Towards a Modeling and Simulation Interoperability Standard for Cybersecurity

Michael Papay, PhD
Northrop Grumman
McLean, VA
michael.papay@ngc.com

Aaron Fansler
Northrop Grumman
Colorado Springs, CO
aaron.fansler@ngc.com

ABSTRACT

Despite the fact that the World Economic Forum declared that cybersecurity is one of the top five global risks to watch in 2011, little has been done to date to organize the defense community to prepare for the effective utilization of modeling and simulation of cyber theft, cyber espionage, cyber war, or cyber terrorism. Recently, the technologies associated with computer network operations have grown dramatically, with an associated increased emphasis and capability across academia, industry and government organizations. In order to secure the future of cyberspace, it is necessary to develop a modeling and simulation interoperability standard for cybersecurity that will enable many organizations to bring forth their best threat models, network simulations, and attack and exploitation analyses so that they may work together on cyber ranges.

The history of other M&S interoperability standards is well known; the Distributed Interactive Simulation (DIS) and the High Level Architecture (HLA) standards were both born out of the need for interoperability among models and simulations. For battlefield simulations, for instance, the organization that knew the most about a particular platform could also build that model, and expect it to operate within the bounds of a simulation that adhered to the standard. The research shows that no one has yet successfully implemented a cybersecurity interoperability standard using the DIS or HLA framework, including their extensions. This paper also proposes the top level organization of a new cybersecurity interoperability standard, suggests a concept of operations for building and maintaining this standard, and recommends stakeholders that should be involved in the balloting for the standard.

ABOUT THE AUTHORS

Mike Papay is the Vice President of Cyber Initiatives with Northrop Grumman. He has over 25 years experience in engineering and developing solutions for the Department of Defense and Intelligence Community, including ICBMs, a variety of missile defense systems, Command and Control Systems, networking solutions, satellite and ground systems, airborne ISR platforms, modeling and simulation programs, military training tools, and most recently, cybersecurity. Mike is a Northrop Grumman Technical Fellow, and has a B.S. and a Ph.D. in Aerospace Engineering from Virginia Tech.

Aaron Fansler is the Program Manager for the Cyber Critical Infrastructure Protection (CCIP) Program with Northrop Grumman. He has over 15 years experience working for the Department of Defense (DoD) and the Department of Energy (DOE) in support of Computer Network Operations (CNO). Aaron is a doctoral candidate and has a Master's degree in Information Assurance from Capitol College and a B.S. in Applied Mathematics from the University of Colorado.

Towards a Modeling and Simulation Interoperability Standard for Cybersecurity

Michael Papay, PhD
Northrop Grumman
McLean, VA
michael.papay@ngc.com

Aaron Fansler
Northrop Grumman
Colorado Springs, CO
aaron.fansler@ngc.com

Definitions and Market Scope

The terms "cyber", "cybersecurity" and "cyber attack" are everywhere today. They are continuously covered in the news media, talked about in presidential speeches, and discussed around the dinner table. For the purposes of developing cyberspace as a war-fighting domain, the United States Department of Defense (DoD) Vice Chairman of the Joint Chiefs of Staff developed a standard joint cyber operations lexicon. The definition of "cybersecurity" in that lexicon is useful to set the stage for the development of a standard, since common terminology is critical when discussing how systems interoperate. "Cybersecurity", as defined in that lexicon, is "All organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents and failures."[1] That definition is fairly broad, and indicates the scope of the cybersecurity modeling and simulation task at hand. The DoD now recognizes Cyberspace as a "new domain of warfare" just like the warfare domains of Air, Land, Sea and Space.[2]

In business terms, the size of the cybersecurity problem is immense. In the six year period from 2010 through 2015, the cyber market is expected to top $342B across the US DoD, Federal/Civil, Commercial, and International Information Technology (IT) Security and Cyber market sectors.[3] In addition, cybersecurity of the "Critical Infrastructure" looms large in many DoD and corporate strategies. Critical Infrastructure Protection (CIP) is commonly defined as protecting the following five sectors from cyber attack: energy, communications, financial, transportation, and health IT. A market this large and varied requires some sort of structure at the next level down in order to understand how to approach the problem, and therefore how to simulate it. Several organizations have made an attempt at this next level structure.

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The institute maintains a consensus document of 20 crucial security controls designed to establish a prioritized baseline of information security measures and controls that can be applied across Federal enterprise environments.[4] The SANS 20 Critical Controls (CC) for effective cyber defense range from Inventories of Authorized and Unauthorized Devices and Software (CC 1 and 2) to Wireless Device Control and Data Loss Prevention (CC 14 and 15). In addition, the National Institute of Standards and Technology (NIST) has developed a set of recommended security controls for Federal information systems and organizations.[5] While the selection and implementation of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization, neither of these documents provides an appropriate decomposition of the cybersecurity domain for use as a standard for modeling and simulation.

Recent government efforts are seeking to improve our understanding of our Information Technology systems and promote open discussion around the funding and direction necessary to prevent cyber attacks on these systems. A May 2011 Defense Science Board Task Force on Resilient Military Systems states "An important step toward designing, implementing and maintaining more resilient systems is to understand how to measure the resiliency of those systems relative to various cyber attacks and adversaries. Establishing useful measures and metrics is a first step toward quantifying and developing systematic methods and standards to improve both real resiliency and confidence in our process."[6] The US Congress proposed House Resolution 2096 on June 1, 2011, the Cyber Security Enhancement Act of 2011 calling for the Director of the National Institute of Standards and Technology (NIST) to "ensure coordination of United States Government representation in the international development of technical standards related to cybersecurity."[7]

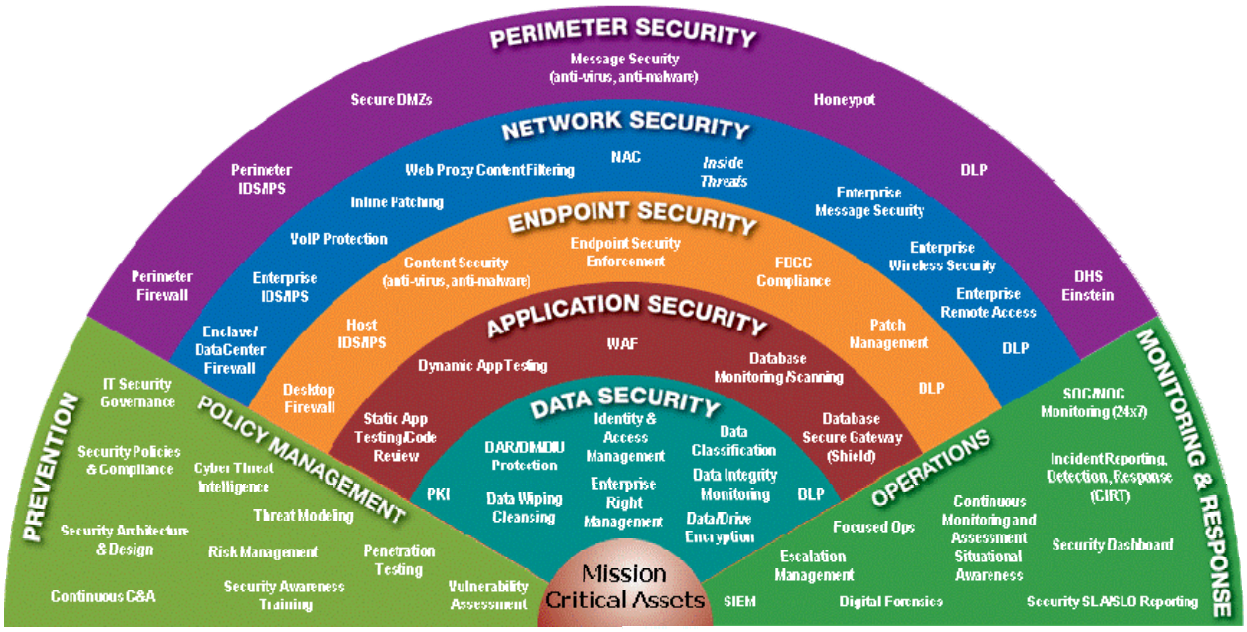

Figure 1. A Layered Cybersecurity Defensive Reference Model

Building on Previous Efforts

Most experts in cyber would agree that "defense in depth" is critical to solid cybersecurity. An example of a layered cybersecurity defensive reference model[8] that provides defense in depth is shown in Figure 1. Similar to describing defense in depth in the missile defense domain, in the cyber domain the mission critical assets are located at the core of the diagram, with the defensive security layers progressing outward from data and application security through endpoint, network and perimeter security. These security layers are supported by the policy management and monitoring and response processes, important functions to ensure that the security measures are successful.

An example of a hierarchical structure in the network modeling and simulation domain is the OPNET Modeler tool. "OPNET models are structured hierarchically, in a manner that parallels real network systems. Specialized editors address issues at different levels of the hierarchy. This provides an intuitive modeling environment and also permits re-use of lower level models. OPNET has defined four modeling domains: Network, Node, Process and External System. The Network Domain's role is to define the topology of a communication network. The communicating entities are called nodes and the specific capabilities of each node are defined by designating their model."[9] While not specifically developed to provide a modeling environment for cybersecurity, this hierarchical model is certainly an approach worth integrating into a cybersecurity interoperability standard.

Applicability of Previous M&S Standards

There have been several successful standards in the modeling and simulation of battlefield entities and their interactions in the past 20 years. Distributed Interactive Simulation (DIS) is a government/industry initiative to define an infrastructure for linking simulations of various types at multiple locations to create realistic, complex, virtual worlds for the simulation of highly interactive activities. The standard was developed in an open forum including government, industry, and academia, and was refined in a series of semi-annual Workshops that began in 1989.[10] The DIS Standard, IEEE 1278.1a, has an extension, IEEE 1278.2, for Communications Services and Profiles. While IEEE 1278.2 is also a layered model, it is only based on the seven layer Open Systems Interconnection Reference Model and it defines the communication services required to support the message exchange described in IEEE 1278.1, not an interoperability standard designed to integrate cybersecurity simulations.[11]

The long lasting success of the DIS standard in analysis, training and engineering simulations led to the development of the High Level Architecture (HLA) standard that incorporated an improved mechanism for simulations that required time management and data distribution. The HLA provides a general framework within which simulation developers can structure and describe their simulation applications. Flexibility is the

aim of the HLA. In particular, the HLA addresses two key issues: promoting interoperability between simulations and aiding the reuse of models in different contexts.[12] The three main components of the HLA: the Framework and Rules Specification, the Object Model Template Specification and the Federate Interface Specification, provide most of the generic interoperability required for the majority of simulations. If the HLA was selected as the integrating mechanism for a variety of cyber simulations, the seven step Federation Development and Execution Process (FEDEP) would be used to design, develop and test the federation. It is likely that this approach in the cyber domain would immediately lead to an effort to develop a standard Federation Object Model, or CYBER FOM, much like the Real-Time Platform Reference (RPR FOM) evolved from the DIS representation of entities on the battlefield. For battlefield entities and interactions, this approach worked well, because the characterization of the battlefield was well known. New simulations wishing to join the federation needed to merely adapt their interface to the FOM, run a common RTI, and join the exercise. In cyber, the characterization of the "battlefield" is still evolving. New threat vectors, malware, and exploits are being uncovered every week, and many of the players in the cyber domain have little experience with HLA or M&S, making a solid, lasting FOM definition very challenging.

Agent-Based Modeling and Simulation

A recent approach to developing simulations with excellent flexibility is agent-based modeling and simulation (ABMS). Unlike other modeling approaches, agent-based modeling is addressed from the agent's perspective, and entails a set of agents, relationships and a framework.[13] In ABMS, the emphasis on modeling the heterogeneity of agents across a population and the emergence of self-organization are two of the distinguishing features of agent-based simulation as compared to other simulation techniques such as discrete event simulation and system dynamics.[14] In ABMS, agents may be adaptive and goal-directed. These qualities are important in the cybersecurity domain. Several tools and frameworks exist in the open such as Repast Simphony (http://repast.sourceforge.net) and NetLogo (http://ccl.northwestern.edu/netlogo); these are both available for a variety of institutions and industry partners. They allow very simple models to be developed quickly, and very complex models to be examined completely.

Agent-Based Modeling and Simulation has its roots in the field of autonomous agents and multi-agent systems (MAS). An MAS can be defined as a loosely coupled network of problem solvers that work together to solve problems that are beyond the individual capabilities or knowledge of each problem solver.[15] There are clear advantages to developing cybersecurity simulations in a framework based on ABMS. The basic makeup of an agent is shown in Figure 2.[16]

Figure 2: The Basic Agent Ingredients

When this field was just starting, it was obvious that tools and frameworks were necessary to allow significant progress to be made. Now that some tools are available, is a standard required to allow agents to work together with simulations in other frameworks? Let's look at some applications and a case study to determine the answer to that question.

LVC Applications

The definition of any cybersecurity standard must work well across the Live, Virtual and Constructive (LVC) domains of M&S. In cyber, the Live domain is equivalent to operations in a Cyber Security Operations Center (CSOC) (Figure 3), where network defenders are continuously monitoring cyber attacks and the appropriate response. The Virtual domain is akin to conducting experiments on a cyber range – a controlled environment where simulated networks are built, attacked, and measured. The Constructive domain for cyber needs to be able to model very large networks, a variety of operating systems, firewalls and Intrusion Detection Systems, and cyber threats from viruses, worms, and malware to denial of service attacks. A standard built for the constructive domain should be able to be easily extended to the live and virtual domains.

Figure 3. A Typical CSOC

Case Study – Critical Infrastructure

Control system networks make up a vast amount of the critical infrastructure in the world. In particular, every modern technology for everyday activities in the US relies on the generation, transmission, and distribution of electric power. This simple fact makes the US power grid the most depended on critical infrastructure in the United States. Past real world events and numerous government demonstrations have shown just how vulnerable the electric power infrastructure can be, not only from natural disasters but more importantly, increasingly malicious cyber activity. Cyber threats to the infrastructure range from having a simple power outage with minimal impact to catastrophic cascading interdependent infrastructure failures caused by script kiddies, hackers, insiders, and even adversarial countries.

Critical infrastructures such as the power grids involve highly complex, multi-dimensional cross infrastructure connections with other infrastructures; effects from attacks are hard to predict and compare analytically. The major factor in not being able to conduct a vulnerability assessment evaluation on a system is the fact that existing systems are in use and cannot be used for experimentation nor can they be shut down. Another option is to develop a real-life duplicate system to be used merely for research purposes, but this is time-consuming, extremely cost prohibitive and will become exponentially more difficult to develop if multiple interlinked infrastructures need to be recreated. Therefore, relying on models for scenario driven simulation and emulation is the only effective approach available. This approach introduces other problems such as calculating the effects of one complex infrastructure network model on other interconnected models. These analytical computations of each critical infrastructure network become nearly impossible in existing simulation frameworks. This makes it crucial that real-time modeling, simulation and emulation of these control networks be developed. The only way to properly protect control networks will be through the discovery of potential single and interdependent vulnerabilities to cyber attacks, and determine mitigation actions. The best way for this to occur will be to execute multiple modeling scenarios to study the initial, secondary and tertiary effects as they cascade through the interconnected networks to discover and mitigate potentially catastrophic failures.

Throughout each critical infrastructure community there exists numerous modeling and simulation tools that are used for their respective critical infrastructure network. Simulated worlds can be built in simplistic worlds such as SimCity (Figure 4), but don't contain enough fidelity to resolve many detailed issues needed by each sector. To achieve more detailed modeling, currently the energy sector has simulation tools such as Powerworld and Real Time Digital Simulator (RTDS), the pipeline industry has Stoner Pipeline, and the railroad industry has RAILSIM. Communications, banking, water and other industries each have their own tools to study their particular area of interest. Over the past decade, multiple efforts[17,18,19,20] have been conducted to study vulnerabilities and behavioral analysis caused by interdependencies through a number of modeling & simulation approaches. Among these approaches, Complex Network (CN) theory, Federated Object Modeling (FOM), and Object-Oriented Modeling (OOM) have been widely used as the best approaches for performing modeling of complex systems.[21]

Despite individual successes, no singular approach has moved to the forefront as a comprehensive simulation integration mechanism for the critical infrastructure. The questions that continue to challenge the industry are: how to integrate all models to a specific standard, how to integrate the simulated heterogeneous system components associated with each network; how to integrate the simulation engines; and what standardized integration framework should be used. Currently, no unified standards exist specifically for dealing with efforts focused on crossing the boundaries of the critical infrastructure modeling, simulation and emulation field. Several standards such as HLA and DIS are currently being employed by users to exchange information between cross-infrastructure distributed simulation models that are built at the same level of abstraction.

In order to ensure that realistic effects will be recreated within the critical infrastructure, a simulation environment with sufficient detail and complexity is needed to produce the multifaceted interdependencies that occur between real world devices. An oversimplification of the environment or the interoperability standard will result in the introduction of errors and produce meaningless results.

Figure 4. A Simulated Model of the Critical Infrastructure

The adoption or creation of a new recognized standard used for modeling, simulation, and emulation architectures for use in cross domain interdependency studies is needed to uncover and address the cyber vulnerabilities. More importantly, the ability to create a more accurate and robust environment to generate both physics-based and effects-based high precision real world interactions across all infrastructures is needed. The merging of simulation and emulation at the network level will then become indistinguishable from the physical (real-world) level (Figure 5). More is needed than just ones and zeros or "on" and "off" being represented as the only values for cross domain infrastructure modeling. The HLA standard has been successfully used by The Idaho National Laboratory (INL) with their CIPR/sim tool[22] in recent years to integrate a few basic simulations, but a more careful examination is required before determining that it can be extended to integrate all cyber domains.

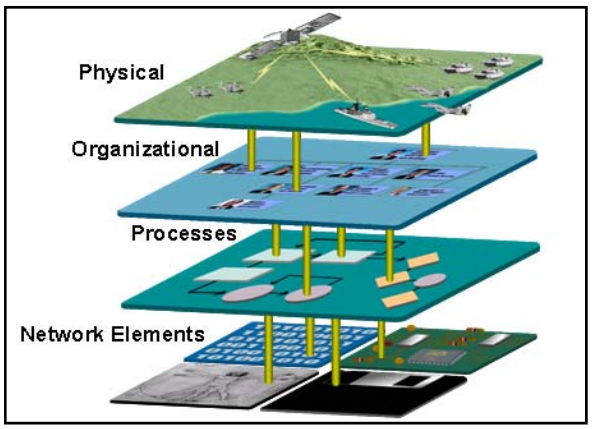

Figure 5. Physical to Network Level Modeling

A New Kind of Standard

The research presented here has led the authors to conclude that there is potentially a new kind of standard on the horizon for integrating cybersecurity models and simulations.

CONOPs for Building and Maintaining a Standard

A reasonable approach to understanding what is needed is to first build a series of conceptual models that define the cybersecurity domain at a variety of levels, from simplistic to complex. A conceptual model provides a simplified abstraction of the real world. At a basic level, a conceptual model must describe the simulation content in four areas: entities, environment, events and interactions, and modeling approaches.

A simple conceptual model that shows internet threats, firewalls, and enterprise networks would lead one to believe that a very straightforward Internet Protocol (IP) based model would be sufficient to capture the interactions between cyber simulations. After all, most people are familiar with the majority of cyber attacks that are transmitted via email. However, further investigation into the case study presented above reveals that many other cyber threats such as Stuxnet (a cyber worm that targets critical infrastructure components) can be easily transmitted via physical means such as a USB drive, CD, or SD card, and can communicate with servers in other parts of the world with complex command and control protocols. In addition, mobile devices often interact with enterprise networks using non-IP based protocols. A more complete representative conceptual model of cyberspace is shown in Figure 6. So far, our modeling

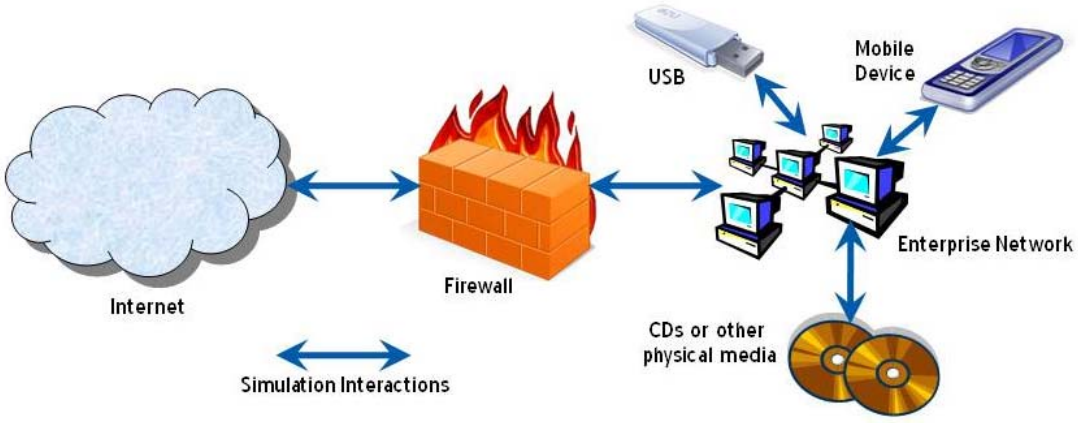

Figure 6. A Conceptual Model of Cyber Entities and Interactions

and simulation interoperability standard for cybersecurity must contain some pieces of information from the Internet Layer of the Internet Protocol Suite (to address the left half of the conceptual model), and the Physical Layer of the OSI Model (to cover the right half of the conceptual model). However this still does not accurately characterize the necessary interactions required to describe cyber threats and their interactions once they are inside the Enterprise Network. The Enterprise Network is often made up of various servers, desktops, routers, and switches that are all running different operating systems, virus software, databases and other applications, not to mention a variety of patches that may or may not be up to date. To fully define this next level, we need to describe the data and application layers from Figure 1 in more detail, including information about classification, identity, rights management, and data in use protection. At first glance, the result from the conceptual modeling effort seems to yield a somewhat uneven top level organization of an interoperability standard (Figure 7), requiring stakeholders from a variety of communities to work together to develop and integrate the details of the standard. However, upon further review, the applications and data layer is the cyber equivalent of the DIS Entity State PDU, and the other layers represent the necessary communications with the environment and external threats and devices. This construct would allow the greatest flexibility in developing both internal and external network models that can interoperate with each other, instead of developing clumsy workarounds that describe the state of the device in an IP format.

Further development of the standard could be led by the Simulation Interoperability Standards Organization (SISO), or NIST, as recommended in the recent congressional language. Potential contributors to the standard are experts in the critical elements from leading companies like OPNET, CISCO, IBM, and Microsoft, as well as Internet Service Providers and leading integrators in the Defense Industrial Base. A simple balloting process could be used as a draft standard is developed and released for use in the open market. This would allow users of the ABMS open source tools, OPNET simulations and interoperability frameworks to pilot the interoperation between simulations.

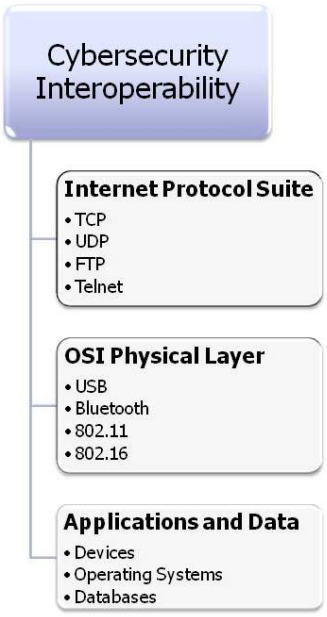

Figure 7. Top Level Standard Organization

Summary

It is clear that there is much more work to be done to develop a comprehensive modeling and simulation interoperability standard for cybersecurity. The technical aspects of the cybersecurity field are still emerging, coursework at major universities is still being developed, and simulation models are in their infancy. A top level interoperability organization has been proposed, based on preliminary conceptual models and a solid understanding of today's threats and networks. It is hoped that the industry will pick up from this staring point and continue the development, because the cyber threat continues to threaten our networks, our infrastructure, and our lives.

References

[1] Memorandum for the Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, "Joint Terminology for Cyberspace Operations". Vice Chairman of the Joint Chiefs of Staff, General James Cartwright. November 2010.

[2] http://www.af.mil/news/story.asp?id=123226840, Deputy Defense Secretary William Lynn III, 18 October 2010.

[3] Cyber Assessment, Market, and Budgets, The Goyak Group, June 2011.

[4] http://www.sans.org/critical-security-controls/guidelines.php

[5] Recommended Security Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 3, May 2010.

[6] Memorandum for Chairman, Defense Science Board, Terms of Reference – Defense Science Board (DSB) Task Force on Resilient Military Systems, 16 May 2011.

[7] House Resolution 2096, the Cyber Security Enhancement Act of 2011, put forward on 1 June 2011.

[8] Lyons, Barry. Applying a Holistic Defense-in-Depth Approach to The Cloud, SANS Cyber Defense Initiative 2010, Northrop Grumman, 14 December 2010.

[9] OPNET Modeler/Release 16.0, Modeling Overview. OPNET Technologies, Inc.

[10] IEEE Standard 1278.1a-1995. Distributed Interactive Simulation—Application Protocols. Distributed Interactive Simulation Committee of the IEEE Computer Society, Approved 19 March 1998.

[11] IEEE Standard 1278.2-1995. Distributed Interactive Simulation—Communications Services and Profiles. Distributed Interactive Simulation Committee of the IEEE Computer Society, Approved 21 September 1995.

[12] IEEE Standard 1516-2010. IEEE Standard for Modeling and Simulation (M&S) High Level Architecture – Framework and Rules. IEEE Computer Society, 18 August 2010.

[13] Introduction to Agent-based Modeling and Simulation, Charles M. Macal and Michael J. North, Argonne National Laboratory, 29 November 2006.

[14] Tutorial on agent-based modelling and simulation, C.M. Macal and M.J. North, Journal of Simulation, 2010.

[15] A Roadmap of Agent Research and Development, Nicholas R. Jennings, Katia Sycara, Michael Wooldridge, Autonomous Agents and Multi-Agent Systems, 1, 275–306 (1998).

[16] Agent-Based Modeling and Simulation, C.M. Macal and M.J. North, Proceedings of the 2009 Winter Simulation Conference.

[17] The C2 Wind Tunnel, https://wiki.isis.vanderbilt.edu/c2w/

[18] Haimes YY, Jiang P. Leontiff-based model of risk in complex interconnected infrastructure. Journal of Infrastructure System 2001;7:1–12.

[19] Apostolakis GE, Lemon DM. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Analysis 2005;25:361–76.

[20] Setola R, De Porcellinis S, Sforna M. Critical infrastructure dependency assessment using the input-output inoperability model. International Journal of Critical Infrastructure Protection 2009; 2:170–8.

[21] W.J. Tolone, D. Wilson, A. Raja, W. Xiang, H. Hao, S. Phelps, and E.W. Johnson, "Critical Infrastructure Integration Modeling and Simulation", in Proc. ISI, 2004, pp.214-225.

[22] Critical Infrastructure Resiliency Simulation (CIPR/sim), http://www.inl.gov/research/critical-infrastructure-resiliency-simulation/