ensures that targeting of specific system components complies with the law of armed conflict and the rules of engagement. Once targets are developed, vetted, and validated, the military planners nominate them for approval for military action in a given time period. When the commander approves a joint integrated prioritized target list, the target development step concludes for that planning cycle.

Capabilities analysis is the Joint Targeting Cycle step that evaluates existing military capabilities, usually weapon systems, against approved targets. The product of this step is appropriate options available to the commander. Evaluating specific capabilities against identified target vulnerabilities to estimate effectiveness is the crucial aspect; however, determining appropriate actions includes understanding many aspects: required resources, costs, risks including loss of personnel and weapon systems, expected effectiveness and its contribution to the objectives, and collateral effects such as possible civilian casualties. For conventional weapons, JMEM mathematical models and associated data support determining these weapon-on-target evaluations. The capability analysis builds the target development, both for information that characterizes the physical, functional, and behavioral vulnerability of the target, impact on the targeted system, and its contribution to achieving the objectives. The combatant command and its component planners use the capability analysis to make the force assignments that result in the course of action. The dynamic nature of target susceptibility to cyber actions affects how cyber capabilities can be integrated.

Over the years, particularly this last decade, military planners expanded both the range of targets and breadth of military capabilities considered in the joint targeting cycle.

The name of the third step changed from weaponeering to capability analysis to reflect the concept that the military can use a variety of means to accomplish its objectives. Better integration portends two benefits. First, selecting from a wider variety of alternative military means allows more options, and therefore should result in a better plan. Second, integrated consideration should enable accounting for synergistic effects. For example, a hypothetical jamming attack at one point may cause the adversary to resort to another communication system that improves targeting a different component. Without integrated planning, synergistic opportunities may be missed. In 2011, the Secretary of Defense [5] redefined information operations to give impetus to the concept of integrated planning.

In our view, implementation of integrated planning is encountering three practical challenges: scope, target description, and classification. For simplicity and speed, the scope of the Joint Targeting Cycle has focused on the offensive "end-game" of weapon release through target impact. The ability for the weapon delivery platform to arrive at the weapon release point has been considered separately. For strikes with conventional weapons, the operators consider it in their mission planning without extensive concerns; if they cannot strike it today, the target remains on the list for subsequent cycles. In contrast, planners for strategic nuclear strikes, concerned that there may not be another opportunity to strike the target, have established a separate process for assessing probability of arrival. As we discuss later, the end-game focus is problematic for cyber attacks; typically, probability of access is the difficult phase of a cyber attack, rather than the end-game probability of effect. Another aspect of scope on integration is considering how defensive systems contribute to achieving the objectives. Just expanding the analysis requirements to consider all military means would make the process considerably more complex and require more time. Many expressed similar complaints against another integrating concept called Effects Based Operations [1].

A second practical challenge to greater integration is expanding the considered targets. For example, some have proposed including behavior for segments of a population. While influences on behavior are clearly important for the military to consider, inserting these considerations into what is basically a weapon-target assignment process is problematic. Individual behavior is affected by culture, personal bias, and perceived actions over time. Connecting specific actions, like making a radio announcement or dispersing leaflets, with resulting behavior changes is considerably different than describing the physical effects of a weapon detonating on a concrete building. While different, and even more complex, the military should consider its actions more extensively, including impacts on population perceptions and their resulting behavior. Marketing corporations and political campaigns have clearly established connections between actions taken and population responses. However, the different scale of effects – from bombs-on-targets to messages for various target audiences – makes predicting their combined synergistic impacts to be a daunting task. Expanding target descriptions to include cyber vulnerabilities has a slightly different challenge. Generally, the intelligence community organizes their target information based on geographic location. Cyber vulnerabilities may be virtual nodes or links that are not physically located with other components of the targeted system. The intelligence community is relating the information of system components together, and they need to continue expanding in a similar manner to include the cyber components and their vulnerabilities.

A third practical challenge on integrating various means is differing security classification levels. While some dismiss this as merely a policy issue, there is serious justification for higher classification of some targeting information. Many cyber capabilities exploit vulnerabilities, such as computer network access, that an adversary could easily remove if they knew about them. Furthermore, our knowledge of foreign systems may expose our intelligence agents or sources. Hence, cyber operations are usually planned and conducted in a separate process conducted with more stringent security requirements. The value, and even existence, of Cyber JMEM is challenged by the needed security classification. However, if military planners are going to consider cyber alternatives, they need to have some indication of the potential cyber capabilities. We propose, in the last section of this article, a scheme where the highly classified data is aggregated to a lower classification that only describes the cyber effects and not the means of achieving them.

We discussed three practical challenges of scope, target descriptions, and security classification to expanding the

joint targeting cycle to account for other means. Furthermore, some combatants do not even accept this systematic approach at all. The average soldier or marine most likely would define "target" as what he points his rifle at, rather than installations on the approved joint targeting list. Similarly, many fighters, such as pilots providing close air support, strike targets of opportunity rather than vetted and prescribed targets. This difference of targeting pace underlies different views of planning cyber operations. Are cyber operations similar to a firefight or a strategic attack? The answer depends on the target, the attacker, combat conditions, and possibly many other factors. While many offensive cyber operations can fit in one of these categories, a clear distinction for others may not be possible. Some targets' vulnerabilities to cyber operations may be planned in advance, and subsequently these targets may be engaged in dynamic combat.

We examine these issues through kinetic planning in the following section and information operations in the next section. The final major section addresses the cyber issues.

KINETIC OPERATIONS PLANNING

In this section, we will examine conventional and nuclear weapon planning. We start with conventional planning because it has the most widely applied planning system. When we examine nuclear planning, we will see that it applies a variation of the same process.

Morris Driels, in his textbook and website [3], provides the history of JMEM for conventional weapons. In the early 1960's, the Close Air Support Board, which was composed of Army and Air Force personnel, identified "large gaps" and "gross inaccuracies" in the conventional munitions data along with differences in conventional weapon effectiveness methodologies. This Board recommended to the Joint Chiefs of Staff that they publish a joint manual containing "a list of targets with corresponding data on the effectiveness of aerially delivered munitions." In 1964, the Joint Chiefs of Staff directed the creation of what became the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) to publish a JMEM.

Over five decades, JTCG/ME has continually adapted to support the operational and targeting planners. Scientific, engineering, operational, and planning professionals from various DoD and intelligence community agencies continue to collaborate in these flexible forums. Their products provide the DoD with mathematically valid and standard methodologies to conduct weapons effectiveness planning and procurement. Currently, the Office of Secretary of Defense, Director for Operational Test and Evaluation, manages JTCG/ME. The Army is the lead service. The JMEM for conventional weapons relies almost exclusively on the test and evaluation community for their empirical data; therefore, the primary supporting agencies are the test communities of Army's Aberdeen Proving Ground, Air Force's Eglin Air Force Base, and Navy's China Lake. JTCG/ME responds to requests from all the combatant commands and military services.

JTCG/ME has developed, collected, accredited, and published numerous algorithms and the necessary data to evaluate the effectiveness of conventional weapons against targets. These JMEM products are the recognized standard for conventional weapons planning and are implemented in a wide array of DoD planning tools, models, and simulations. Since JMEM focuses on the end-game from weapon release through target impact, it combines the three aspects of target vulnerabilities, weapon characteristics, and mathematical methods. Targeteers using JMEM models and data typically produce a probability of damage (PD), which is the likelihood of destroying a particular target given a specified weapon release and conditions. In an effort to expand these capabilities, some analysts are calculating probability of effect (PE), which is the likelihood of achieving a functional impact against a target at a time (that may be delayed) and duration (depending on adversary response) given specified initial conditions. Besides these probabilities, JMEM products include target system studies, target vulnerabilities, duration of effect, and collateral damage along with weapon characteristics including release conditions, delivery parameters, accuracy, reliability, and range. They vet each of their models though military service reviews to ensure the quality of their computational tools. The standardization has enabled planners to compare employment of alternate weapons. Planners are now demanding more precise information necessary for these tools from the intelligence community.

Besides operational planners, acquisition professionals, programmers, budgeters, and analysts use JMEM models and data to support resource decisions. All the current major combat simulations in the United States incorporate JMEM methods and data. Since these models support acquisitions and budgeting decisions, senior defense leaders are basing their force structure decisions on JMEM products. While the analytic community replaces these campaign simulations about every decade, the underlying JMEM models and data continue to be updated and maintained.

The nuclear weapons community developed a similar approach to maintaining the models and associate data for planning and executing nuclear missions. The Defense Threat Reduction Agency (DTRA) and its predecessors have maintained a model called Probability of Damage Calculator (PDCalc). The intelligence community has organized to determine the installation vulnerabilities. One of the main differences between planning with conventional weapons and nuclear weapons is the scope considered. Conventional planning data and models have focused on the end-game. In contrast, the strategic nuclear community has also been concerned with meeting the condition of weapon release that is assumed in the PD. Hence, the nuclear community also calculates probability of arrival (PA). Damage expectancy (DE) is the product of PA and PD (appropriately multiplied since PD as a conditional probability is statistically independent of PA). Analogously, the cyber community is using the product of probability of access (PA) and PE, called Effect Expectancy (EE). Similar to the nuclear planning paradigm, the analysis of cyber operations is evaluating the likelihood of achieving arrival/access.

IO JMEM HISTORY

In 2003, US Strategic Command conducted an offensive cyber operation experiment. As part of this experiment, we established an analysis group to predict effectiveness, and we purposely copied the JTCG/ME structure with groups for target vulnerability, weapon capabilities, and methodology to start developing the same analytical rigor as the conventional JMEM. In response to US Strategic Command's request for a computer network attack subgroup, JTCG/ME [8] approved our initiating an IO subgroup. We called this forum IO JMEM. Since, at that time, IO had five pillars – computer network operations, electronic warfare, psychological operations, operational security, and military deception – we organized six subgroups (dividing computer network operations into computer network attack and computer network defense). Since the Unified Command Plan in 2004 [9] assigned to US Strategic Command responsibility for IO crossing geographic areas of responsibility, our leading the IO JMEM under the JTCG/ME made sense. For oversight over the IO JMEM, we organized an executive committee and user groups. In 2003, we did not find anyone developing planning models for these information-related capabilities, so we started developing new models.

We encountered several challenges. Many argued that since IO actions were not munitions, using the name JMEM was not appropriate; however, the name JMEM provided great understanding for what we were trying to accomplish: produce planning models and data for these new capabilities. While we applied the JTCG/ME approval process, we needed to ensure the appropriate experts accredited the models. We continue to use the broader term of capabilities, rather than weapons or munitions, to discuss the information-related capabilities.

Many also argued that since JMEM only focused on the end-game from weapon release through target impact we also should maintain that limited focus. Our experience from conducting a cyber experiment indicated that often the reliability failures are not in the end-game. An advantage from this project being initiated at US Strategic Command is that we could draw on the begin-to-end nuclear strike analysis as a foundation. We adapted the phases extensively to represent computer network attack (CNA). We saw the phases including access, delivery, and even subsequent actions much more critical for IO actions. Hence, we decided that, just as JTCG/ME taking on IO was broader than traditional JMEM, the IO JMEM would address the beginning-to-end in its effectiveness tools for information-related capabilities.

The main challenge has been access to data, particularly test data on effectiveness. The JMEM for conventional weapons relies on the operational test and evaluation community to provide data. The behavioral information-related capabilities cannot even be tested on a range. While cyber actions can be tested, the concern about exposing vulnerabilities or intelligence sources requires strict clas-

sification control. Developing an approach to maintain the necessary security, yet provide sufficient data to provide adequate assessments for operators and planners, is crucial to further development of Cyber JMEM.

By 2011, IO JMEM had produced six accredited models (described in the Appendix). Even though many contend information operations are "too soft" for quantitative models, we demonstrated that tools that aid planners could be developed. Initially, the operational security experts were extreme skeptics; however, once they considered that most of their practitioners work as an additional duty, they realized a planning aide would be very beneficial to their community. In 2007, their Operations Security Collaboration Architecture (OSCAR) was the first JTCG/ME accredited IO tool. Two of the six IO JMEM tools apply to cyber. The US Strategic Command experiment led to the creation of Computer Network Attack (CNA) Risk Evaluation Analyzer (C-REA). This tool guides an analyst through each part of an offensive cyber operation to identify and quantify successes and risks. In addition, planners or analysts may use Network Risk Assessment Tool (NRAT) for a more aggregate evaluation of potential cyber attacks and their chance of success for either offensive or defensive cyber operations. NRAT may also be appropriate for analyzing future scenarios since it requires considerably few inputs. These tools are a start to institutionalizing these new capabilities into DoD's standard planning, operations, and resourcing processes.

Recently, three organizational changes have affected IO JMEM. First, while JTCG/ME continues to charter the IO JMEM, in 2011 the supporting lead switched from US Strategic Command to the Air Force Targeting Center (AFTC). A military service lead aligns better with the conventional JMEM. The realignment is also consistent with organizational changes in the Secretary of Defense memorandum and changes in the Unified Command Plan. Furthermore, the (AFTC) provides an operational and user perspective to the efforts. After the transition, AFTC reorganized the IO JMEM into three subgroups for cyberspace operations (CO), electronic warfare (EW), and military information support operations (MISO). In their joint role under JTCG/ME, AFTC oversees and manages the development, review, accreditation, and distribution of quantitative and qualitative models and data to evaluate capability effectiveness for CO, EW, and MISO. US Cyber Command leads the subgroup for cyberspace operations, which we have been calling Cyber JMEM.

The second organizational change is that the Secretary of Defense [5] redefined IO to be the process of overarching integration of capabilities. Since the JMEM focuses on effectiveness of information-related capabilities, the name of IO JMEM needs to change. AFTC, reflecting their goal to integrate all military capabilities, is calling these collective efforts the Joint Capabilities Analysis and Assessment System (JCAAS).

The third organizational change is that the test community is improving their ability to evaluate cyber capabilities. For example, the DoD Test Resource Management Center developed and is maintaining the Cyber Operations Research and Network Analysis (CORONA) capability. This suite of models enables detailed live, virtual, or constructive simulation of cyber networks. Cyber JMEM desires that the test community initiatives lead to providing cyber test data similar to how the conventional weapon test ranges collaborate with JMEM. While in many ways cyber is an emerging capability, these three changes incorporate cyber more in the established processes within DoD.

CYBER ANALYTIC CHALLENGES AND VISION

Data requirements change, and classification challenges exist in producing cyber JMEM. First, compared to conventional JMEM, more detailed data is required in two aspects. Whereas conventional JMEM focuses only on the endgame from after a weapon launches through impact, cyber actions are more affected by the ability to gain or maintain access to the target – even the means of access can significantly affect the overall effectiveness. Hence, Cyber JMEM must access the operation from a much earlier stage. In addition to modeling more of the operation, cyber effectiveness is often more dependent on small details such as the specific version of hardware devices or software installation – or even options enabled. As a result, the intelligence requirements are more detailed. Furthermore, many of these details change with normal network maintenance or periodic upgrades; hence, cyber predictions are valid for considerably shorter time periods.

Because of the ability to counter cyber attacks along with potentially exposing vulnerabilities to allied systems, cyber weapons are highly classified. Limited clearances inhibit the analysts' ability to build and use planning models. The combined impact of these challenges makes some question the viability of Cyber JMEM. In response, Cyber JMEM proponents contend these capabilities will not be employed to their potential without providing military leaders with credible assessments of the expected consequences and risks when they need to authorize use. Cyber JMEM provides the forum to debate, propose, and advance models and data that support planning, execution, and resourcing offensive cyber weapons and cyber operations.

Another major argument against Cyber JMEM is that cyber operations are dynamic and quick and do not allow time for planned modeling and assessment. However, many kinetic fights are also dynamic; we already mentioned soldiers entering into a firefight or fighters conducting close air support. JMEM techniques are not used real-time in these dynamic scenarios although commanders may use JMEM data to decide what rifles and other weapons their troops should carry or what weapons should be loaded on aircraft conducting close air support missions. Similarly, we won't expect a Special Forces team to check JMEM when using a localized cyber approach to affect a local network, such as jamming a wireless connection. However, they probably should use JMEM data in planning the mission to determine the likelihood their cyber technique would work if needed. Along similar lines, some contend that cyber is mostly an intelligence function and very little an operational attack. The counter argument is whenever the action is offensive, military authority must have a concept of the consequences when approving the attack. We contend, like JMEM for conventional weapons, that cyber JMEM would be useful in different ways in different situations.

We also contend that cyber effectiveness data is required for planning against strategic targets and determining resource trades. For major targets, military commanders need to have an idea of how likely the cyber actions will achieve the desired effect. Without sufficient data to build confidence, military commanders will rely on kinetic destruction of targets. The second aspect deals with senior leaders determining the amount of resources to commit to cyber operations. Without having models and data to indicate effectiveness, these leaders will have difficulty reaching a consensus on how much funding to dedicate to develop and conduct cyber operations. Spending funds on cyber reduces the available resources for other types of operations. Analysts show decision makers the implications of different resource levels through the use of effectiveness data.

Cyber effectiveness requires an extrapolation of the approach applied for conventional weapons. The JMEM methods for planning conventional weapons are not the most accurate. However, they are tools deemed sufficiently accurate to support planning and execution of the missions. The JTCG/ME has more detailed engineering models that are more accurate. These more detailed models are used to parameterize the actual planning tools so as to spare the intelligence community the frustration of being asked for extremely precise data, and similarly, help the targeteers avoid frustration from laborious and time-consuming input of voluminous data. Cyber JMEM has begun the necessary standardization of the processes through their development of a Target Vulnerability Manual and a Weapon Characteristics Manual to support offensive cyber operations. Analogous to JMEM for conventional weapons, cyber testing should be conducted at a detailed and appropriately classified level; then, the testers should provide the cyber planners aggregate effects data that does not reveal classified aspects of the weapons or targets.

SUMMARY

We reviewed the development and use of JMEM data in planning and executing operations with conventional weapons. We also discussed how equivalent models and data exist for planning nuclear operations. We discussed that cyber operations require more detailed data; however, security restrictions make that corollary data considerably more difficult to access. While some argue that similar planning data is not appropriate for cyber, we contend that, like the conventional weapons, some situations require the planning effectiveness calculations. Besides supporting operations, JMEM data also provides data for resourcing decisions, which are necessary for organizations that conduct or support cyber operations. We propose a scheme where highly classified precise tests are conducted; however, the planning tools should only include aggregate data that does

not reveal how the cyber effect is achieved or is provided to the operational planners. We conclude the equivalent of Cyber JMEM is necessary for cyber operations to perform to their full potential.

References

[1] Correll, John T., "The Assault on EBO," Air Force Magazine: Journal of the Air Force Association, Arlington, Virginia, Volume 96, No. 1, January, 2013, pp. 50-54.

[2] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3370.01, Target Development Standards, Joint Staff/J2, The Pentagon, Washington, DC, 15 September 2011.

[3] Driels, Morris, Weaponeering: Conventional Weapon System Effectiveness, American Institute of Aeronautics and Astronautics (AIAA), Reston, Virginia, 2004. www.weaponeering.com.

[4] Gallagher, Mark A., Gregory Ehlers, Wes True, and Marc Washburn, "Defining Effects for Probabilistic Modeling," *Military Operations Research*, Vol. 13, No. 4, 2008, pp. 5-18.

[5] Gates, Robert M., Secretary of Defense Memorandum, Strategic Communications and Information Operations in the DoD, Office of the Secretary of Defense, Pentagon, Washington, DC, 25 January 2011.

[6] Joint Publication 3-13, Information Operations, Joint Staff, Pentagon, Washington, DC, 27 November 2012.

[7] Joint Publication 3-60, Joint Targeting, Joint Staff, Pentagon, Washington, DC, 13 April 2007.

[8] JTCG/ME Memorandum to USSTRATCOM/PR, Aberdeen Proving Ground, Maryland, 10 November 2003.

[9] Unified Command Plan (UCP) 04, of the Secretary of Defense, Pentagon, Washington, DC, 1 March 2005.

APPENDIX: IO JMEM (2003-2011) MODELS AND PLANNING TOOLS

CNA Risk and Effectiveness Analyzer (C-REA)

C-REA provides a simple user interface to elicit expert planning input data for cyber operations. It provide overview information to support planning decisions as well as providing the user with an ability to generate logic models to calculate predictive assessments of risk and effectiveness. The output displays show assessments of where the operation might be changed to enhance effectiveness or mitigate risk of candidate CNA Courses of Action (COA). JTCG/ME accredited C-REA in August 2008.

Network Risk Assessment Tool (NRAT)

NRAT provides a high-level analytical tool for evaluating attacks on information systems. NRAT uses probabilistic risk analysis underpinnings to assess the likelihood of an attack based on the capabilities and intent of potential threat actors, the effect mechanisms of the attack, and the vulnerabilities of the target information system. Further, the risk assessment is completed by evaluating the potential severity of impact of the attack on the operational mission that the system supports. NRAT can provide insight to vulnerabilities and analyze the trade space of alternative security postures and operational support.

Operations Security Collaboration Architecture (OSCAR)

OSCAR is an interactive risk assessment tool to assist the operational security (OPSEC) planner and commander in determining OPSEC posture. OSCAR facilitates the analysis of threats based on a unit's mission, location, and critical information list, and recommends appropriate countermeasures to improve overall OPSEC posture. In November 2007, JTCG/ME accredited PC-OSCAR, which was the first IO JMEM operational tool they accredited. The web-based version of OSCAR is currently available on the SIPRNET at https://oscar.dtic.smil.mil/oscar.

APPENDIX: IO JMEM (2003-2011) MODELS AND PLANNING TOOLS (CONTINUED)

Communications & Radar Electronic Attack & Planning Effectiveness Reference (CREAPER)

CREAPER is an Electronic Attack (EA) JMEM-like decision aid capability that provides operational EW planners a geospatial EA effectiveness capability to assess communications and radar weapon-to-target pairings, QuickLook and Geospatial EA analyses, and a GWOT Ad Hoc Comms network (GRID) analysis. CREAPER calculates the initial Comms/Radar jammer-to-signal (J/S) ratio required to affect a target receiver and then applies the weapon manager's technique for achieving effectiveness. CREAPER provides war planners quantifiable EA effectiveness results for EW weapons systems.

Joint Broadcast Analysis Tool (JBAT)

JBAT is a predictive operational modeling capability for Psychological Operations (PSYOP) in support of operational and tactical level theater objectives. As a radio frequency (RF) based modeling capability, JBAT provides measurable and verifiable PSYOP system effects in the electromagnetic spectrum. As a planning capability, JBAT provides an initial operational capability of analysis of specific PSYOP systems effects against a specified target audience. JBAT has the ability to access a library of Geospatial Analysis tools which can be used to evaluate population densities, cultural and political areas. JTCG/ME accredited JBAT in March 2009.

Effectiveness of Psychological Influence Calculator (EPIC)

EPIC provides an analytical tool for forecasting the effectiveness of military information support operations (MISO) strategies. MISO was formerly called psychological operations (PSYOP). EPIC is grounded in MISO doctrine. EPIC evaluates MISO products with four primary factors: distribution, dissemination, reception, and accessibility. EPIC provides a logic mechanism to aggregate the effects of numerous products supporting a series, the strength of the argument or line of persuasion presented through the products, and the effectiveness of the target analysis to accomplish a Supporting MISO Objective and its satisfaction.

Authors' Biographies

Dr. Mark A. Gallagher

Dr. Mark A. Gallagher is a Senior Leader serving in the position of Technical Director in AF/A9. As a Captain, he was Chief of the Target Analysis Branch in the Targeting Division, Intelligence Directorate, Headquarters Strategic Air Command. As a Lieutenant Colonel, he led the Information Operations Analysis Branch (J533) at US Strategic Command. In this position, he supervised analyses of US Strategic Command's cyber experiment. After his military retirement, he held several civilians positions at US Strategic Command including Division Chief for Analysis Management. He founded IO JMEM in 2003 and led it until 2007. Since 2009, he has been a member on the JTCG/ME Steering Committee. In 2008, he chaired the Military Operations Research Society (MORS) Cyber Analysis Workshop. Currently, he is guiding the Air Force in developing cyber analytic tools. Dr. Gallagher earned a B.S. in operations research and computer science from the US Air Force Academy. He also earned an M.S. and PhD in operations research from the Air Force Institute of Technology, where he later taught and continues as Adjunct Associate Professor.

Dr. Michael Horta

Dr. Michael Horta is the Functional Area Lead to Cyber JMEM in addition to serving as the Technical Director in USCC/J38. He has an extensive military career that started as active duty enlisted growing to a reserve Officer where he continues to serve. He has earned several advanced degrees in computer science and business management.

Cyber Operations Research and Network Analysis (CORONA) Enables Rapidly Reconfigurable Cyberspace Test and Experimentation

AUTHORS

Mr. Ryan Norman
Test Resource Management Center

Mr. Christopher E. Davis
Sandia National Laboratories

KEYWORDS

CORONA, Test Resource Management Center (TRMC), cyberspace test, cyberspace experimentation, acquisition systems, common tools, architecture

CURRENT DEPARTMENT OF DEFENSE (DOD) CYBER TESTING CAPABILITIES CANNOT ADEQUATELY SUPPORT THE ROBUST CYBERSPACE EXPERIMENTATION AND TEST AND EVALUATION (T&E) NECESSARY TO PROPERLY TEST ADVANCED WEAPON SYSTEMS. ENVIRONMENTS ARE INADEQUATE BECAUSE INTEGRATING WHAT ARE TYPICALLY PROPRIETARY OR STOVE-PIPED CAPABILITIES IS COSTLY AND TIME-CONSUMING. THESE INTEGRATION COMPLEXITIES CAUSE FEWER RESOURCES TO BE AVAILABLE FOR ADDITIONAL ENVIRONMENT NEEDS, SUCH AS INCREASED OPERATIONAL REALISM AND POST-TEST DATA ANALYSIS. THE GOAL OF CORONA, A MODELING AND SIMULATION COORDINATION OFFICE (M&SCO) HIGH-LEVEL TASK MANAGED BY THE DOD ACQUISITION TECHNOLOGY AND LOGISTICS (AT&L) TEST RESOURCE MANAGEMENT CENTER (TRMC), IS TO BREAK DOWN THESE STOVEPIPES BY CREATING A MODULAR CYBERSPACE MODELING AND SIMULATING FRAMEWORK AND ENVIRONMENT THAT RAPIDLY INTEGRATES LIVE, VIRTUAL, AND CONSTRUCTIVE ELEMENTS. WITHIN ITS MISSION OF DOD TEST INFRASTRUCTURE OVERSIGHT, THE TRMC PROMOTES AN ENTERPRISE APPROACH TO THE DEVELOPMENT AND SUSTAINMENT OF CYBERSPACE INFRASTRUCTURE THAT LINKS EXISTING OPEN-AIR RANGES AND LABORATORIES USED TO TEST WEAPON SYSTEMS WITH CYBER-FOCUSED CAPABILITIES, SUCH AS THE TRMC NATIONAL CYBER RANGE. THIS ENTERPRISE APPROACH PROVIDES THE INFRASTRUCTURE NECESSARY TO PERFORM CYBERSPACE TESTING ON WEAPON SYSTEMS WHILE MITIGATING DUPLICATION, IMPROVING EFFICIENCY AND REUSABILITY, AND OPTIMIZING LONG-RANGE IMPROVEMENTS AND MODERNIZATIONS ACROSS THE DEPARTMENT. CORONA PROVIDES THE ENTERPRISE ARCHITECTURAL FRAMEWORK AND MATURES SELECTED CRITICAL TECHNOLOGIES IN ORDER TO ACHIEVE THIS ENTERPRISE APPROACH TO DOD CYBERSPACE INFRASTRUCTURE.

THE CYBERSPACE MODELING AND SIMULATION (M&S) PROBLEM SPACE

Traditional testing and experimentation practices are ill-suited for the rapidly changing and highly agile nature of offensive and defensive cyberspace capabilities development and deployment. The result is an inadequate M&S cyberspace test and experimentation environment for conducting test and evaluation (T&E) on DoD weapon systems. Some examples of the inadequacies of current practices include the following:

- Proprietary and/or non-interoperable government and industry stovepipes cause integration of live, virtual, and constructive (LVC) components to be a manual process requiring significant teams of highly-specialized Subject Matter Experts (SMEs)
- Tests and experiments expend funds on integration and setup at the expense of analysis and evaluation
- System representations are transient, hard to maintain, and hard to reconstitute
- Computer networks, threats, and cyberspace effects on systems are often white-carded or unrealistic
- The concept of security in depth is typically not represented well in test or exercise, resulting in analysis that generates both false-positives and false-negatives
- Robust cyberspace models have not yet been developed even though operating entire systems live is too costly, reduces availability, and, in some cases, is unsafe
- Humans-in-the-loop can create affordability, availability, sampling, and scalability issues
- Existing test and experimentation infrastructure prevents leveraging of commercial and academia best practices for agile development and testing

Fortunately, many of these inadequacies can be addressed or mitigated through investments in technological improvements to our cyberspace test and experimentation infrastructure. Specifically, the tenets of an efficient enterprise Cyberspace M&S Environment include the following:

- Seamless integration of LVC cyberspace capabilities
- Common mechanisms for experiment command and control
- Persistent representation of complex networks and systems

CORONA is a M&SCO High-Level Task managed by the DoD AT&L TRMC and executed by Sandia National Laboratories, Defense Intelligence Agency–Missile and Space Intelligence Center, and the United States Air Force 90th IO Squadron. CORONA has the mission to provide the necessary architectural foundation of interoperability standards and common solutions that enforce these tenets, enabling the creation of efficient LVC environments for cyberspace test and experimentation.

WHY IS INTEGRATING PARTICIPANTS EXPENSIVE AND TIME-CONSUMING?

Many of the models being re-used and integrated into a cyberspace test and experimentation environment were designed to answer specific questions inside a different, non-cyberspace environment and context. The issue is not that the original engineers lacked skill, desire for their model to be maintainable, or foresight into the interoperability needs of the future. Most models are built using the latest engineering tools and approaches, requirements, and complexity at the time of inception balanced with the budget available to answer the question at hand. The simple fact is that integration issues inevitably arise when models and other systems are repurposed to answer new or emerging challenges that they were not originally designed to address. This problem becomes magnified when a repurposed model is coupled with other repurposed and non-interoperable models and capabilities in the creation of a robust environment. The result is a highly complex cyberspace test and experimentation environment that often serves a single purpose, provides minimal reuse, and must be recreated each time the same or a similar environment is needed in the future.

HOW TO BREAK A STOVEPIPE

One major point to understand about building an integrated system is complexity. Designing a system to be multi-purpose from the start by leveraging concepts such as open standards can help facilitate reuse, but oftentimes results in added system complexity. There are numerous kinds of complexity, but the two most relevant to this problem are accidental complexity and essential complexity (Brooks). Efficiencies can be achieved in integrating disparate capabilities by avoiding or removing unnecessary accidental complexity and embracing and simplifying the environment-representative essential complexity. In cyberspace T&E, there

are a number of essential pieces of complexity that must be solved. A modular solution to these complexities allows the experimenter to apply the appropriate technology to the appropriate problems. Within the CORONA Architectural Framework, there are a number of examples of modular components that solve essential complexity problems. The basic steps in the lifecycle of a cyberspace event are (1) design, (2) deploy, (3) execute and monitor, (4) analyze, and (5) sanitize. Providing common solutions throughout the cyberspace event lifecycle provides a foundation from which to build and reconfigure cyberspace test and experimentation environments more efficiently. It is this very modularity that has allowed the CORONA team to extend modules to include strong support for LVC representations of system components.

TRMC PROVIDES DOD CYBERSPACE INFRASTRUCTURE

The TRMC is uniquely positioned in DoD to work with the Components, Services, and Agencies to develop and then institutionally maintain common tools and standards on behalf of the Department. The mission of the TRMC is to ensure all DoD test Infrastructure is operated, improved, and sustained to meet current and future DoD requirements. To accomplish this mission, the TRMC utilizes its three infrastructure investment programs as well as its Congressionally-mandated infrastructure oversight requirements, promoting an enterprise approach to the development and sustainment of cyberspace infrastructure. This approach ensures that common tools and standards are utilized to the fullest extent possible to most efficiently integrate and reconfigure cyberspace test environments. CORONA provides DoD with the necessary technology maturation needed to achieve this enterprise approach.

Figure 1 depicts the DoD enterprise cyberspace infrastructure. The TRMC envisions a persistently connected joint infrastructure that links the existing open-air ranges and laboratories used to test weapon systems with cyber-focused capabilities, such as the TRMC National Cyber Range (NCR). Connecting these disparate capabilities will be possible by leveraging the existing investments in the Joint Staff Joint IO Range (JIOR) and the TRMC Joint Mission Environment Test Capability (JMETC). This enterprise approach provides the infrastructure necessary to perform cyberspace testing on weapon systems while mitigating duplication, improving efficiency and reusability, and optimizing long-range improvements and modernizations across the Department. The result is the expenditure of fewer resources while achieving more frequent and more robust cyberspace T&E.

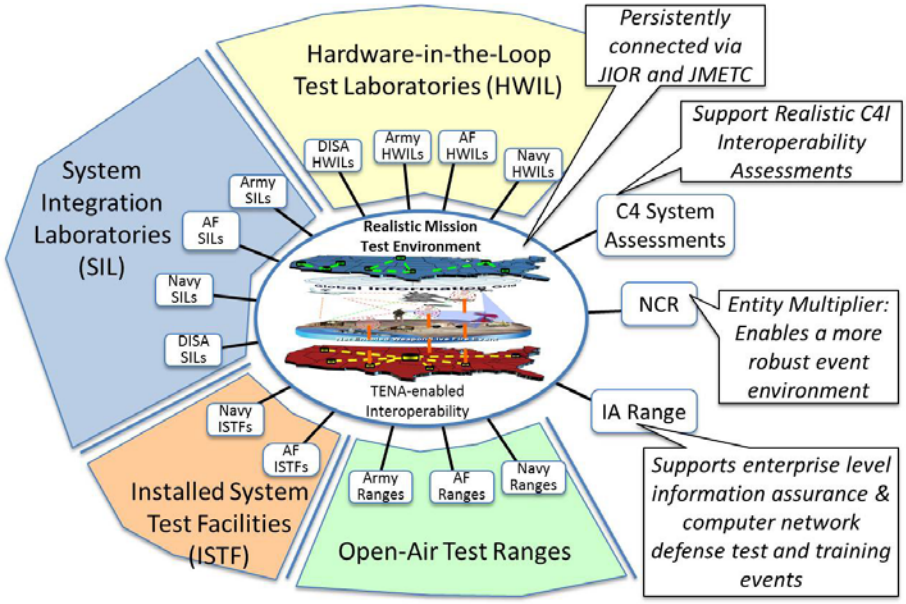

Figure 1: DoD Enterprise Cyberspace Infrastructure

WHAT IS CORONA?

In order to achieve the TRMC vision for cyberspace infrastructure, community standards and common interfaces must be developed in concert with cutting-edge technologies. This will enable the continued improvement in the fidelity and capability of our cyberspace environments without sacrificing the efficiencies needed in the creation and execution of cyberspace test and experimentation. Thus, the overall goal of CORONA is to bring the DoD, Department of Energy, and Intelligence Community together

in order to create a framework of standard interfaces and tools that support this enterprise approach to cyberspace infrastructure. Specifically, CORONA addresses four needs:

NEED	CORONA ATTRIBUTE
1. Enable standards-based interoperability	1. CORONA Architecture Framework
2. Reduce integration time for cyberspace test & experimentation	2. Standard Interfaces and data exchange mechanisms (eg. middleware)
3. Provide common tools for use DoD-wide	3. CORONA design, planning, execution, and analysis tools
4. Leverage existing investments	4. Examples: TENA, M&SCO High Level Tasks

The CORONA approach to cyberspace M&S provides a set of mechanisms and processes to enable rapid construction of a LVC cyberspace environment. This means CORONA strives to seamlessly integrate actual acquisition systems and networking equipment, emulations (real software running on different hardware), and constructive simulations. These LVC elements are used to represent the cyberspace attack, the network, and the system under test (SUT) to permit the optimum configuration. These efforts go beyond the typical cyberspace experimentation focus on network-based elements. CORONA is investigating ways of using innovative M&S techniques to discern the causal impact of specific cyberspace events on both acquisition system and overall mission effectiveness. CORONA provides the foundation for a robust LVC cyberspace environment, enabling efficient cyberspace test and experimentation, including (but not limited to) the following:

- Evaluation of cyberspace impact on weapon systems
- Rapid and cost-effective analysis of highly complex networks
- Plug-and-play support for a variety of threat and target systems
- Representation of threat and target systems with sufficient fidelity to assess the effects of cyberspace activity
- Ability to operate in federated, distributed, and stand-alone modes

WHAT IS RAPIDLY RECONFIGURABLE CYBERSPACE TEST AND EXPERIMENTATION?

Building custom test harnesses for every system is unaffordable. The propagation of cyberspace capability stovepipes is a symptom of the time-consuming and expensive issue of conducting cyberspace test and experimentation. In order to have confidence in the analysis of a system, it is desirable to have both strong guarantees from the design of the system, and a rigorous collection of supporting data. However, limited time and budget often force a lower number of samples and state-space coverage when assessing a system. Removing inhibitors to time and cost constraints helps ensure an environment where robust and thorough cyberspace test and experimentation can occur. In an environment where zero-day threats appear out of nowhere, it is imperative that the cyberspace test and experimentation infrastructure be as agile as our adversaries.

Testing agencies need reusable resources capable of testing any number of related systems. Since there are multiple systems that require examination, the test resources must be reconfigurable in a rapid manner such that testers and experimenters are spending more time analyzing the system than reconfiguring the test resources. Because of its modular approach and focus on standard interfaces, CORONA automates environment usage and reconfiguration based on requirements. Modularity and standard interfaces also enable environment configurations to shift between LVC components as experimentation needs or resource availability dictates. CORONA does not provide a universal translator for federation of LVC capabilities, but this modular approach reduces the resources required to use a specified capability.

CORONA ARCHITECTURE FRAMEWORK

CORONA was designed to improve the cyberspace test and experimentation of acquisition systems and networks. Capturing the detailed requirements and necessary components to do so in an efficient, rapidly reconfigurable manner begins with the CORONA Architecture Framework. An

architecture forms a bridge from requirements to design that defines the purpose, function, interfaces, relationships, and evolution guidelines for each system component. For CORONA, the "system" is the cyberspace test and experimentation environment. Architectures put constraints on developers in the service of achieving higher-level goals. For the cyberspace test and experimentation "system," reduced integration time and rapid reconfiguration are the higher-level goals. The CORONA Architecture Framework was built to ensure interoperability and reduce setup and sanitation times for the cyberspace infrastructure, enabling cost-effective system, and mission effectiveness assessments of cyberspace exploits on weapon systems. It also addresses a specific need to establish a common lexicon and shared understanding of the problem space and its processes. This common understanding will enable sharing of investments through the reduction of stovepipes across cyberspace test and experimentation. Fewer stovepipes will reduce integration time and allow for more efficient investments based on engineering analyses across the cyberspace infrastructure.

To design this architecture, the CORONA team surveyed as many solutions as possible to capture the essence of the problem space. The team collected as many details about the various solutions and their patterns as possible then represented the concepts in a series of Department of Defense Architecture Framework (DoDAF) and Unified Modeling Language (UML) diagrams. The diagrams were then configured to reflect the phases of the cyberspace event lifecycle. Figure 2 depicts a high-level view of CORONA. It highlights how CORONA acknowledges the need for an operationally realistic environment to seamlessly interact between a SUT, a Network Under Test (NUT), and the attack itself.

The SUT Module provides a common interface to LVC systems targeted by a cyberspace attack. The contents of the SUT Module are designed to rapidly integrate complex systems where questions about the effectiveness of a cyberspace attack that could affect the ability of the system to execute its mission exist. The NUT Module interconnects LVC network technologies with the SUT to ensure an operationally relevant environment for cyberspace test and experimentation. The application of live, virtual, or constructive networking technologies is chosen according

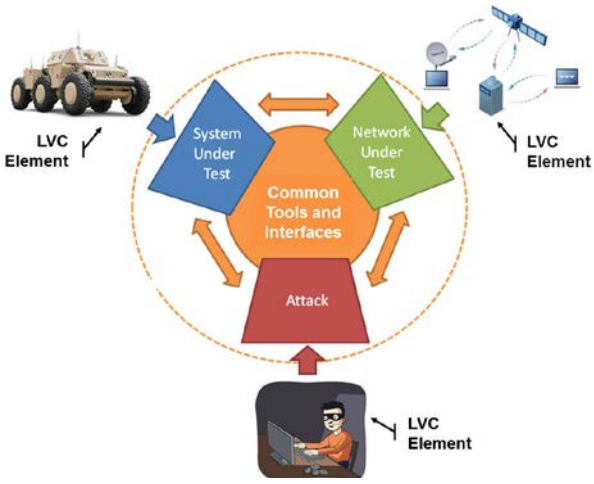

Figure 2: CORONA System Overview (SV-1)

to the fidelity required by the scenario. Current technologies include: networking equipment (such as firewalls, routers, and switches), the Common Open Research Emulator GOTS tool which is used to emulate network components, OPNET, EXata, GNS3/Dynamips, Lariat, and Breaking Point. The Attack Module provides a common process for injecting cyberspace attack tools, malicious software (malware), and cyberspace effects representative of the types of cyberspace threats of interest to the SUT and NUT. The Attack Module integrates an actual or representative threat and, to the extent possible, automates their execution within a cyberspace environment. Providing repeatable threat representation is a cornerstone of statistically sound cyber test and experimentation.

CORONA COMMON TOOLS

CORONA is also maturing critical technologies to ensure a rapidly reconfigurable and operationally realistic environment for cyberspace test and experimentation. Figure 3 depicts the tool areas where CORONA is improving technologies. CORONA has used off-the-shelf capabilities as a starting point wherever possible. Using existing solutions has allowed the research team to focus on solving new and impactful problems. Examples of off-the-shelf solutions that have been used include Emulab, VMWare, and OPNET. Upon maturation, these cyberspace technologies will be transitioned to existing TRMC investment programs to be sustained and available for use across the community.

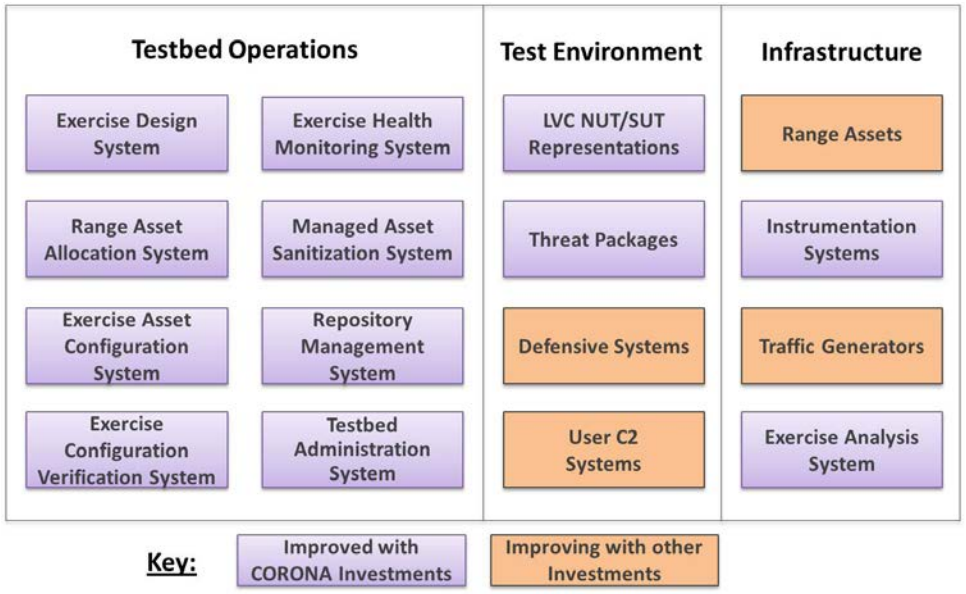

Figure 3: CORONA Architecture Framework Components and Technology Improvements

CORONA IN THE TEST AND EXPERIMENTATION PROCESS

The most intuitive way to understand the value added by CORONA is to walk through a generic cyberspace test or experiment. Figure 4 depicts the generic cyberspace test and experimentation process. CORONA has improved capabilities in each of these phases to enable a rapidly reconfigurable test or experimentation environment. Starting with the off-the-shelf capability provided by Emulab, environments create and deploy faster to a generic collection of hardware. Multiple extensions have been added to help automate time-consuming portions of the experiment. By automating multiple parts of the cyberspace experimentation process, the time to design, test, analyze, and repeat has been dramatically improved. By creating repositories of both operating system (OS) and experiment configurations, the re-usability of environments created with CORONA is improved. Reducing the time and effort needed to conduct an experiment enables more testing to occur, allowing research time to be maximized on the essence of the problem.

DESIGN

The design phase involves determining how the network and its components will be represented to support test/experiment requirements. Designing a CORONA experiment involves the following steps:

- Identifying the network and system components and the configurations, connections, and characteristics that are required to support an experiment/test
- Determining the appropriate application of LVC for each element of the experiment
- Providing a description of the network to CORONA
- Gathering and configuring required components, including live components, OS images, etc., for deployment

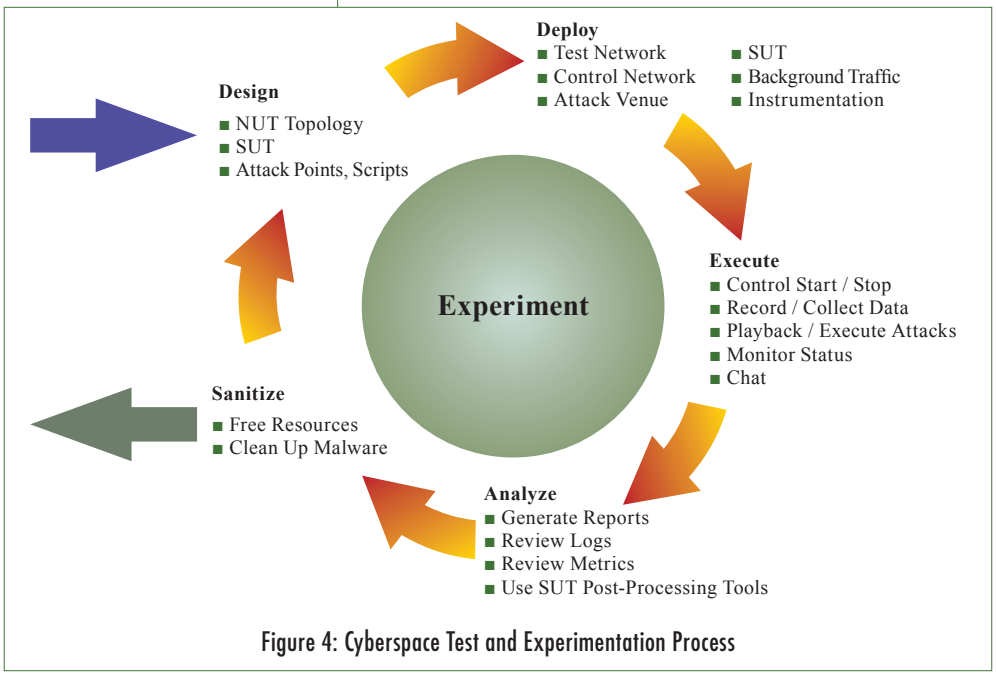

Figure 4: Cyberspace Test and Experimentation Process

Technical challenges of the design phase include (but are not limited to): complexity, re-use, abstraction from problems, instrumentation, and planning for analysis. Prior to CORONA, Emulab provided capability for defining testbed topology, assigning images to nodes within that topology, and managing constraints such as bandwidth and memory. However, adding capabilities to the Emulab repository is a resource-intensive process that required too much user interaction, particularly when setting up a fully representative environment consisting of large numbers of virtual machines. CORONA has enhanced the state of the art in experiment design by reducing the difficulty of importing custom OS images through automated scripting, thus increasing the ease of incorporating a wide variety of LVC components that can be included in a design through improvements to the deployment process. Reuse of previous components (hardware, OS images, and network description files) is encouraged, as this reduces design difficulty and enables experiment repeatability and comparison. Users need to merely point and click on previous components or environments saved in the library to use them as a starting point for their current cyberspace environment. Additionally, the ability to explicitly design live networking equipment into an experiment has been developed.

As a result of the collection of improvements, CORONA has been able to reduce the time to create cyberspace environments from weeks to days. By spending less time on design, researchers are able to spend more time focused on the problems they are trying to solve.

DEPLOY

Deployment involves pushing OS and network images and configurations specified during the design phase to experimental testbed hardware. This process creates an instance of the experiment's systems and networking environments, including the configuration of the live equipment required for the experiment and the set-up of instrumentation and data collection resources. The technical challenges of the deployment phase include delivering a mix of LVC elements to the test plane and configuring connectivity with other sites and other hardware.

Prior to CORONA, a manual mapping of a system-in-the-loop interface to a network interface was required. This manual mapping was dependent on specialized SMEs and, thus, was error-prone in large simulations and time-consuming. Conducting cyberspace experiments across a distributed environment encompassing multiple sites further complicated this mapping and oftentimes resulted in the environment being too cost prohibitive to build. Through extensions that carefully map the deployed images to specific network ports, CORONA has leveraged the off-the-shelf capability of OPNET to automate the inclusion of network simulations in these localized and distributed LVC environments. In addition, CORONA has extended Emulab to include support for large OS images, increased density of virtualization, better management of live assets, stronger security features for the control plane, and strong support for OPNET and NETWARS.

CORONA improves performance and lowers costs. CORONA automated deployment tools significantly reduce the potential for human error and provide a reduction in deployment time from days or weeks to minutes.

EXECUTE

Event execution involves launching the experiment then monitoring the status of the running nodes, including collection of experimental data to support analysis. The technical challenges of the execution phase include starting environment components, event management scripting, and non-intrusive instrumentation and monitoring. As with any test or experiment, repeatability is paramount to understanding the data collected and having the confidence to formulate a definitive conclusion. CORONA provides common mechanisms to ensure reliable and repeatable command and control of a cyberspace environment. Control of the experiment can be managed in a number of ways including using Emulab runtime control features, using an experiment manager module, or executing in an "unmanaged" mode. Different experiments may utilize the most appropriate management and execution tools depending on the requirements and the components that are part of the experiment. Typically, an experimenter will issue start commands to SUT and NUT for establishing baseline behavior, or execute cyber-attacks and apply defenses. Monitoring and data collection take place to permit later analysis, and the resulting telemetry is carefully segmented from the test data so that it does not taint the experiment.

CORONA provides essential execution management and monitoring capabilities present in Emulab, extending the state-of-the-art by providing the ability to automatically configure separate network overlays and enabling out-of-band instrumentation-sensor data collection to occur without compromising experiment isolation. Using a Sandia National Laboratories capability, LAASER (Live All-encompassing Automated Scoring and Event Reconstruction), CORONA is also extending the state-of-the-art instrumentation at the OS kernel-level, increasing our understanding of cyberspace effects. With the use of common interfaces, application programming interfaces (APIs), and control logic, CORONA manages and instruments cyberspace SUT.

ANALYZE

Analysis involves manipulating experimental data to determine cause-and-effect relationships within experiments. Some of the technical challenges of the analysis phase are collecting and storing of data, storing the test configuration, and providing repeatable analysis. Today, data analysis capabilities exist in external packages, such as in off-the-shelf tools like Wireshark. While many of these capabilities provide a means of displaying network-level events or OS-level events, none provide a direct means of correlating these events to recover a systemic picture and determine causality.

CORONA has demonstrated cutting-edge protocol analysis and event causality reconstruction through two different tools. By using LAASER to instrument at the OS kernel level, CORONA is able to use causal event reconstruction to visually examine the causal impacts of introduced cyberspace effects across the entire cyberspace environment. CORONA has also developed advanced analysis of protocols that are not natively supported in off-the-shelf protocol analyzers such as Wireshark.

CORONA enables the storing of the complete environment configuration for use during analysis or for follow-on experimentation and testing. Storing the test configuration is an important piece of responsible experimentation. Not only does it allow analysts to understand the conditions under which the data was collected well after the experiment has concluded, but it also facilitates independent verification of experimental results.

SANITIZE

Sanitization is a process of eliminating experiment data from the nodes, thus returning them to a pristine configuration. Many experiments involve fielding cyberspace threats. Failure to sanitize might leave active threats on the nodes, corrupting future experiments. Once an experiment has completed, CORONA has saved any data collection results, and the user has decided to terminate the current instance of the experiment, the process of sanitizing the infrastructure from any remnants of the experiment can begin. Emulab provides a user-settable algorithm for sanitizing hard drives in the experiment as well as rolling back network settings. This sanitization is not a complete solution; for example, changes to BIOS are not rolled back. However, some research groups, such as the TRMC NCR, have point instances of solutions that are complete and could potentially be reused by others.

CORONA technologies automate the sanitization process wherever feasible. This reduces time and effort for the current experiment while maximizing the available computing resources for other concurrent cyberspace experiments. The result is the ability to execute more cyberspace experiments with a smaller hardware footprint. Sanitization of live hardware can be complex, and as such there are several approaches to sanitization of equipment. If the equipment had an auto-generated interface to interact with the Experiment Manager, the wrapper will define the method and manage the sanitization of the equipment. If the equipment has been managed via Simple Network Management Protocol, configurations will be wiped to attempt to set the system back to a factory state. This is not a complete solution, but does represent an advance to the current capabilities.

CONCLUSION

Understanding the impacts of cyberspace effects on our national infrastructure, networks, and weapons systems is essential to protecting the United States from its adversaries. As such, and in spite of the R&D nature of CORONA, the DoD, the Department of Energy, and the Intelligence Community have already taken advantage of CORONA in a number of settings. It has been operated in both a stand-alone lab environment and in a distributed and federated

test environment over the JIOR. In these settings, CORONA has enabled a rapidly reconfigurable cyberspace test and experimentation environment, reduced the amount of time needed to design and deploy a cyberspace environment, and has enabled researchers to ask and answer questions that were previously not possible to address.

CORONA is scheduled to complete in September 2013, and at that point the architecture and critical technologies will be transitioned to the TRMC for sustainment and future use by the community. At project completion, CORONA will include cutting-edge tools and technologies, a collection of user documentation, a community-reviewed architecture, and a capability that has been shown to interoperate and extend the capabilities of other extant cyberspace range technologies. CORONA does represent the cutting edge in cyberspace range technology. However, there is still much work to be done to achieve the TRMC vision for an enterprise approach to cyberspace infrastructure. The strengths of this research and development effort will be carried forward and provide leap-ahead technology to the next generation of cyberspace testbed technology.

References

[1] Emulab Total Network Testbed. http://www.emulab.net/.

[2] University of Utah School of Computing, Flux Research Group, http://www.cs.utah.edu/flux.

[3] Frederick Brooks (1986) "No Silver Bullet—Essence and Accidents of Software Engineering," Proceedings of the IFIP Tenth World Computing Conference, 1069–1076.

[4] Christopher E. Davis, Vincent Urias, Brian P. Van Leeuwen, Information Operations Network Analysis (IONA): Final Report, SAND2011-0986P. Sandia National Laboratories, 2011.

[5] Flux Research Group, An Evaluation of Emulab Software and Its Evolution for the National Cyber Range, University of Utah School of Computing, 2009.

[6] Fabien Hermenier, Robert Ricci, "How to Build a Better Testbed: Lessons From a Decade of Network Experiments on Emulab," TridentCom, Thessalonique, France, 2012.

[7] Mike Hibler, et al., "Large-scale Virtualization in the Emulab Network Testbed," Proceedings ATC'08 USENIX 2008 Annual Technical Conference, 2008.

[8] Christopher E. Davis, et al., CORONA Functional Capabilities Document.

[9] OpenStack Open Source Cloud Computing Software, http://openstack.org.

[10] National Cyber Range, http://www.darpa.mil/Our_Work/STO/Programs?National_Cyber_range_(NCR).aspx.

[11] OPNET, http://www.opnet.com.

[12] Lee M. Rossey, "LARIAT: Lincoln Adaptable Real-time Information Assurance Testbed," Aerospace Conference Proceedings, 2002.

[13] Stephen Neville, "The Rational for Developing Larger-scale 1000+ Machine Emulation-based Research Test Beds," International Conference on Advanced Information Networking and Applications Workshops, 2009.

[14] Gil Torres, "Test & Evaluation/Science & Technology Net-Centric Systems Test (NST) Focus Area Overview," 2010.

[15] Pascale Vicat-Blanc, "Modeling Virtual Networks and Clouds," Future Networks Technologies WS ETSI, 2011.

[16] Christopher E. Davis, Lon A. Dawson, Arlo L. Ames, Theodore M. Reed, Samuel D. Olsen, Michael G. Stickland, David R. Grochocki, Nicholas D. Pattengale, PhD, Anna M. Larez, Brian P. Van Leeuwen, Cyber Operations Research and Network Analysis (CORONA) Year-1 Final Report SAND2012-5633. Sandia National Laboratories, 2012.

[17] R. Dewitt, B. Denton, J. Garrison, J. Schneider, CORONA: Year One Design & Experiment Process DIA-15-1206-002. Missile and Space Intelligence Center, 2012.

Authors' Biographies

Mr. Ryan Norman

Mr. Ryan Norman currently serves as the TRMC Lead for Army Range Oversight, providing the Army a single point of contact for the TRMC role in Test Resource Strategic Planning, T&E Budget Certification, Major Range Test Facility Base (MRTFB) oversight, and infrastructure improvements, modernization, and maintenance. He also serves as the PM for CORONA. Mr. Norman earned his B.S. in Computer Science from the Georgia Institute of Technology.

Mr. Christopher E. Davis

Mr. Christopher E. Davis is a Principal Member of the Research and Development staff at Sandia National Laboratories (SNL) and the Principal Investigator on CORONA for the Sandia team. He earned his M.S. in Computer Science from the University of New Mexico in 2005. Mr. Davis has been involved in computational economics, cognitive modeling, and cyber effects based studies while at SNL.

Evaluating the Impact of Cyber Attacks on Missions

AUTHORS

Mr. Scott Musman, Dr. Aaron Temin, Dr. Mike Tanner, Mr Richard Fox, Mr. Brian Pridemore
MITRE Corporation
McLean, VA, 22102

ABSTRACT

USING CURRENT METHODS, IT IS VIRTUALLY IMPOSSIBLE TO DETERMINE THE IMPACT OF A CYBER ATTACK ON THE ATTAINMENT OF MISSION OBJECTIVES. DO WE KNOW WHICH MISSION ELEMENTS ARE AFFECTED? CAN WE CONTINUE TO OPERATE AND FULFILL THE MISSION? SHOULD WE WAIT FOR RECOVERY? CAN WE SALVAGE PART OF THE MISSION? SINCE IT IS CURRENTLY SO DIFFICULT FOR HUMANS TO COMPREHEND THE MISSION IMPACT OF A CYBER INCIDENT, OUR ABILITY TO RESPOND IS MUCH LESS EFFECTIVE THAN IT COULD BE. WE BELIEVE THAT IMPROVED KNOWLEDGE OF THE MISSION IMPACT OF A CYBER ATTACK WILL LEAD TO IMPROVED, MORE TARGETED RESPONSES, CREATING MORE ATTACK RESISTANT SYSTEMS THAT CAN OPERATE THROUGH CYBER ATTACKS.

Our work addresses the "mission" part of "mission assurance," focusing on cyber mission impact assessment (CMIA). Our challenge is to create mission models that can link information technology (IT) capabilities to an organization's business processes associated with Measures of Effectiveness and Performance (e.g., attrition of enemy forces, targets destroyed, blue force protection). Measuring mission impact requires knowing the mission activities that fulfill mission needs, the supporting cyber assets, and understanding how the effects of an attack change mission capability. This paper is about developing the techniques that make estimating the mission impact of cyber attacks possible.

INTRODUCTION

Increased integration of computers and IT into the war fighting process has created an environment where compromise, damage, or loss of IT assets can result in mission failure. Thus, our expectations of the success of a mission that is under cyber attack (i.e., attacks against the IT supporting a mission) greatly depend on the understanding of how the cyber attack has degraded capabilities in kinetic (non-IT) space. This report on research in progress describes a system that evaluates the effect of a cyber attack by predicting the impact of the attack on the mission's measures of effectiveness (MOE).

Consider the following example. A time sensitive targeting (TST) mission thread is being executed. The mission commander's ability to select a weapon to deploy against a target depends on information about available airborne weapons and ground-based weapons. Either type of weapon might be useful depending on the type of target. At 1130 hours, two events occur:

- The TST cell is unable to access airborne weapon data for unknown reasons
- The network operations center supporting the TST cell has a report of a denial of service (DoS) attack on several routers, disrupting network traffic; there is no estimate of how long the effect of the attack will last

Currently, the mission commander only knows that there is no access to some of the data needed. The best he can do is to proceed with the data to which he has access, which means planning an attack using a ground-based weapon, even if

Musman Scott et al, (2010) Evaluating the Impact of Cyber Attacks on Missions, in The Proceedings of the 8th International Conference on Information Warfare and Security, Edited by Leigh Armistead, ACL, Reading, UK, 446-458.

an airborne weapon would improve the mission's chances of success. At the same time, the IT administrators know there is a cyber attack that is stopping data from moving over the network, but don't really know which mission systems and missions rely on the routers under attack. The IT administrators are unable to tell the mission commander what he needs to know to figure out his options.

We propose that information about the DoS attack be provided as input to a model of the mission and its supporting IT assets. The model infers that the routers under attack are necessary for transmitting the airborne asset status to the TST cell, confirming the connection between the two events. Further, the model calculates the change in the measures of mission success as the duration of the attack extends, and provides the mission commander with the assessment that he can choose to wait 10 minutes for the attack to be cleared without reducing the likelihood of mission success; and if at that point the attack can be cleared within another 10 minutes, he should wait for connectivity to be restored, otherwise he should continue the mission with just the ground-based weapons information.

PREVIOUS WORK

We currently have very little capability to estimate the mission impact of cyber incidents. The state of the art is such that even the most basic mapping of dependencies among mission objectives, mission activities, and IT assets rarely exists. Even when these mappings are determined as part of risk analysis, they are not carried over into use operationally when incidents occur.

The thesis of Fortson [2007] highlights a number of deficiencies of current practice, describes a number of scenarios illustrating operational deficiencies, and provides requirements for an impact assessment solution. Although not phrased in the following manner, the various examples highlight the objectives for mission impact assessment:

1. Make it possible to document the dependency relationships between cyber assets, mission activities, and mission objectives so that the relationships can be used operationally.
2. Make it possible to determine the mission impact of the cyber attack based on the timing and duration of the incident.
3. Make it possible to predict mission impact, even if an affected IT resource is not currently in use.
4. Make it possible to predict the impact on mission instances that are planned or anticipated in the future.

These objectives impart requirements and restrictions on appropriate techniques for a solution. For example, understanding the relationship between incident duration and impact requires that time versus mission value knowledge about activities and data be captured in mission models. These temporal mission system characteristics are rarely considered or documented. Popular architectural notations such as Unified Modeling Language (UML) or Department of Defense Architechure Framework (DoDAF) do not include these aspects in their descriptions of the mission.

Existing practices in modeling mission systems are inadequate for our intended purpose. Some existing modeling approaches (e.g., UML, DoDAF) are diagrammatic rather than computable. Some modeling paradigms lack the ability to represent time, or workflows (e.g., Bayesian networks, Influence diagrams, dependency maps), which is important since the duration of an incident will often affect the amount of impact an incident will have. Critically, many approaches are also unable to represent information dependencies, a necessity since information attacks are common in the cyber domain.

Although there are existing tools for performing cyber risk assessments [Watters, web][Whiteman, 2008], the mission models that are created and used in these tools have limited use for computing online impact assessments. Because formal cyber risk assessments are currently an offline process, they focus on the potential cyber effects against a wide variety of possible mission instances, where the specific timing and duration of the attack effect is not specified. As a result, risk assessment mission models tend to lack, for example, timing and workflow information which make it impossible for them to differentiate between attacks that can be recovered from quickly and attacks that would take much longer to recover from. Since many missions are dynamic and have temporal constraints the added details that we would include in our mission models (e.g., activity timing, workflow, and MOE mappings) will allow us to make additional mission impact assessments that are not possible with a more static model.

Existing DoD processes label systems and information as mission critical that are then considered to be mission critical for all time. The reality is that systems and information can be more or less important depending on the time, or phase of a mission. Knowing which systems and information are important to the mission at the time of an incident can help to focus recovery activity and speed up the recovery process. Atemporal representations of missions cannot accommodate these requirements.

Some related work has focused on battle damage assessment (BDA). Although BDA is an integral part of the military process, as of yet there is no standardized BDA process for IT effects [Thiem 2005]. There is an important distinction between BDA and mission impact assessment (MIA). BDA assesses the damage associated with an attack on the resources, while MIA assesses the anticipated effectiveness of the mission resources to carry out the mission after an attack has occurred. In this context we are equating MIA with combat assessment (as defined in JP-102, 2006). Grimaila and Fortson [2007] focus mainly on the BDA processes, rather than the impact assessment process.

Since an important characteristic of impact assessment is its temporal nature, including more than just knowing the current capabilities of the IT and mission activities immediately following an attack, it is sometimes necessary to be able to make predictions; therefore, effective impact assessment involves understanding anticipated activity. Whether it is scheduled, or based on historical expectations, anticipated activity indicates what is likely to be lost in the face of failure or degradation. It is also worth considering that, depending on where and how your mission systems are instrumented, you may only be able to observe indirect effects of an attack, and so in some circumstances the observed lack of expected activity may be the first opportunity to notice that there is a problem that threatens the mission objectives.

There is a large body of existing work, tools and techniques that address mission modeling [Clancy et al. 1998]. Emerging standards such as Business Process Modeling Notation (BPMN) [White and Miers, 2008], and the integration of the modeling notation with executable simulation engines [Anupindi 2005], provide methods to describe a business process as an executable model that can then be used to predict various mission specific metrics and measure various performance characteristics given architectural decisions.

For CMIA we consider the possible effects of cyber attacks, as would be reported by a BDA process. Existing cyber attack effect models such as those discussed by [Howard 1998] are less suitable for our needs. Howard's incident taxonomy is information centric, and hence does not include the process oriented characteristics needed to compute the impact of activity interruption, degradation, fabrication, or information unavailability. Although not focused on mission relevance, Blyth and Kovacich [2006] describe effects that come closest to addressing our needs.

TECHNICAL APPROACH

Our technical approach involves dividing the problem into several parts. First, we discuss the requirements for modeling missions. Next, we show how we have reduced the number of cyber attack scenarios for us to consider for making impact calculations down to only six classes describing the effects on IT of any cyber attack. We then discuss how we express knowledge of the mission activities and the supporting IT in BPMN and use that to compute MOE for a mission instance.

Requirements for Modeling Missions

To understand the characteristics of mission systems, we reviewed a variety of mission systems—including advanced sensor networks; time critical targeting; Joint Surveillance Target Attack Radar System (JSTARS); the Federal Aviation Administration (FAA) enroute automation system; a census address canvassing system; and several others. The result of this review was a list of modeling requirements for how the expressiveness of the mission model affects our ability to compute mission impact (see Figure 1).

In order to understand how to compute mission impact it is necessary to understand what impact is and how it might be reported. Since impact assessment is concerned with changes in the expected outcome of a mission, the types of impacts can vary. Consider the following examples that illustrate a variety of mission impact assessments:

- We can no longer determine which ground weapons are available
- The mission system is now operating at only 70% capacity
- We can only hit 50% of the high value targets
- Target #356 can no longer be engaged
- Our planned engagement of target #4557 is unaffected by the cyber attack

Dependencies Between Mission Elements

- Allows us to relate between Mission Objectives, activities, cyber assets, and information assets

Workflows

- Makes it possible to represent ordered interdependencies and forecast the impact of resources not currently in use

Uncertainty

- Allows us to represent the relative likelihood of events and outcomes

Utility

- Represents the value estimates of different mission outcomes, since they may not all be equal

Time Value Characteristics of Activities and Information

- Makes it possible to represent time constraints for activities and information, and predict how the duration of an incident changes its impact

Fallback and Failover Activities

- Represents what kicks in, in the face of failures

Implicit Mission Decisions

- Allows us to capture when certain mission outcomes depend on "built-in" decisions that can change when information is no longer available

Mission MOEs/MOPs

- We can't evaluate what we can't measure

Scenario Characteristics

- Sometimes the impact of an incident depends on the context of how/where the system is being used

Figure 1: Modeling Requirements

- There will not be any impact to the mission if we can recover from the cyber attack within the next 15 minutes
- Because we cannot restore the server till tomorrow, tonight's planned mission will be affected

These impact statements represent different types of impacts on a mission system but are not mutually exclusive. In general, impact statements might be in terms of:

a) ability to perform mission activities

b) capabilities of the mission system in general

c) achieving specific mission objectives

d) information about specific mission instances

e) prediction of how mission impact might vary over time

f) prediction of how affected resources not currently in use may cause future impact

g) prediction of how affected resources may cause impact on future mission instances

The fact that a mission impact assessment might involve any of these statements illustrates the complexity of the problem of selecting a technical approach to compute it. It would seem necessary to either select a general purpose approach that can compute these different statements, or to pick a subset of these impact statement types that is "good enough" to provide operational value. In either case, we still want only a single mission model over which to compute these impacts. Thus the mission model must be descriptive enough to support the different calculations, whether they are temporal, probabilistic, or value based.

Representing Cyber Attacks

Although various languages exist that can be used to describe cyber incidents (e.g., Intrusion Detection Messege Exchange Format (IDMEF), Common Event Expression (CEE)), these languages characterize incidents in terms of the activities of the attack (e.g., a rootkit attack modifies a system library file; a buffer overflow allows a user privilege escalation). What is needed for impact assessment is a standardized way to characterize the *effects* of cyber incidents, and as of yet no such language exists. As a step to address this deficiency we developed categorical descriptions of cyber attack effects (Figure 2). Interruption, interception, modification, and fabrication were in Blyth and Kovacich; the others we added based on our examination of the mission assurance domain.

Degradation

- An attacker causes a degradation in the performance of an information asset

Interruption

- An attacker causes an information asset of the system to become unusable, unavailable, or lost for some period of time

Modification

- An attacker causes a modification of information, data, protocol, or software

Fabrication

- An attacker causes information to be inserted into the system

Unauthorized Use

- An attacker uses the system resources for their own purposes

Interception

- An attacker causes or takes advantage of information leaked from the system

Figure 2: Cyber Attack Effects

Regardless of the mechanism used in a cyber attack, we believe that its effect can be characterized as being one or more of the listed effects on one or more of the mission IT assets (including both IT components and information assets). Although our characterization of attack effects is not a formal language, when combined with information about which resources are affected and estimates of start and end times for the incident, these categorizations provide enough information to allow us to compute impact, and provide the basis for the rest of the work we have done on impact estimation.

Modeling Missions for CMIA

A challenge of cyber mission impact assessment is relating the needs of the mission to the IT that support it, and capturing these relationships in a mission model. We view a mission as being a collection of activities that must be performed to accomplish a task. The activities are accomplished using mission resources, some of which are human, some might be mechanical, and some are IT. Associated with these activities, various types of information are exchanged, created, or used. The specific information involved is typically described as an information asset, where information assets are assigned to resources, some of which are IT.

Based on analysis of model representation versus impact computation tradeoffs we selected BPMN, along with some proposed extensions to represent information dependencies, as the formalism in which to represent mission systems. BPMN is an emerging standard for process engineering, so significant modeling expertise is available. There are Commercial Off The Shelf (COTS) products that connect BPMN models to executable simulation engines that support offline performance analysis that is similar enough to some of the impact calculations we need to perform.

Figure 3 illustrates a top-level mission model that, when used in a simulation (e.g., iGraphx software), allows us to

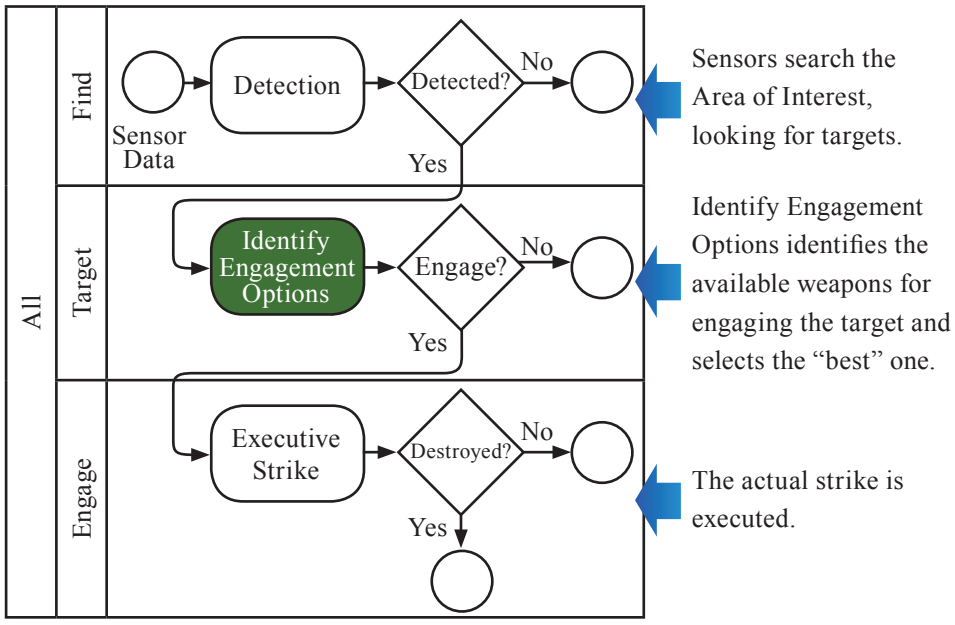

Figure 3: A top-level TST (like) mission model in iGraphx that can compute mission MOEs

modify various mission system characteristics (e.g., add or remove sensors, perform activities faster) and compute the effect of these changes on simulated mission outcomes (MOEs).

This model represents a performance engineering model, in this case for the domain of TST that may already exist for the domain of the mission system for which we are trying to perform CMIA. Typically missing in existing models that represent mission systems are the IT resource dependencies and the information dependencies.

As illustrated in figure 4, the information used to populate the IT portion of the model is derived from several sources. A network diagram usually exists that inventories the network hardware and describes how it is interconnected. Information from network audits and vulnerability testing can also populate this information, as well as identify the software applications that run on the hardware. At the software level, we want to identify algorithmic or configuration items that affect the workflow, such as data caching or flows decision made by the software algorithms.

with each activity. Also not shown are various modeling parameters associated with activities that identify the timing and decision points that might affect the mission MOE calculations. By explicitly adding the IT related activities into the model, any changes to the capabilities of the IT resources to reflect the effects of a cyber attack can now change the outcomes of running the model. This particular model includes parallel activities to access information about air and ground weapons assets, and also includes a representation of software caching that makes access to remote information unnecessary if recent status information is available locally. Backup and failover activities can also be represented.

The ability to represent information asset dependencies is missing in almost all mission model representations. Existing workflow modeling approaches, such as BPMN, do not include acceptable methods to represent information to activity dependencies in computational form. Such dependencies are typically represented only graphically. Since cyber attacks include data attacks that affect integrity or confidentiality, we want to represent how each modeled

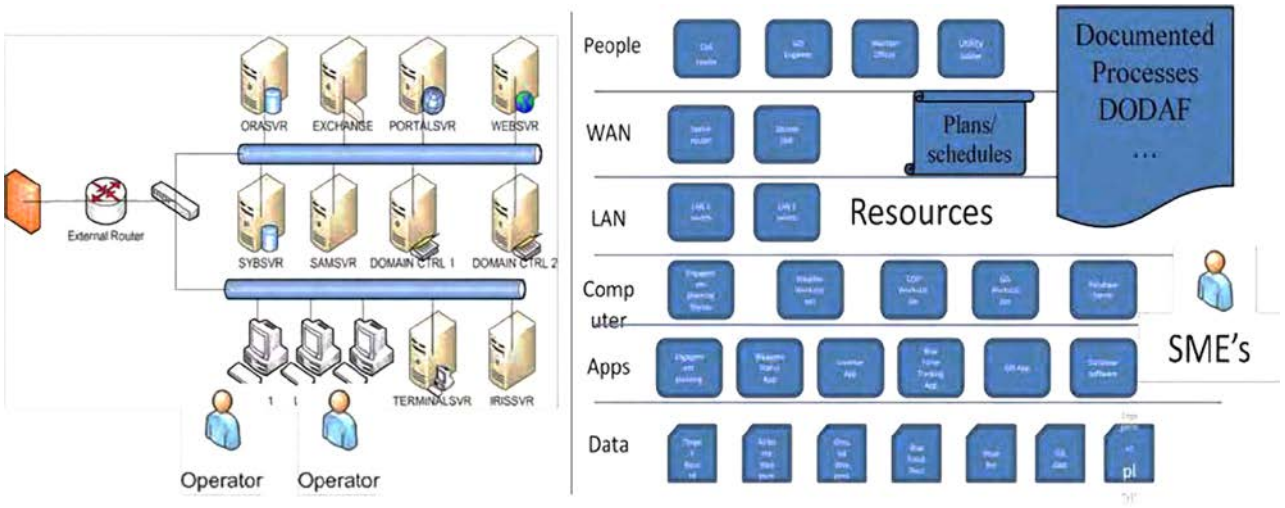

Figure 4: Information sources for representing IT include network diagrams, resource inventories, plans/schedules, architectural documentation, and subject matter experts

Figure 5 illustrates an example of the details found in the sub-model for the "identify engagement options" activity of figure 3. This model fragment shows how the mission workflow has been expanded to include activities for the IT resources. Although not illustrated in the diagram, modeled resources mapped to IT assets are associated

activity depends on these information assets. Moreover, we want to do it in a way that allows us to compute the resulting impact on MOEs when the integrity or confidentiality constraints of information assets are violated. These information dependencies are shown in figure 6.

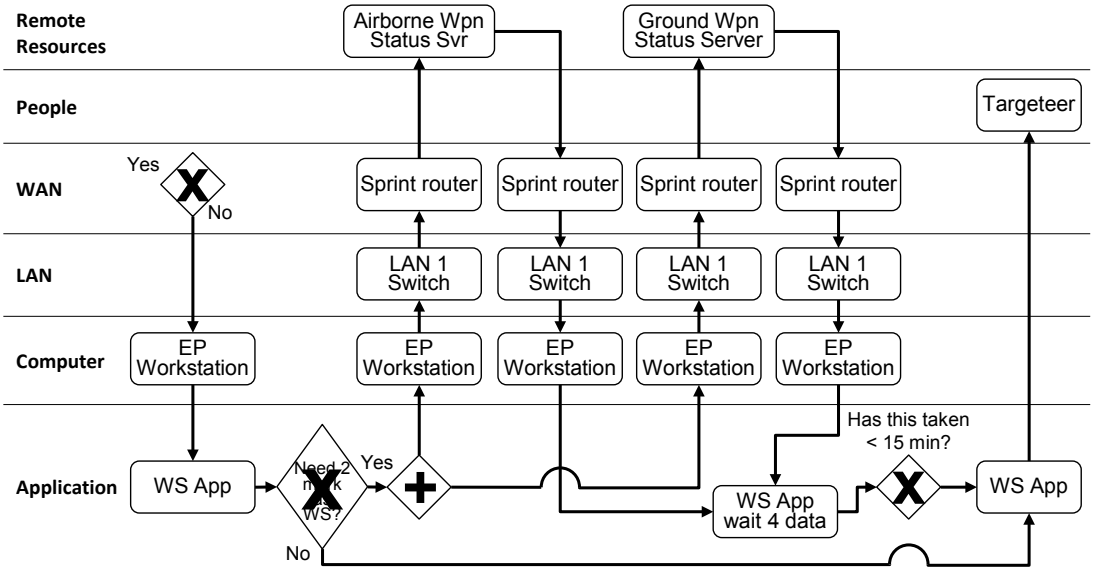

Figure 5: Part of an IT activity model for assessing the available weapons assets

To address this modeling deficiency we have proposed some extensions to the BPMN models to allow us to explicitly represent the constraints in a computable form. By defining information assets as resources, activities that use these information asset resources can be defined in the model. Since it is possible to define attributes (variables) for resources, we will define attributes for integrity and confidentiality for all of our information asset resources. If activities are then performed using information assets whose integrity or confidentiality constraints have been violated, we can have the model implement mathematical functions that would alter the MOE calculations.

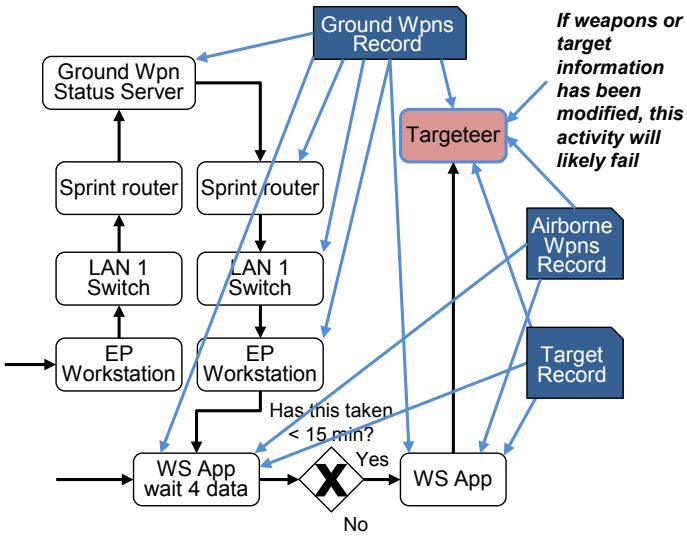

Figure 6: Information dependencies associated the IT activities

Computing Cyber Mission Impact

To estimate mission capability we apply computational algorithms to a mission model in a manner that allows us to link system capability to mission-oriented MOEs. Using our approach, when a cyber attack occurs, we envisage that an incident report would provide details of the effect on IT resources. We use that information to modify the mission model to reflect changes in system capabilities caused by the cyber attack. Then we rerun the model to produce new MOE estimates. This is illustrated in figure 7. The impact of the attack can then be determined by comparing the two MOE values (before and as a result of the incident).

Our method currently requires manual intervention to alter the mission model to reflect the cyber effect of the incident, and repeated runs of the simulation to reflect the normal variations in mission instances. Below we illustrate an example of computing mission impact for a specific incident.

Since our objective is to implement a solution that can be run on-line and produce mission impact estimates

as incidents occur, our current manual intervention approach is an unacceptable solution. Additionally, simulation as a computational strategy to compute impact is not an ideal solution for producing timely impact estimates. Fortunately, we are aware of several alternatives, and are exploring techniques to transform (or compile) our mission model into constraint models, decision trees, or schedule representations that would be amenable to much more efficient run-time evaluation.

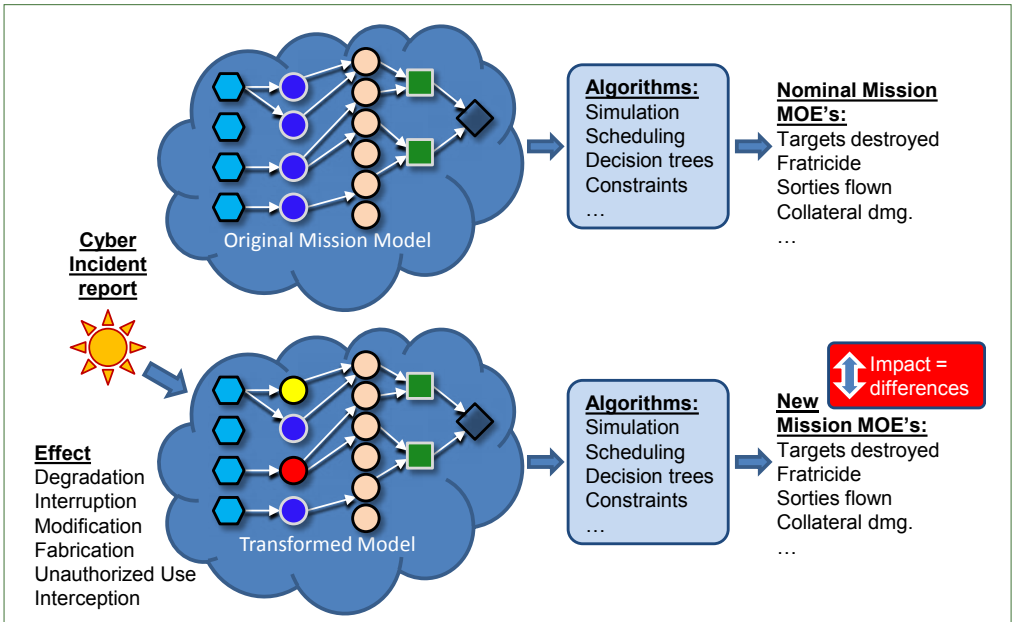

Figure 7: Estimating mission impact by comparing model MOE's with and without the effects of the cyber attack

Since there are currently no standardized processes for characterizing and reporting cyber incidents to a system such as the one we are developing, we are also working on how to use our approach offline to evaluate the cyber mission assurance properties of mission systems. Traditional approaches to cyber risk analysis are capable of identifying high risk components, but say very little about which specific threats will have the most impact, how the timing of attacks affects impact, or what to do when an attack occurs. Our techniques might be used to pre-compute a playbook of response options and actions in the face of different cyber attacks.

A cyber incident forces mission personnel into decisions that relate to the executing mission. There are a finite number of alternatives that we need to compute to be able to assist mission operators in making a decision:

- Whether to continue with the mission using the affected IT resources (if possible)
- Whether to continue with the mission and not use the affected IT resources (if possible)
- Whether to continue with the mission after having recovered the affected resources
- Whether to abandon the mission

AN EXAMPLE OF COMPUTING MISSION IMPACT

Consider the following incident:

"1130 hours: An inability to access AWACS or AOCC (both of which can provide information about available airborne weapons) coincides with a network DoS reported on several GIG routers. There is currently no way to know how long the DoS attack will last."

This incident is one where access to a source of weapons information is made unavailable, as shown in figure 8. Since the sources of weapons are independent of each other for any given target, there is some likelihood that there may be ground weapons available to engage the target, and there is a different likelihood that airborne weapons might be available. Some weapons are more suited than others to the particular type of target that is being engaged. Our mission model represents our characterization of how these various factors affect mission outcome.

Since the mission thread can proceed using only the information about available ground weapons, the mission level decision posed to mission personnel is to try to understand: (1) whether they are going to be better off continuing with the mission using only the partial weapons availability information, (2) whether to hold off in proceeding with the mission until after the missing information about available

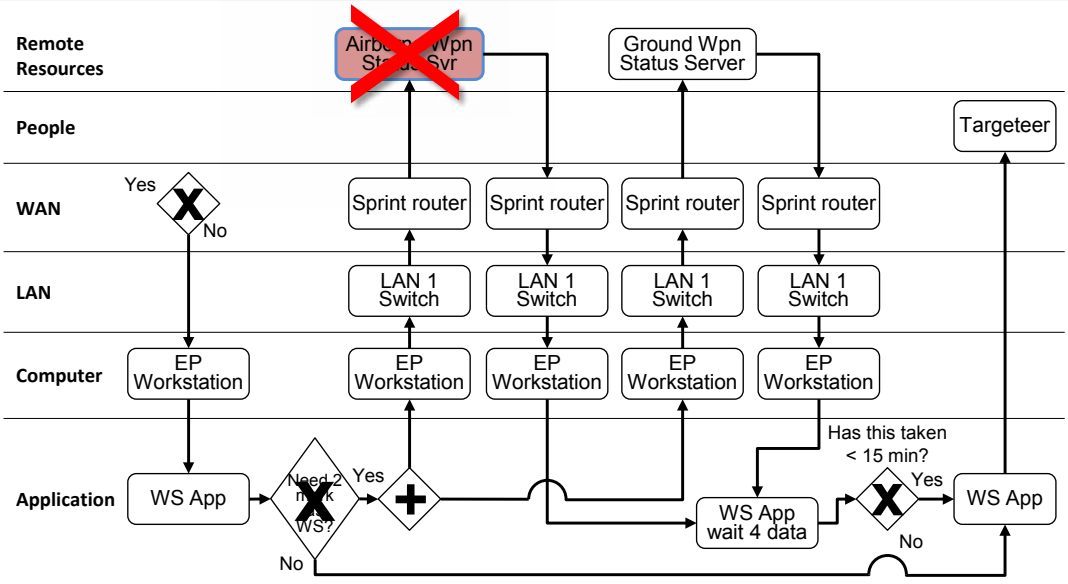

Figure 8: Access to remote mission information becomes unavailable due to an attack

weapons becomes available, or (3) whether to abandon the mission instance because of the incident.

Our mission model makes estimating the impact of these options possible. Figure 9 illustrates estimating a mission MOE for the various decision cases.

The green line in the figure illustrates the model estimated impact variation over time when waiting for recovery from the incident to access the airborne weapons status data. Since there would be a delay in proceeding with the mission till recovery takes place, the curve computed by the model reflects the fact that less time to prosecute a time-sensitive target leads to less chance of mission success. The red circle in the figure on the vertical axis illustrates the reduced chance of mission success if the mission was to continue immediately, using only the ground weapons known to be available. The red line in the figure illustrates the temporal characteristics of holding off acting on the partial weapons information. Although displaying results in this form is not ultimately the way we want to present this information to an end-user, these curves can be the basis of advice to mission personnel. These curves indicate to us (as technical professionals) that in this situation the mission personnel can afford to wait 10 minutes to see if the denial of service ends, and suffer no additional impact if they then proceed with the information they currently have now. It also indicates that if they believe the incident can be recovered within 20 minutes, obtaining additional weapons options, then the likelihood of mission success would increase over the options they have right now.

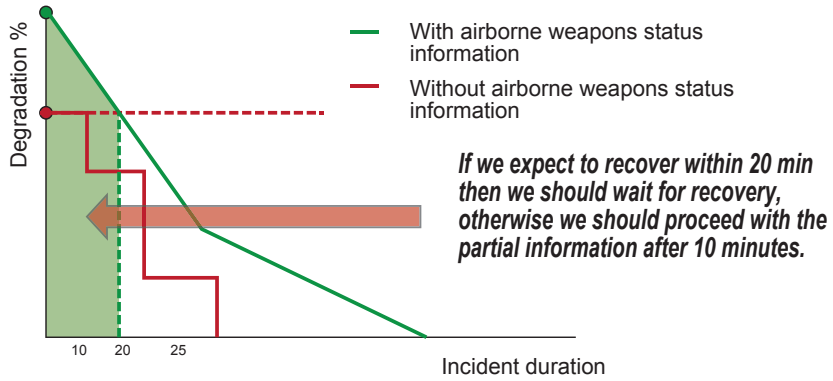

Figure 9: Impact curves and conclusion for losing access to airborne weapons status

This example of estimating mission impact illustrates the computations we can now make with our mission model when a cyber event occurs, and illustrates putting the results of those calculations in a mission context. The result helps to inform mission personnel in making operational decisions about what to do as a result of the cyber attack.

SUMMARY

We have demonstrated how one can compute the mission impact of cyber attacks and shown how the outcomes of the impact estimates provide mission personnel information relevant to mission level decisions. The models shown in figures 3 and 5 produce the graph in figure 9, which describes the complete impact of the example incident. We have not addressed the question of how to present this information to mission operators, although we are fairly sure that the graph shown is not the presentation we would like to use.

Our work on characterizing cyber attack effects is pertinent to all related activities that need to report cyber incidents. The "DIMFUI" effects (see Figure 2) at least notionally provide a set of output statements for a cyber BDA process. With attacks characterized in this way, a number of mission-level assessments can be supported, one of which is the mission impact described in this paper.

Our analysis for understanding what to include in mission models provides a set of requirements for the documentation and characterizing of mission systems in order to be able to do mission impact assessments (Figure 1). It is important to note that these things are necessary for assessing mission impact of cyber events, or any mission resource setbacks, irrespective of if there is a mission model to support automated assessment.

This paper describes research in progress, and our work continues on developing dedicated software that can do the calculations that we have so far demonstrated by making manual changes to the models.

REFERENCES

Air Force Operational Test and Evaluation Center (AFOTEC/XRC). (1995). AFOTECH 99-101, *Test Concept Handbook*, Jan 95. Kirtland AFB, NM.

USAF (USAF/TEP). (1994). AFI 99-103, *Test and evaluation process*, 25 Jul 94. Washington, DC.

Anupindi, R. "Managing Business Process Flows: Principles of Operations Management," 2005, Prentice Hall, ISBN 0131676865.

Blyth A., Kovacich G., *"Information Assurance (security in the information environment),"* 2nd edition, 2006. Springer-Verlag Ltd. London.

Clancey, W. J., Sachs, P., et al. Brahms: *"Simulating practice for work systems design,"* Int. J. Human-Computer Studies, 49: 831-865, 1998.

DeMarco, T. "Controlling Software Projects: Management, Measurement, and Estimates," Prentice Hall, 1982 (ISBN 0-13-171711-1).

Fortson L. "Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology," AFIT Masters Thesis, March 2007.

Grimalia M., Fortson L. *"Towards an Information Asset-Based Defensive Cyber Damage Assessment Process,"* Proceedings IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007), 2007.

Howard, J., Longstaff, T. *"A Common Language For Computer Security Incidents,"* Sandia National Laboratories, Sandia Report, SAND98-8667 1998.

Lane, N.E. (1986). Issues in performance measurement for military aviation with application to air combat maneuvering (NTSC TR-86-008). Orlando, FL: Essex Corporation.

Theim, L. "A Study to Determine Damage Assessment Methods or Models on Air Force Networks," Department of Engineering and Management, Air Force Institute of Technology, Wright Patterson Air Force Base, OH., 2005.

TST, *"MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR TARGETING TIME-SENSITIVE TARGETS,"* 2004, FM 3-60.1, MCRP 3-16D, NTTP 3-60.1, AFTTP(I) 3-2.3.

Watters, J., *"RiskMAP — Tool for building a business case for investing in security*," Web, http://www.thei3p.org/publications/.

White, S., Miers, D. *"BPMN Modeling and Reference Guide*." Future Strategies Inc. 2008, ISBN 978-0-9777-5272-0.

Whiteman, B. *"Network Risk Assessment Tool (NRAT),"* IA newsletter, Vol 1, Spring 2008, http://iac.dtic.mil/iatac/download/Vol11_No1.pdf.

Authors' Biographies

Mr. Scott Musman

Scott Musman has a B.Sc.(Hon) in Engineering from the University of Sussex in the U.K. and a M.Sc. in Computer Science from Johns Hopkins University. In addition to working in other domains that usually involve complex decision making in uncertain environments, he has been working cyber security problems since the mid 1990's, acting as Director of R&D for Integrated Management Services Inc., head of Enterprise Security Research for Alphatech/BAE Systems-AIT, and as a Principal Engineer for the MITRE Corporation.

Dr. Aaron Temin, CISSP-ISSAP

Aaron Temin, PhD, CISSP-ISSAP, is a lead cyber security researcher at the MITRE Corporation. His current interests are mission assurance, adversary modeling, and software security. He received a doctorate in computer science from the University of Texas at Austin and a Bachelor of Arts in applied mathematics from Harvard University. He is a member of AAAI, ACM, IEEE, ISSA, and USENIX.

Dr. Mike Tanner

Mike Tanner is a lead artificial intelligence engineer at the MITRE Corporation. His research interests are in automated planning, plan recognition, and abductive reasoning. He has a PhD in computer science from Ohio State University.

Mr. Richard W. Fox

Richard W. Fox (now retired to golf, motorcycles, and photography) was the Principal Systems Architect for MITRE Corporation in Suffolk, VA, when this article was written. Mr. Fox designed multiple large-scale systems for the FAA, HUD, IRS, commercial airlines, the Air Force, the Army, Lockheed Martin, and AT&T. At MITRE Corporation, Mr. Fox provided large-scale systems engineering and analysis to Joint Forces Command, TRADOC, and other MITRE Corporation customers. A retired Army Colonel, he received his M.S. in Computer Science from Kansas State University. His current email is stcfox@gmail.com.

Mr. Brian Pridemore

Brian Pridemore supports Modeling and Simulation efforts and has been working on Mission Level Modeling (MLM) to identify and exploit areas for process improvement and information sharing strategies. His range of mission thread modeling, simulation, and analysis (MS&A) projects include using mission thread modeling to support operational requirements decomposition and analysis and process engineering analysis for a Joint NetOps (JNO) Functional Solutions Analysis (FSA); 4-D trajectory modeling simulations of the air traffic control (ATC) system for the Federal Aviation Administration (FAA) and in Europe, exploring advanced control concepts for the future; simulations-of-simulations projects for integrating multiple ATC simulations for prototyping advanced ATC Controller Training with Voice synthesis/recognition; simulations for the U.S. Office of Border Patrol to analyze impacts of tactical infrastructure, technical improvements, and personnel on the Border Patrol mission; and the Strike Cell federation for training and concept analysis. Mr. Pridemore received a double major with a Bachelor of Science in Mathematics and Computer Science from Ohio University and a Master of Science in Systems Engineering from Johns Hopkins University.

Synthetic Cyber Environments for Training and Exercising Cyberspace Operations

AUTHORS

Stephanie D. Harwell & Christopher M. Gore
Camber Corporation
O'Fallon, IL 62269
sharwell@camber.com, chgore@camber.com

ABSTRACT

TO COMBAT THE CYBERSPACE THREAT FACING THE NATION, AN INTEGRATED COMBINATION OF TECHNOLOGY, EDUCATION, TRAINING, AND EXERCISE IS NEEDED. THE AIR FORCE CYBER SIMULATOR JOURNEY BEGAN IN 2001 WITH A SMALL EXERCISE. TODAY, SYNTHETIC LIVE ENVIRONMENTS (CYBER SIMULATORS) ARE IN USE FOR TRAINING AND EXERCISES, MISSION REHEARSAL, AND TOOL DEVELOPMENT FOR CYBERSPACE OPERATIONS. THE AIR FORCE HAS 78 SIMULATORS AT 3 LOCATIONS IN ILLINOIS, MISSISSIPPI, AND FLORIDA. SOLUTIONS SIMILAR TO THE AIR FORCE ARE ALSO IN USE BY THE NAVY (NAVY CYBER OPERATIONS RANGE (NCOR)) IN NORFOLK; UNITED STATES STRATEGIC COMMAND (STRATCOM), STRATCOM CYBER OPERATIONS RANGE (SCOR) IN NEBRASKA; AND THE NATIONAL GUARD, ARMY GUARD ENTERPRISE NETWORK TRAINING SIMULATOR (ARGENTS) IN ARKANSAS AND SEVEN OTHER STATES. IN ALL, THERE ARE OVER 100 ACTIVE SIMULATORS IN THE UNITED STATES. EVOLVING OVER TIME, THE REQUIREMENTS OF THE CYBER SIMULATOR HAVE GROWN FROM JUST REPLICATING THE OPERATIONAL DAY-TO-DAY ENVIRONMENT OF THE BLUE FORCE TO MODELING THE ENVIRONMENT OF THE RED THREAT. THE ENVIRONMENT NOW ENCOMPASSES A WORLD-WIDE ROUTABLE GRAY SPACE AND IS INTEROPERABLE WITH OTHER SYNTHETIC ENVIRONMENTS.

Cyber simulators expose operators to various network situations and threats and advance their technical skills. They are used in validating solutions and the development of innovative approaches enhancing operational competencies. The risk-free environment of a cyber-simulator and scenario based stimuli allow crews to experience and conduct aggressive activities to: disrupt, obstruct, and destroy the integrity of the network; infiltrate a simulated computer network for intelligence collection; and train on procedures and tactics to defend and protect the network. Fidelity and realism throughout the physical and virtualized platform, appliances, and applications is paramount and must also be present in traffic generation, data, and the synthetic internet. While these key factors are critical to an immersive experience, the simulator must be constructed within a rapidly reconstitutable environment with the capability to start, stop, and re-roll scenarios from a requisite state.

INTRODUCTION

So how do you model or simulate cyberspace? Is the realm of cyber a venue for modeling and simulation? When taken to its root form, it is using a network of computers to model a network of computers. Adding to that, it is using virtualization and compression to simulate an environment that is already virtualized and compressed. For the cyber arena, the purpose of the model or simulator drives the composition.

I/ITSEC 2012, paper number 12408, *Synthetic Cyber Environment for Training and Exercising Cyberspace Operations.*

For the Air Force, the purpose of the cyber simulator is to:

- Assess and train defensive and offensive forces to decisively operate in cyberspace
- Develop, validate and train rigorous, relevant and standardized cyber tactics and Command and Control (C2) procedures
- Evaluate and refine information dissemination, Indicators and Warnings (I&W), and synchronization of U.S. computer network operations
- Determine effectiveness and priority areas to refine cyber readiness and mitigate the full spectrum of rapidly-evolving threats and vulnerabilities
- Provide simulator-based education, training, crew certification, mission rehearsal and exercise capabilities at the individual, crew position, unit and Air Force levels to ultimately increase Air Force cyber operations effectiveness

The Air Force Cyber modeling and simulation objectives are:

- Provide realistic threat emulation
- Be interoperable with Modeling and Simulation (M&S) live-virtual-constructive environments
- Create a simulated environment to exercise fighting through a cyber attack
- Adapt to current threats (0-day)

The overall goal is *to provide the best training to the Cyber Network Ops community.*

The term cyberspace conjures up a vast virtual electronic universe that is increasingly becoming the center of our ability to exist in a modern world. The term denotes the internet – an interwoven world of computer technology, networks, sensors, infrastructure, control mechanisms, processing end units and users. Cyberspace contains the information and the networks over which information is transmitted and on which digitized information is stored.

As critical as cyberspace is, cyber security is its potential Achilles heel. Computer networks that are not properly protected with adequate security software, hardware and trained personnel are vulnerable to aggressive and malicious activities that can, at the very least, disrupt information flow. Establishing robust communications, computer networks, information assurance, and cyber security is more important now than ever before if we are to protect the vital networks that play such a critical role in achieving national security, economic independence, and secure and organized daily lives. Effective cyber operations must be employed and managed by professionals who are well versed in protecting their networks and have a firm understanding of security policy and procedures and the tactics and tools of the cyberspace adversary.

Commercial certifications and vendor product courses will never be able to teach the integrated solution of people/communication, processes/tactics, and the Service technology set. Acquiring and honing this type of skill can only be done when the cyber operator is immersed in a training environment that provides:

- The cyber weapons in the operational arsenal
- Realism and stressors of the watch floor
- Exposure to repeatable events with realistic effects

Conducting training and exercises in a risk-free environment is paramount. A risk-free environment ensures each individual has the freedom to explore without fear of catastrophic system failure or a security breach to operational systems.

ORIGINS

In 2002 the Air Force conducted a "first of its kind" computer network defense exercise called Black Demon. The Air Force wanted to develop tactics for responding to a large scale computer network attack and provide the network defender their first 10 cyber warfare combat "sorties." The focus of the initial exercise was on developing tactics, techniques, and procedures for reconnaissance, insider threat, web defacement, viruses, intrusion detection and other malicious threats. Ancillary objectives included improving network operator situational awareness, response to multiple threats, and network defense reconfiguration.

The exercise was conducted on a first-generation (simple) network simulator (referred to as the range) designed to emulate the operational Air Force network. Components were borrowed from wherever they could be found (bench stock, test networks, programs) and software was acquired from the program office or trial licenses were used. It provided a fairly realistic training environment for network defenders and gave them the ability to interact with other participants. However, there were many shortcomings:

- No configuration control between the ranges so each of the four solutions was slightly different
- Network traffic to mask the activities of the red team (attackers) was nominal
- Resetting the simulator took hours
- Exercise inter-connectivity was constrained to a 56K (serial) Virtual Private Network (VPN) connection at the player locations. (This was the approved solution to preclude network saturation and "spillage" of attack events onto the operational network)

Despite the range environment shortcomings, the After Action Report (AAR) from Exercise Black Demon 2002 praised the exercise and recommended that the Air Force develop a permanent environment. The range would provide a risk free environment where network operators can continuously exercise and practice their skills and develop additional tactics to defend against cyber threats. This recommendation generated the original requirements for what is now the Air Force Simulator Training and Exercises (SIMTEX) program.

In 2003, the Air Force followed up on their Black Demon successes and developed the SIMTEX network which was first used for quarterly training exercises. The training events generally focused on providing operational training on new or specific network operations or defense tools used throughout the Air Force. For the 2004 Black Demon event, the Air Force unveiled a standardized simulator suite – SIMTEX– to be used for exercises modeled after its network core, the Combat Information Transport System (CITS) (Figure 1). The SIMTEX network has been used to support training exercises, operational exercises, and Joint network exercises over the past nine years. Thousands of cyber operators have participated and been trained on the latest cyber defense tools, tactics, techniques, and procedures (TTPs), cyber C2, and current threat signatures utilizing SIMTEX. Using the SIMTEX network and Air Force Combat Training Exercises, Air Force cyber operators receive practical experience on the cyber battlefield – their "first 10 combat sorties" in network defense, exposure to real-world threats, and training on cyber C2 processes.

The lack of professionally trained cyber operators led the Air Force to recognize the need to increase the available avenues for simulator training. SIMTEX provided the solution through the use of scenario based training within the synthetic environment and increased the numbers of those trained while greatly improving retention of material taught. The Air Force has placed variants of its SIMTEX simulators in formal school houses at Keesler AFB, Mississippi and Hurlburt Field, Florida, for Communications/ Cyber Operations, Undergraduate Cyber Training, and Defensive Counter Cyber (Intermediate Network Warfare Training) courses.

Even with SIMTEX as the standard solution, its routine use in exercises identified shortcoming and new requirements:

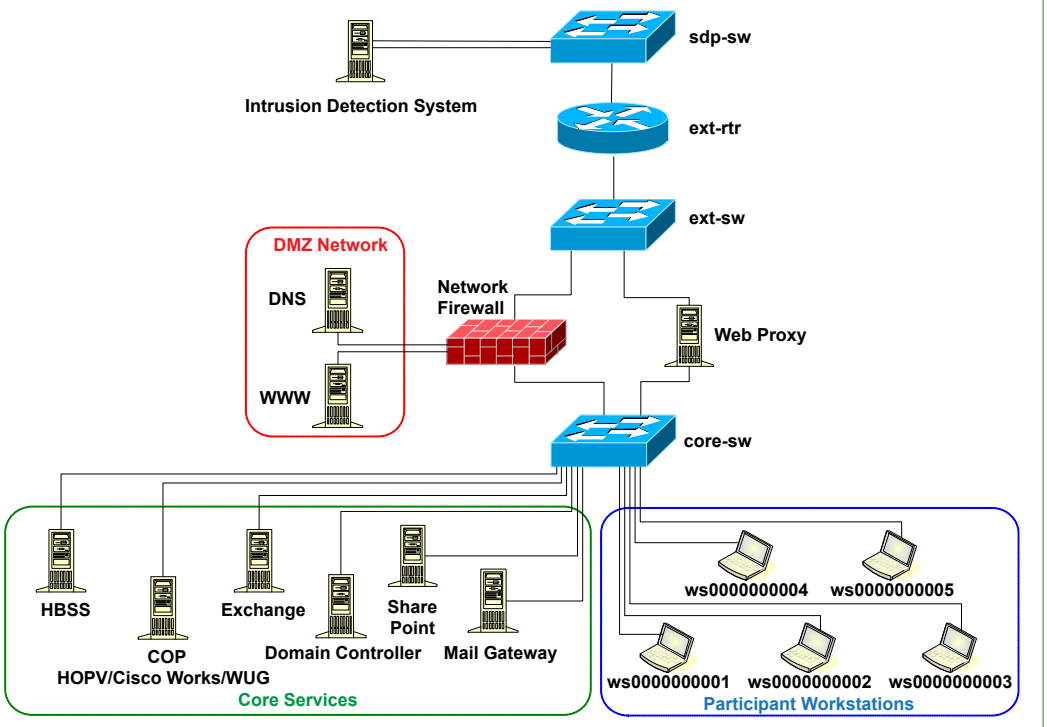

Figure 1: Notional Simulator Architecture

- Realistic network traffic to obfuscate attacks was lacking
- Network traffic produced by the traffic generators did not have payloads that triggered alerts from the network security devices
- An automated means for executing events across the entire interconnected range was needed; use of Information Warfare Squadron personnel to execute the attacks was very expensive
- A status window showing scenario execution status was needed
- Rapid simulator reconstitution capability needed to be developed so scenarios could be quickly re-rolled
- The serial connection between the ranges limited training realism; an approved Wide-Area-Network (WAN) VPN for worldwide interconnections was needed

Over the past nine years, through technology advancements and lessons learned, SIMTEX has evolved into an interoperable network environment based on an open-systems architecture that includes physical, virtual, and simulated network components. SIMTEX models the architecture of the Air Force enterprise network and has expanded to include wide-area network connectivity through the Joint Cyber Operations Range (JCOR) VPN for Joint and Inter-service exercises and training. Through the JCOR VPN, SIMTEX connects to other Service and Combatant Command (COCOM) cyber simulators and ranges.

SIMTEX's synthetic environment is provided through the commercial application SLAM-R® (Sentinel-legion-AutoBuild-Myrmidon-Reconstitution.) The SLAM-R® application provides:

- Institute of Electrical and Electronics Engineers (IEEE) Request For Comment (RFC) compliant real-world network traffic
- Over 3000 simulated users
- An attack manager
- Simulated network events (attacks) within the simulated real-world traffic
- Social media services (comparable to Facebook®/Twitter®)
- A simulated internet
- Reconstitution capability

The integration of commercial applications, appliances, and infrastructure (either virtualized or physical) and SLAM-R® provide a synthetic-live simulator/trainer. The integration of the commercial products with SLAM-R® results in true-life system response either from user actions or from the attacks/events. As in real world operations, user actions can impact the simulator's network (for example, a self-inflicted denial of service). Air Force cyber operators and decision makers (as well as other Services, Joint, and 5-Eyes) utilize the SIMTEX risk-free environment for classroom training, small and large-scale exercises, team competitions, tool development, and mission rehearsal.

LESSONS LEARNED AND INNOVATION LEAD TO EVOLUTION

Governments, corporations, small businesses, and individuals spend millions of dollars annually for commercial training programs and vendor courses. These programs and courses, while teaching industry best practices, accepted standards, and tips and tricks of vendor products, are not enough. To truly be considered an expert in the cyber defense community, cyber operators not only need to know how to use specific products according to vendor guidelines, they must know how their capabilities, when intertwined within their network, provide integrated situational awareness.

The Network Environment–Physical or Virtualized

Many a masters thesis has been written extolling the virtues of virtualization and how it can be used to create a cyber simulator/trainer with a small footprint at a low cost. In theory this is true, if the goal is to create a "generic" cyber environment to only teach basic principles.

The Air Force cyber simulators provide network professionals opportunities to practice classroom learning in a realistic environment that does not impact any operational network. The simulator provides the participants with the same "look and touch" of the computer network environment they manage and defend day-to-day.

At the start of the Air Force program in 2001, virtualization was not as evolved as it is today. Each core service application, infrastructure device, or security appliance was a physical server or device in the simulator. The typical "base" solution filled a 42Unit (U) rack. Today, with virtualization, that same simulator

is still approximately 9U even though the servers for the solution only take up 2-3U. This is because not all of the infrastructure and security devices in the Air Force network come in a virtual appliance. The core services that are virtualized are rapidly reconstitutable. An entire simulator's system baseline can be restored in less than 10 minutes.

For the sake of a smaller footprint and being able to snapshot all components of the simulator, advocates of new cyber simulators entering this arena are encouraging adopting a simulator that is completely virtualized. Air Force lessons learned point toward a different solution – a hybrid of virtualized machines and hardware-in-the-loop. For training/exercising operational forces, replacing brand-name physical devices (loaded with proprietary operating systems) that cannot be virtualized with available open-source virtual devices falls short of meeting the requirements the cyber simulator program evolved from – *train like you fight*.

Attack Engine

During the early stages of cyber exercises, attacks were executed by members of information warfare squadrons (the red cell). In late 2003 the Air Force decided to put a SIMTEX type capability in the Communications school house. Having live players (red aggressors) physically execute each attack wasn't cost effective or feasible. This meant that an alternative solution to the way attacks were delivered to participants had to be developed – an automated method. The attacks/events students would be exposed to had to execute the exact same way for each student for each class. This generated the initial need for simulated attackers – the attack engine.

The attack engine used in SIMTEX (the Myrmidon module) generates network attacks within the simulator's network environment. The core includes a module configured for creating one or more attack events against the network devices (physical or virtualized). Individual attack events are grouped into scenarios. The attack events include exploitations of published vulnerabilities (e.g., SysAdmin, Audit, Network, Security Institute (SANS) Top 10) and failures of hardware and software within the simulator. Scenarios are also created to replicate actual occurrences that affected Air Force operations.

As a result of the comments received from the '07 Bulwark Defender, a graphical user interface (GUI) was developed. As the scenarios got more complex, controllers required insight into the execution status of each attack/event in a scenario. Further, controllers needed a quick view of the details of each attack/event (description of the attack, objective of the attack, system indications and warnings for the event, and attacker and target information).

The GUI provides the interface for controlling and monitoring the creation and execution of the attack events (Figure 2). The GUI includes an attack event editor configured for

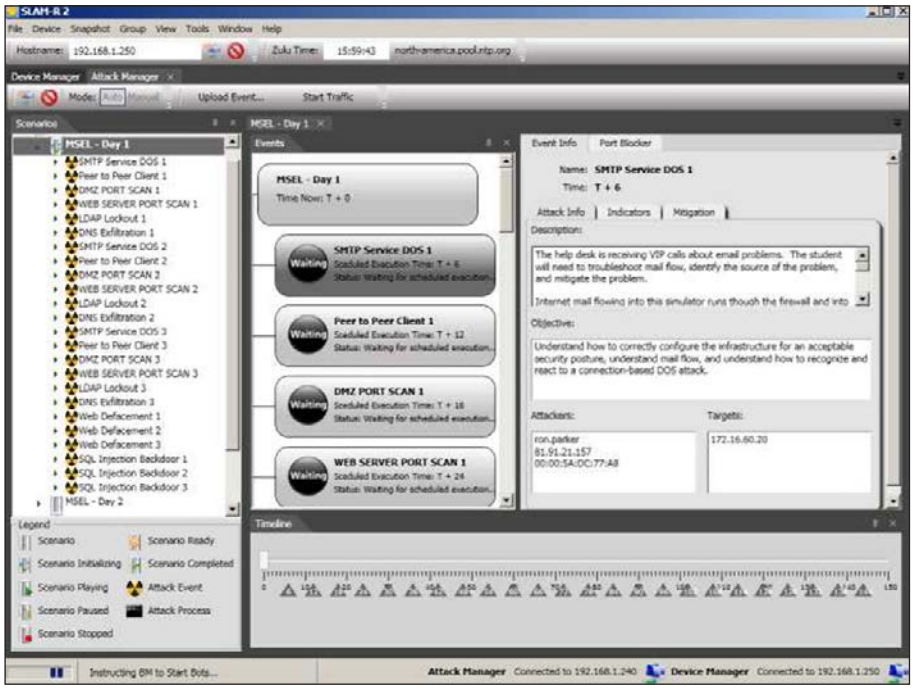

Figure 2: GUI Displaying the Attack Engine

writing the attack events into a standard Extensible Markup Language (XML) file, and wherein the control module is configured for automatically generating unique attributes within each attack event. Attributes include: the source of the attack (both Internet Protocol (IP) and Media Access Control (MAC) address), the attack target, how long into the scenario should the attack start, and how long the attack should run.

The early attack engine required the controller or instructor to be at the keyboard/mouse to execute an event. Exercise participants and students keyed in on the controller/instructor's position at the keyboard in relation to when events would occur. As a result, the capability for the events in a scenario to auto-execute on a timeline was added. Controllers/instructors can start, stop, pause, re-roll and adjust the event kickoff time on the timeline within a scenario.

To show the status of attack/event, an attack scenario execution manager tab populates when an event starts. At execution, a bot server module is generated within a bot of the simulator utilizing at least one of the created attack events. The execution module is configured for monitoring the creation and transmission of the attack events including the success of the attack event within the simulator and attributes of the attack event (Figure 3). This information is relayed back to controller/instructor via the bot to the control window.

Figure 3: GUI Displaying Attack Status

Network Traffic

When the standardized simulator suite was being designed one of the requirements was for traffic generation. The purpose of the traffic was to mask the activities of the adversaries within a "normalized" traffic flow representative of an installation's day-to-day traffic pattern. Over the course of five years, the Air Force integrated two different commercial traffic generators in an effort to populate the simulator with realistic cyber operations traffic. The available solutions were not satisfying the "realistic" requirements. The selected solutions were fashioned for performance testing and did not generate RFC compliant packets to the degree that the network devices (firewall, intrusion detection system, proxy server) were able to inspect the packets (deep packet inspection). This shortfall meant the security devices and applications did not throw the correct indicators and warnings. Network traffic, representative of day-to-day activity that was RFC compliant and attributable to the simulators domain (source and/or destination IP) was ellusive. At the time a cost effective solution providing traffic that met the requirements for the cyber simulator wasn't found. This led to the development of a traffic generation capability focused on producing cyber effects.

The traffic generator in SIMTEX (the Legion module) creates network traffic patterns within the simulator replicating actual network traffic patterns within the Air Force operational network environment. The created patterns generate network traffic between a plurality of network

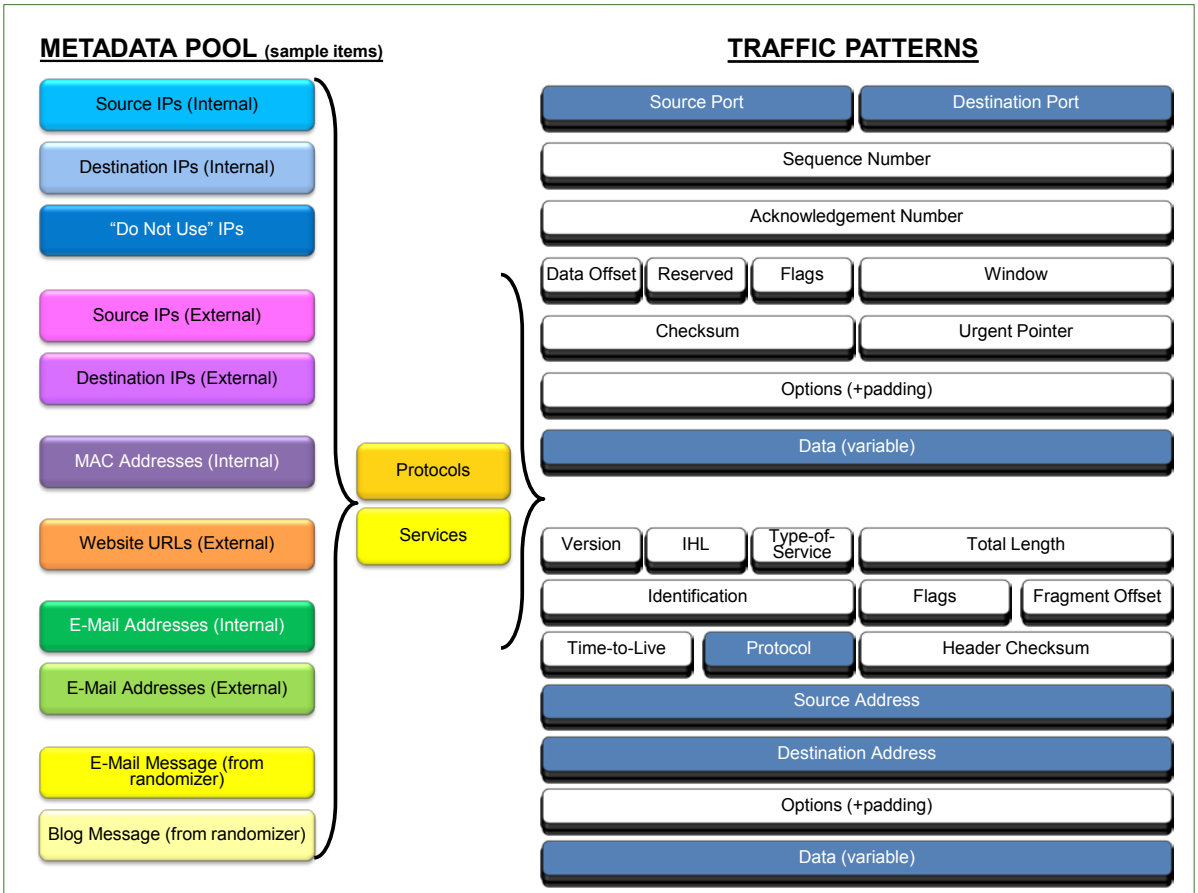

Figure 4: Sample Traffic Metadata Types

devices within the simulator (router to router, router to server, server to server, server to workstation, workstation to server). The module is configured for creating a network traffic agent utilizing one or more of the patterns. The traffic agent is a group of one or more patterns (Figure 4).

The module is further configured for creating a traffic scenario that includes a group of created agents and traffic scenario virtual machines (VM). The VMs act as senders and receivers of packets (patterns) defining a relationship between one or more of the agents in the scenario (Figure 5). An interface is configured for:

- Receiving pattern metadata and adding the received metadata to the associated patterns
- Adding the patterns to the traffic profile
- Generating the scenario VMs and adding the VMs to the traffic scenario

The incorporated network traffic patterns include one or more network traffic protocols selected from the group. (e.g., Domain Name Service (DNS) requests and DNS responses, Hyper Text Transfer Protocol (HTTP) and HTTP Secure (HTTPS) requests and responses, Simple Mail Transfer Protocol (SMTP) send and SMTP receive, Internet Control Message Protocol (ICMP), Transmission

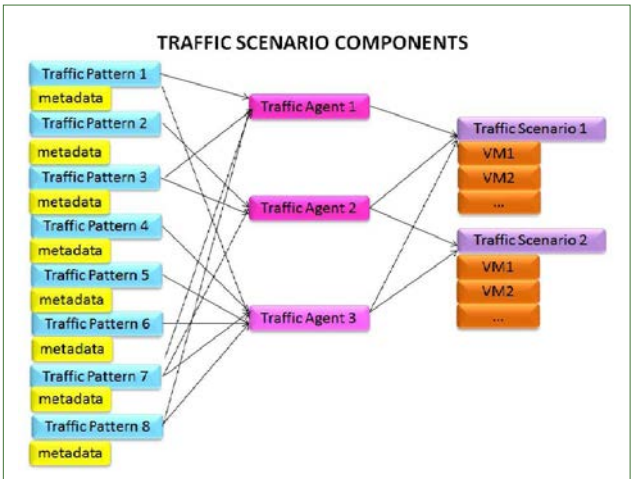

Figure 5: Traffic Scenario Elements

Control Protocol (TCP), and various Remote Procedures Calls (RPC)). The result is network traffic that has source/destination IP addresses, valid e-mail addresses, is RFC compliant, has valid data payloads, and has IP addresses or URLs that resolve with the simulator's DNS structure. Feedback from participants operating the Air Force Information Operations Platform (IOP) during the May '12 Global Lightening exercise was that Legion's traffic is the most realistic they had ever seen.

An example algorithm for generating these patterns is: a user enters the names of 100 different web sites. The user then selects an integer which can be used as input for the level of variance between the basic traffic patterns. A mathematical algorithm is then applied, producing a sequence of number pairs such that they represent the web sites surfed to and the length of time in seconds until the next pair is to be read. Take [23,30:99,13:40] means the 23rd web site is surfed to immediately, then the 99th web site is surfed to 30 seconds later, and then the 40th web site is surfed to 13 seconds later. In this example, the list of 100 different web sites and the integer for variance provides the specified criteria. Based on the requirements of the attack/event scenarios in the exercise or training, the individual traffic scenarios are created by applying the algorithm.

The Internet and Beyond

Bulwark Defender '08 saw the inclusion of robust HTTP traffic added to the simulator and web defacement exploits added to the available attacks/events. A lesson learned from this event generated the requirement for root (tier 1) DNS services. Although the HTTP traffic was realistic, the URLs being outside of the local simulator structure were generating errors because there was nowhere to get the A records. A requirement for a simulated internet of websites followed. The simulated web-site internet is "surfable" by all participants, all web-site URLs resolved in DNS, and generated HTTP traffic (both inbound and outbound) has actual source and destination points (Figure 6).

In 2009, the requirements for the European Command (EUCOM) exercise Austere Challenge dictated more realistic adversaries, targets, and launching platforms. With botnets compromising "innocent victim" machines

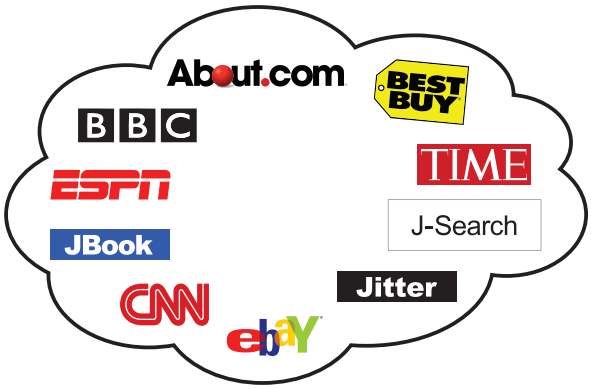

Figure 6: Simulated Internet

around the world, a world-wide botnet attack scenario was detailed in the exercise requirements. To complement the current SIMTEX simulators/JCOR, a simulated Range Global Internet (RGI), a Synthetic Non-Kinetic Bombing Range of sorts, was designed and implemented (Figure 7).

The RGI provides a look and feel comparable to the actual internet. It provides for controlled and secure training scenarios outside of the public realm. The RGI is completely virtualized, using open source utilities where possible, and utilizes real IP addresses found in the global internet structure.

The RGI is made up of 30+ backbone routers, with more than 150 class C subnets, supporting 150+ domestic and international web-sites and 35 fully functional e-mail servers along with global DNS and Network Time Protocol (NTP) services. J-Services provides social media services ranging from domestic to foreign personal blogs, and Facebook® and Twitter®-like services. The RGI also includes RFC compliant internet traffic-generation providing routine traffic activities between internet routers, DNS queries to actual servers, website "GET" request, e-mail generation, along with other miscellaneous random traffic (e.g., ICMP). The RGI is comprised of four (4) interconnected networks spread across six (6) continents. Multiple location types are represented around the globe: hospitals, banks, universities, cyber cafés, commercial business, churches, government entities, and the military. The locations have full domain services and defense in depth construction.

With the true-IP global routing infrastructure in place and various location types populating the subnets around the

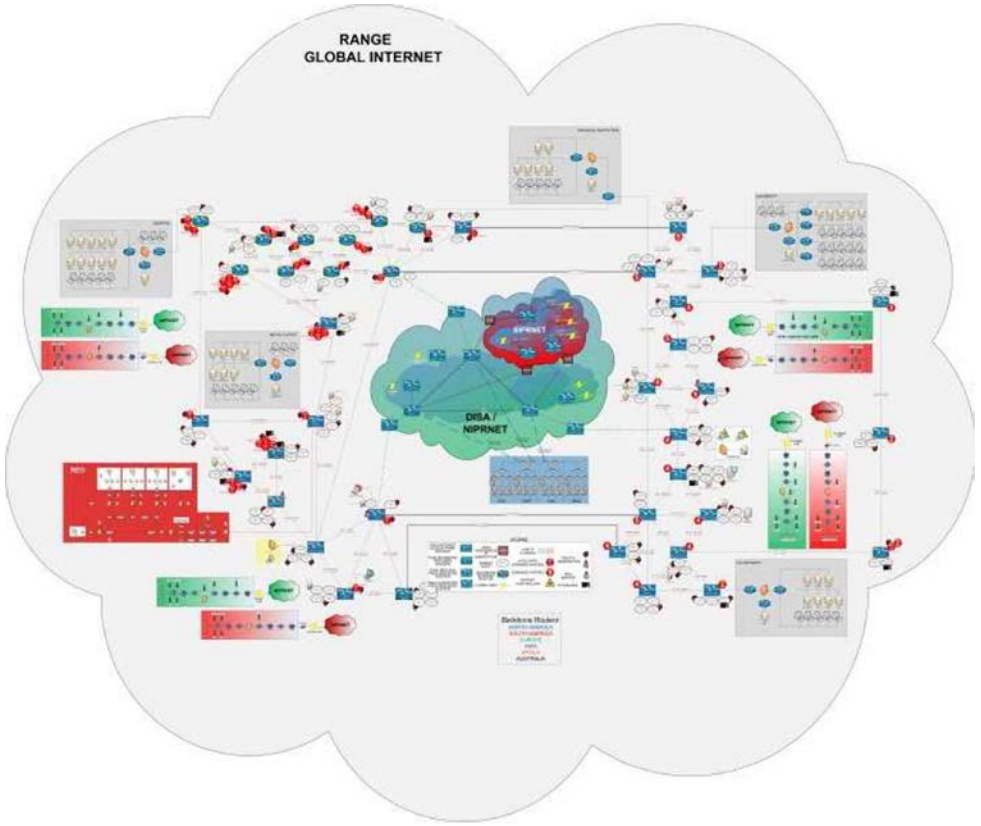

Figure 7: Range Global Internet

world, exercise engineers built out the gray-space locations for Austere Challenge. During the exercise, a trace of an attack showed gray-space machines (and victim machines of the botnet) virtually located around the world.

FUTURE WORK

Modeling and simulation work in the area of cyber is still in its infancy. There is a large need for additional capabilities and interconnections for synthetic-live Cyber environments.

SCADA

It can be assumed that any major engagement in the near term with a capable opponent will involve a major component in the cyber arena. It can also be assumed that one of the main targets within the cyber arena for any such opponent will be our critical infrastructure and industrial control systems. Therefore, it is vital that we train a new type of cyber-defender specializing in their defense. Integrating this capability into SIMTEX/JCOR and the RGI is a logical next step.

Internet Supervisory Control and Data Acquisition (SCADA) refers to industrial control systems (ICSs) that monitor and control industrial, infrastructure, and facility-based processes. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. These systems encompass the transfer of data between a SCADA central host computer and a number of Remote Terminal Units (RTUs) and/or Programmable Logic Controllers (PLCs), and the central host and the operator terminals.

The current SCADA master station architecture is an open system architecture rather than a vendor controlled, proprietary environment. The architecture consists of multiple networked systems sharing master station functions. While there are still RTUs utilizing protocols that are vendor proprietary, it opens the system architecture, utilizing open standards and protocols and making it possible to distribute SCADA functionality across a WAN and not just a LAN. With critical infrastructure control systems existing on WANs, connected through the public internet, the threat of remote disruption by hostile agents moves out of the arena of science fiction and into reality.

The first publically-acknowledged, real-world example of a government-sponsored attack against critical infrastructure was Stuxnet, a computer worm first discovered in June 2010. Stuxnet targeted Siemens industrial software and equipment, reprogramming PLCs and disrupting the Iranian uranium enrichment infrastructure.

While such sophisticated systems generally require specialized knowledge and are difficult to produce without state support, we can fully expect such systems to be developed and used against our critical infrastructure systems, and therefore we need to be equipped to defend against them.

We cannot expect defenders to be adequately trained to defend modern critical infrastructure from attacks if they are not exposed to realistic training systems. In much the same way that aircraft pilots are trained first in on-the-ground aircraft simulators and then in real aircraft, the need for extremely realistic advanced training systems cannot be overstated. While simulation is useful in the earlier stages of training, these defenders need to be trained on the real-world SCADA systems controlling simulated infrastructure instead of actual real-world infrastructure. Fully integrating SCADA and simulated infrastructure into cyber simulator environments will be critical for our defense in the near future.

Evolutionary Process for Automatic Scenario Generation

One of the key problems with training is that exercises cannot be easily repeated by the same student, since the student will have previous knowledge of the problem space from a previous run. It is unrealistic to manually generate a new environment for them on multiple occasions, but if we can generate their problem environment computationally then the student could be continually exposed to similar situations repeatedly and therefore develop a deeper understanding of the methods for defending their systems.

A typical educational program aimed at young children learning arithmetic is a good example of this idea. Such a system might ask the child to determine the result of 12/55 one time and 7/43 the next. It does not have a large store of predetermined division problems but instead randomly generates those problems for the student to answer. In a similar, albeit vastly more complicated manner, it is feasible using concepts from evolutionary algorithms (EA) to computationally generate useful training environments for cyber operations.

In artificial intelligence (AI), EAs are a style of generic population-based meta-heuristic optimization algorithms whose processes are inspired by those of natural biological evolution (Figure 8).

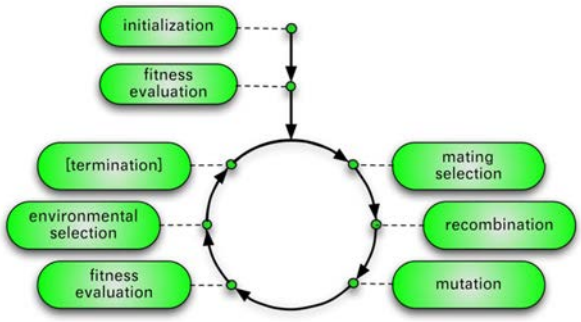

Figure 8: Evolutionary Process

The primary mechanisms employed in EAs to evolve a population of possible solutions towards an optimal one are:

- Parent selection based on fitness
- Recombination
- Mutation
- Survivor selection based on fitness

Evolution serves as a powerful metaphor and demonstrates great creativity in both the natural world and in the world of computer science.

A learning classifier system (LCS) is an EA that operates on a population comprised of rules referred to as the rule set: this rule set is used to attempt to classify a situation. The first LCS was created shortly after genetic algorithms (GA) were created and is considered one of the classical types of evolutionary algorithms. Since then there have been several improvements in the field.

Genetic programming (GP) is an EA-based methodology to find computer programs that perform a user-defined task. GP is a specialization of GA where each individual is a computer program, either partial or complete. It is a machine learning technique used to develop and optimize a population of computer programs according to a fitness landscape determined by a program's ability to perform a given computational task. Techniques derived from GP could be applied to the domain of generating training environments. Many seemingly different problems in AI, symbolic processing, and machine learning can be viewed as requiring discovery of a computer program that produces some desired output for particular inputs. When viewed in this way, the process

of solving these problems becomes equivalent to searching a space of possible computer programs for the "best fit" individual computer program.

There exists the potential to add computational opponents to the training simulation by employing GP. In a game, there are two or more independently-acting players who make choices (moves) and receive a payoff based on the choices they make. A "strategy" for a given player in a game is a way of specifying what choice (move) the player is to make at a particular point in the game from all the allowable moves at that time and given all the information about the state of the game that is available to the player at that time. Strategies for games may be expressed in several different ways, even in terms of the state of the game or in terms of various features abstracted from the state of the game. By abstracting the simulation state space, we could then use that abstracted representation as a basis for evolving computational opponents. These opponents might be defensive, defending their systems from the human student. The opponents may also be offensive, attacking a network that the human student is trying to protect. Both of these scenarios would be useful for training.

Using LCS and GP to computationally generate an attack scenario based on previous responses of the cyber operator would allow for cyber-operations training and simulation as a game that could complement the human-driven environment. It is well known that serious games provide some of the best training methods available. Game-based learning (GBL) is a branch of serious games that deals with applications that have defined learning outcomes. GBL has the potential of improving training activities and initiatives by virtue of its engagement, motivation, role playing, and repeatability. Integrating serious gaming via GP into a cyber simulator would potentially be of great value allowing for automatic scenario generation based on the skill/progress of the players.

CONCLUSION

The Air Force, either in Air Force only exercises/events/competitions or in joint activities has had tremendous success with SIMTEX and JCOR. The consistent feedback from Blue Force operators, students, and Senior Leaders is that the cyber range is a must have commodity. Being on the simulator/range where they are challenged to fight through the attack with the toolset they have available is invaluable.

Depth and breadth of knowledge is required by cyber crews to understand the technically complicated infrastructure and network "system of systems" selected by program offices. Managing and defending it against an ever-increasing number of highly motivated adversaries only comes from using a hands-on training environment comprised of the components used in daily operations so theory can be put into practice.

Much of what cyber operators do is intuitive. Constant exercise of those thought processes provides the continued skill level improvements and innovative approaches needed to stay ahead of the technical problems and hostile activities. Doing this in an environment that does anything other than truly replicate the cyber operator's environment (or the adversaries) falls short of satisfying the goal: achieving and maintaining a cyber security posture for our critical national computer network infrastructure. Training and exercising with a synthetic-live cyber environment provides a foundation for ensuring our critical infrastructure is adequately protected from any and all deliberate attacks and provides the information and mission assurance expected and needed by all levels of leadership.

References

Air Force Network Integration Center (2011). *Cyber Simulator Requirements.*

Andel, T., Stewart, K., Humphries, J. (2010). Using Virtualization for Cyber Security Education and Experimentation. *14th Colloquium for Information System Security Education (CISSE).*

Boyd, Marcus, Colonel, USAF (2012). Air Force Cyberspace Modeling & Simulation (M&S). *AFCEA Orlando: Air Force LVC Operational Training for the Cyber Warrior.*

Corrin, Amber (2012). Seismic Shift Occurs in Air Force Cyber Planning. *Defense Systems,* Vol 6, Number 2, page 14.

Eiben, A. E., Smith, J.E. (2003). *Introduction to Evolutionary Computing.* Springer-Verlag.

Falliere, N. (2010). Exploring Stuxnets PLC Infection Process. Retrieved April 12, 2012, from http://www.symantec.com/connect/blogs/exploringstuxnet- s-plc-infection-process.

Gilmore, J. Michael, Director, DOT&E (2011). Information Assurance (IA) and Interoperability (IOP). *Director, Operational Test and Evaluation FY 2011 Annual Report,* pages 285-291.

Hansen, Andrew P., Major, USAF (2008). Cyber Flag A Realistic Cyberspace Training Construct. *Masters Thesis.* Wright-Patterson AFB, Ohio: Air Force Institute of Technology.

Institut für Neuroinformatik, Ruhr-Universität Bochum (2012). *Shark – EALib Documentation*. Retrieved April 21, 2012, from http://shark-project. sourceforge.net/2.1.2/doc/EALib/index.html.

Koza, J. R. (1990). Genetic programming: A Paradigm for Genetically Breeding Populations of Computer Programs to Solve Problems. *Technical report. Stanford, CA: Computer Science Department, Stanford University.*

Liljenstam, M., Liu, J., Nicol, D., Yougu, Y., Uan, G., Grier, C., (2006). RINSE: the Real-time Immersive Network Simulation Environment for Network Security Exercises. *Simulation*. Vol 82, Issue 1. San Diego, CA: Society for Computer Simulation International.

McBride, Aaron. (2007). Air Force Cyber Warfare Training. *Defense Standardization Program Journal,* pages 9-13, April/June 2007.

National Communications System (2004). NCS TIB 04-1. *National Communications System Technical Information Bulletin 04-1: Supervisory Control and Data Acquisition (SCADA) Systems.* Arlington, VA: Office of the Manager, National Communications System.

Network Centric Operations Industry Consortium (NCOIC) (2010). *Net-Centric Cyber Simulator Capability Pattern.*

Sanger, David E. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times,* June 1, 2012, retrieved from http://www.nytimes.com/2012/06/01/world/middleea st/obama-ordered-wave-of-cyberattacks-againstiran. html?hp&pagewanted=all.

Susi, T., Johannesson, M., Backlund, P. (2007). Serious games – an overview. *Technical Report.* School of Humanities and Informatics, University of Skovde, Sweden.

Authors' Biographies

Stephanie D. Harwell

Stephanie D. Harwell, Vice President, Cyber Solutions of Camber Corporation, has been involved in the evolution of cyber simulators since the Air Force's first implementation in 2001. Her experience includes designing, developing, and maintaining integrated synthetic-live cyber environments. Ms. Harwell is a former Air Force Communications Chief Master Sergeant, retiring in 2004, where she pioneered the concept of using simulators for training and exercising the Cyber Operations crew force. She manages the systems design, software development, and systems integration for Camber's Cyberoperations Enhanced Network and Training Simulator (CENTS®) product line. She holds a Master of Science in Information Technology and a Bachelor of Science in Information Systems.

Christopher M. Gore

Christopher M. Gore is a Research Scientist with Camber Corporation's Cyber Development and Integration team. He received his Master of Science in Computer Science from Missouri University of Science and Technology and his Bachelor of Science in Mathematics and Computer Science from Eastern Illinois University. His graduate research focused on evolutionary algorithms and their application to difficult problem domains in the financial arena. He has worked professionally on embedded avionics systems and cyber-operations systems for several years. His future plans involve applying methods from evolutionary computation towards problems in the cyber-operations arena.

About the *M&S Journal*

The *M&S Journal* is a quarterly publication for modeling and simulation professionals in the Department of Defense and other government organizations, academia, and industry—in the U.S. and around the globe.

- Focus. The focus of the *M&S Journal* is on the topical and the timely: What is changing in M&S applications and practices? What trends are affecting M&S professionals? What challenges can we expect in the future?
- Organized by Theme. Each issue of the *M&S Journal* explores a single area in M&S, offering the reader a greater understanding of the challenges and opportunities from a variety of perspectives.
- Our Authors. Articles are written by accomplished M&S practitioners recognized for expertise in their areas of specialty.
- Guest Editors. Respected leaders serve as guest editors, providing viewpoints relating to the theme of the issue, viewpoints that may change your perspective.
- Editorial Board. Content for the *M&S Journal* is shaped by an Editorial Board comprised of leaders from all sectors of M&S.
- Peer Reviewed. The *M&S Journal* is peer reviewed by M&S professionals. Our review process is based upon substance, accuracy, relevance, and clarity.

How to Subscribe

- If you would like to subscribe to the *M&S Journal*, send an email to:

MS-Journal-Subscribe@Lists.AlionScience.com

Article Submission Guidelines

- **Manuscripts:** Manuscripts should be in camera-ready form for publication.
- **Length:** Articles should be between 1500–6000 words (3-12 pages).
- **References:** References should be included with corresponding callouts in the body of the article.
- **Article Content Order:**
  - Article Title
  - Author(s) names, titles, and contact information
  - Abstract of article (request abstracts not exceed 250 words)
  - Body
  - References
  - Brief biographies of each author (request biographies not exceed 200 words per author)
- **Text Format:** Manuscripts should be submitted in standard Microsoft Word® format. The content of the paper may be adapted to fit the *M&S Journal* layout.
- **Figures and Tables:** Figures and tables should be labeled and referenced within the body of the article. We request high resolution (300 dpi) files or large jpeg files for figures. Readability is essential.
- **Clearance:** All original material must be cleared for public release (Distribution A) if required by author organization prior to submission to the *M&S Journal*. The Editorial Staff will submit accepted articles for DoD Public Affairs Office clearance.
- **General:**
  - Articles should describe efforts that have already yielded documentable results.
  - Authors will receive submission confirmation within a week of article receipt.
  - Authors may be contacted should the Editorial Staff have questions.
  - Notification will be given when the final acceptance/rejection decision has been made.
  - The *M&S Journal* Editorial Staff reserves the right to modify a paper for the purpose of typographical or grammatical corrections.
  - The *M&S Journal* does not accept papers that are structured as commercial advertising, or as promotions of products or services.

Submit articles via email to:

ask.msco@osd.mil

or call for information:

703-933-3323 or 888-566-7672

Future Issues of the *M&S Journal*

—Themes and Dates—

Issue	Theme	Articles Due
Fall 2013:	Reuse for M&S	-
Winter 2013:	M&S for Acquisition	-
Spring 2014:	Research in M&S	09/19/13
Summer 2014:	International M&S	01/07/14
Fall 2014:	Logistics in M&S	02/25/14
Winter 2014:	Medical M&S	06/05/14

Note: Themes and dates of future issues of the *M&S Journal* listed above are subject to change. Prior to submitting, please contact:

ask.msco@osd.mil
or call 703-933-3323 or 888-566-7672

Editorial Board

Editorial Staff

The DoD Office of Security Review has cleared this document for public release (Distribution A)
(Case No. 13-S-2931).

SUMMER EDITION 2013
VOLUME 8 ISSUE 2

M&S JOURNAL

A DoD MODELING & SIMULATION COORDINATION OFFICE PUBLICATION