Methodology for Analyzing the Compromise of a Deployed Tactical Network

Brian C. Asman, Michael H. Kim, Ryan A. Moschitto, James C. Stauffer, and Samuel H. Huddleston

Abstract—**As the Department of Defense transitions to a ubiquitous computing environment, our military operations become increasingly vulnerable to compromise via cyber attacks at echelons as low as the Brigade Combat Team (BCT). There is a need to *design a system to facilitate the analysis of a nation state's ability to compromise the confidentiality, availability, and integrity of a deployed tactical network.* Research demonstrated that, on these networks, compromises due to security protocols violated by humans are much more common than compromises due to technological vulnerabilities. Therefore, this analysis focuses on developing a simulation modeling approach to analyze the effectiveness of security protocols "within the fortress" and to track the damage done by various forms of cyber attacks that have successfully breached the network perimeter. Our network model uses agent-based simulation in order to model the flow of information at the packet level with dictated behavior specific to the agents modeled: individual network packets, computer systems, routers, servers, and files. The advantage to using an agent-based, rather than a discrete-event, simulation model in this situation is that agent-based models focus on the relationship between entities from the bottom-up, such as at the network packet level, rather than the entire system from the top-down. The developed simulation model allows us to simulate various network attacks, observe their interaction with network security protocols, assess the resulting damage in terms of the network's availability, and quantify the damage in terms of sensitive information lost.**

I. Introduction

DUE to the advantage that the U.S. Military enjoys over foreign powers in the realm of technological and operational superiority, many of those powers have refocused their efforts in the cyber realm to create an asymmetric battlefield across the expanse of the digital arena. The National Infrastructure Protection Center (NIPC) defines cyber terrorism as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies" [1]. Related closely with cyber terrorism is the concept of information warfare, which also encompasses physical attacks on computer facilities and communication infrastructure such as transmission lines and satellite arrays.

As the Department of Defense (DOD) transitions to a ubiquitous computing environment, our military operations become increasingly vulnerable to compromise via cyber and information attacks at echelons as low as the Brigade Combat Team (BCT). Even though technological innovation and security/identity management are priorities, and military personnel are required to pass annual training, our networks are still often vulnerable. In the cyber game, the player with the most speed and agility will almost undoubtedly prevail, while the one who practices *fortress warfare*, or placing "increased efforts into blocking malicious software and codes entering military networks…and decreasing the number of gateways to be protected [2]", has little chance of success [3]. Success will only be achieved by preparing for inevitable network compromises.

Given the impact of attacks on our cyber assets discussed above, it behooves the DOD to develop the best possible approach for anticipating the effects of cyber attacks on its systems. One cost effective approach for developing this analysis is the use of simulation models to predict the effectiveness of security policies and assessment of outcomes for various types of attacks on the US cyber networks. This paper provides a methodological approach for assessing the damage from several types of cyber attacks and a simulation model developed to analyze how well various security protocols and network configurations immunize networks against those attacks.

II. Requirements Analysis

A. Problem Analysis

The purpose for this research was to *design a system to facilitate the analysis of a nation state's ability to compromise the confidentiality, availability, and integrity of a tactical network.*

For the purposes of this study, we use the following definitions for the three considered types of cyber attack:

- *Confidentiality Attack* – An agent obtains access inside a network, locates targeted network files on servers or computers and copies those files.
- *Integrity Attack* – An agent locates files on a network and changes the information in them.
- *Availability Attack* – An agent identifies key nodes (network routers or links) on a network and shuts down or denies service to them.

Manuscript received April 4, 2011.

All authors are with the United States Military Academy Department of Systems Engineering, West Point, NY 10996 USA (phone: 845-938-2701; e-mail: Brian.Asman@us.army.mil, Michael.Kim14@us.army.mil, Ryan.Moschitto@us.army.mil , James.C.Stauffer@us.army.mil, Samuel.Huddleston@usma.edu).

Example approaches for confidentiality attacks include: hardware compromises, portable drive infiltrations, and injections of viruses that forward information onto network systems. One key goal in this approach is the ability to send files below the network's detection threshold, allowing attackers to receive numerous files over time. Integrity attacks are similar, but involve altering target files by a worm or virus that implements random (or controlled) shifts to the information stored on the network. When these changes are undetected, critical operational decisions may be based on inaccurate information.

Availability attacks deny the use of a network by attacking critical nodes of the network, such as the use of malicious worms that are capable of crashing multiple routers at the same time. Recently, an international worm known as Stuxnet was speculated by news organizations to be a complex computer worm designed to infect an Iranian nuclear plant staffs' computers in hopes of preventing its use [4]. Another approach is a denial of service attack, which is achieved through an overflow of legitimate requests that overwhelm and freeze the network, and the use of Botnets, which allow one user to control a large number of hosts or "bots" to make the requests [5].

B. *Tactical Network Functional Analysis*

The fundamental objective of a BCT's network is to facilitate the effective communication, coordination, and data sharing necessary for the tactical, operational, and strategic success of the BDE and its subordinate units. A BCT's network has four primary functions: provide communication, provide information, provide situational awareness and command and control (C2), and provide logistical support. Each of these functions have integrated systems that provide that functionality:

Provide Communication

- *Voice Over Internet Protocol (VOIP)* – Phones
- *Microsoft Internet Exchange* – Email Service

Provide Information

- *Microsoft SharePoint Servers* – Data Sharing
- *All-Source Analysis System (ASAS)* – An automated system to gather and analyze intelligence.

Provide Situational Awareness, Command, and Control (C2)

- *Blue Force Tracker (BFT) and Force XXI Battle Command, Brigade and Below (FBCB2)* – Systems which provide real-time information on the location of friendly units to commanders in the field.
- *Aviation Mission Planning System (AMPS)* – Coordinate aviation assets to assist military forces on the ground.
- *Advance Field Artillery Targeting and Direction System (AFATADS)* – Coordinate field artillery assets to assist forces on the ground.

Provide Logistical Support

- *Integrated Systems Control (ISYSCON)* – An automated system to manage logistics-related requests.

A BCT's network also has three primary security functions to maintain: *confidentiality*, *integrity*, and *availability*. A functional analysis of the security systems is displayed in Fig. 1 below.

Fundamental Objective: Protect Tactical Network

Functions	Maintain Confidentiality	Maintain Integrity	Maintain Network Availability
Objective	Minimize Copied Files	Minimize Corrupted Files	Maximize Speed
Measure	Total Network Damage, *Ti* (Eq. 2)	Total Network Damage, *Ti* (Eq. 2)	Bandwidth Available (bitrate)
Objective			Maximize Connectivity
Measure			Connectivity to Nodes (Eq. 3) or Information (Eq. 4)
Objective			Maximize Network Redundancy
Measure			Network Density, *d* (Eq. 5)

Fig. 1. The Functional Analysis of Network Security. This figure shows the fundamental objective of protecting a BCT's network with three primary functions, their respective objectives, and the performance measures developed to assess the performance within each objective.

As hypothetically illustrated in Fig. 2 below, a tactical network has sub-unit clusters that have a router (such as those for each battalion (BN) below) with six client servers – each client is one of the six essential components of a network. The battalions communicate laterally with one another and vertically to their higher brigade (BDE) headquarters through two avenues: a Joint Node Network (JNN) and a Command Post Node (CPN). The JNN communicates via satellite link, while the CPN communicates via line of sight radio. For the sake of redundancy, the BN and BDE networks can communicate with each other via CPN as well. Suppose a personnel request made on the BN ISYSCON network needs to go up to the BDE level. The request would travel from the ISYSCON client server through the BN router to the BDE router via the CPN or JNN. The request would then travel through the BDE router to be received by the ISYSCON client server [6]. Any developed simulation model would need to mimic the network topology, structure, and function of the network illustrated in Fig. 1.

In addition, a simulation model would also need to account for security measures such as intrusion detection systems. There are two types of systems – Network-based Intrusion Detection (NID) and Host-based Intrusion Detection (HID). NID systems constantly scan the network traffic to detect abnormalities or threats and issue alerts to the administrators and possibly block a suspected connection. This system significantly degrades network functionality. HID systems are located on the host computers and scan their own respective computer on a network and only send an alert to the administrator once an abnormality or threat has been identified. This system minimally affects network functionality as the network administrator is notified only after the host finds its own irregularity [7].

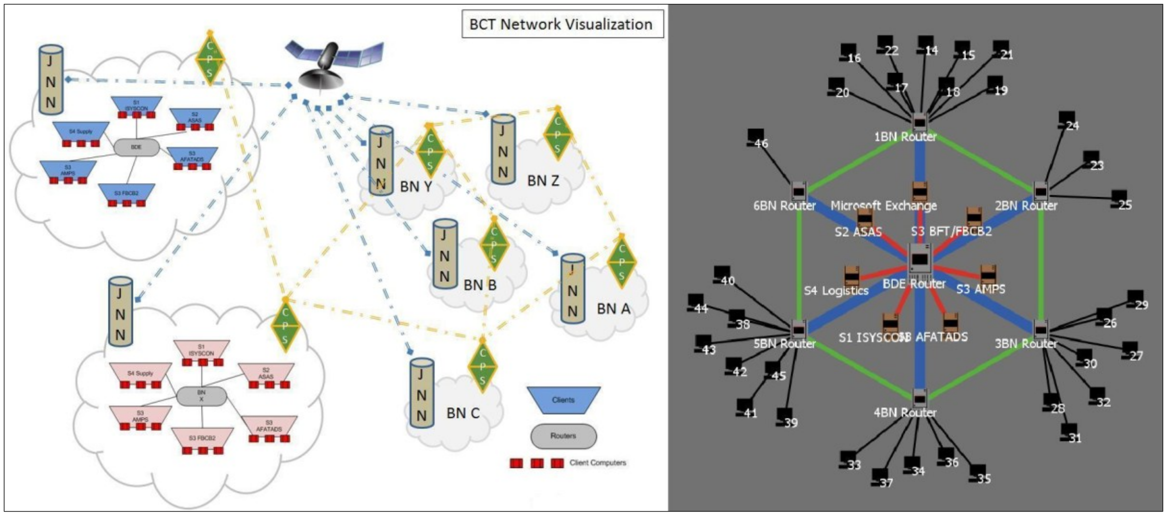

Fig. 2. The figure above depicts the hypothetical topology and structure of a Brigade's (BDE) tactical network (left), and a view of the developed simulation model in a limited mesh hybrid configuration (right). The centrally located router is linked to both specific integrated system servers (ASAS, FBCB2, AMPS, etc.) and battalion (BN) routers. The battalion routers are also linked to adjacent battalion nodes. The width of the links denotes the bandwidth of that connection and the speed with which packets can travel. Blue links between routers represent a satellite link via Joint Node Networks (JNN) and green links represent a line-of-sight communications link between routers via Command Post Nodes (CPN).

There is an inherent tradeoff between the network's ability to detect threats and the network's functionality. The network has a certain threshold, for example, a minimum network load (in files etc.) that a user demands, before an alert is raised to the network administrator that a potential security problem is occurring. If the threshold is set too low, then the network's functionality will decrease due to the increased scanning, alerts will trigger unnecessary investigations, and resources will be wasted. However, if the threshold is set too high, the network will have very good functionality, but large numbers of files will be compromised before an intruder is even detected.

III. Methodology

As previously stated, the three principle variations of cyber attacks studied are those affecting the *confidentiality*, *integrity*, or *availability* of a network or networks. Each variation of attack must be modeled and scored differently in order to most effectively represent the reality of an intruding agent accessing a network and assessing the damage to the network incurred. Our methodology considers both the information on the network and the physical state of the network in terms of remaining connectivity in assessing the damage due to cyber attacks.

A. *Modeling the Value of a Network's Information Loss*

For the purposes of our model, the contributing factors to the measure of overall damage incurred during a confidentiality attack on a tactical network are the type and number of files compromised. Table I provides an example of six files types commonly found on a network along with an example assessment of their value.

The primary measureable quantity from our model will be the count of *unique* files compromised – C_i, as in a network there are often many copies of a file present. Compromise of any one copy of a file represents the compromise of the information contained in the file. The two other numerical values of importance are the total number of unique files of type i– A_i and the file type value weight – W_i, with i as the index for file-type. As both of these measures are designed to fit the specific requirements of any network the model is applied to, the weights of these values are assumed in this paper and can be changed very easily to account for the requirements of any network.

How the files are stored contributes significantly to the degree to which a compromise would affect a network, as the storage medium determines the accessibility of unique files of the same type to a single instance of network intrusion. Equation (1) is used to calculate the % loss in each file-type, F_i.

$$F_i = \left(\frac{C_i}{A_i} \right) \tag{1}$$

For instance, hypothetically, if all SIGACTS reports were stored on a single database file ($A_{SIGACTS}$ = 1) and that unique file was compromised ($C_{SIGACTS}$ = 1), the file type loss would be 100% for SIGACTS. Conversely, if a compromised email server contained many unique files (A_{email} = 10,000) and half the unique files were compromised (C_{email} = 5,000), the file type loss would be 50% for email.

Each type of file susceptible to compromise by an attack is assigned a different weight depending on the file type. In the hypothetical example depicted in Table I below, SIGACTS is most heavily weighted because if compromised and revealed to the public, it could result in a public relations challenge. The respective weights for each of the file types would depend upon an individual unit commander's preference and could be elicited using any of the many available value weight elicitation approaches, such as pair wise comparison or a swing-weight matrix [8].

The total network damage, *T*, is calculated by weighting and summing the damage of each respective file type to arrive at the network's collective damage, represented as a percentage as in Equation (2).

$$T = \sum_{i=1}^{n} (F_i \times W_i) \tag{2}$$

As shown in Table I, the application of both these equations in order to value a network's information loss results in 68% total network damage for this abstract example.

TABLE I
NETWORK DAMAGE

File-Type	C_i	A_i	F_i	W_i	T_i
SIGACTS	1	1	100%	40%	40%
Maps & Graphics	400	500	80%	20%	16%
Orders	6	30	20%	20%	4%
Email	5,000	10,000	50%	10%	5%
INTEL Reports	100	200	50%	6%	3%
C2 Files	0	1	0%	4 %	0%
			Σ	100%	**68%**

B. Modeling the Value of a Network's Performance

For modeling network performance, we considered the speed and connectivity of the network under attack. Network speed (in bit rate) is one measure which is constantly monitored by virtually every network administrator, and is considered self-explanatory. For our other measures of network performance, network graph theory provides a framework for analyzing the performance of a network based upon its topology and connectivity. The *star topology* in Fig. 3 has each node connected to a central hub, where those connections are point to point, and the hub is the critical point of failure [9]. In contrast, the *mesh topology* provides redundant paths between nodes that can be partially or fully connected and there is not a particular critical point of failure [10].

As seen if Fig. 2, a tactical network is often a hybrid of these two topologies. In this figure, each battalion has a star network. This gives the central router connecting each of the clients (ISYSCON, ASAS etc…) on the battalion network a much greater weight than the client nodes themselves with respect to connectivity because if the central router is disabled then that battalion network is disabled. In contrast, the battalions and the higher headquarters communicate in a mesh network consisting of satellite and radio links labeled as the CPN and JNN.

Network graph theory measures provide a convenient way to assess how well connected a network is currently and how robust it is to further attack (i.e. how much redundancy still exists). For our first measure, we acknowledge that our network initially functions at 100% connectivity, meaning all nodes are connected. As an availability attack commences, a subgroup of nodes can lose connection from the network. We call the two separated groups in a network *components* [11]. In order to measure the *connectivity* of the divided network, we divide the size of the larger component, k_L, by the total number of nodes in the network as shown below in Equation (3).

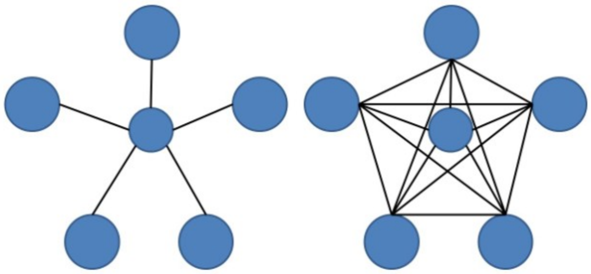

Fig. 3. This figure illustrates network topologies. The figure on the left depicts a *star topology*, in which the central node is the most critical for the network. The figure on the right illustrates the redundant connections between nodes in a *mesh topology*, in which all nodes conect to each other.

$$Connectivity = \frac{k_L}{g} \tag{3}$$

Using as an example a tactical network with 131 nodes; if an attack causes a battalion with 10 computers to lose connection from the rest of the network, the remaining brigade network is the larger component with 120 nodes while the smaller component only has 11 nodes (keeping in mind the battalion router is also a node). Therefore, the network connectivity is $\frac{120}{131} \times 100 = 91.6\%$. Furthermore, we can also calculate the value of information available, *V*, using the ratio between information value available in the larger component and the sum of information value in all components (which is by definition 100%). The value of the information available is calculated using the weighting approach discussed in the previous section.

$$V = \frac{value\ of\ information\ available}{value\ of\ all\ information} \tag{4}$$

In order to determine how robust a network is to future attacks, we measure the density, *d*, of the network [11]. This measure is a comparison between the number of links present in a network, *L,* and the total number of possible links, given by $\frac{g(g-1)}{2}$, with *g* representing the number of nodes in the network. The equation to find the density of our network is Equation (5):

$$d = \frac{2L}{g(g-1)} \tag{5}$$

As an example, we can compare the star and mesh topologies illustrated in Fig. 3. We find the density of the mesh network to be $\frac{2\times15}{6(6-1)} = \frac{30}{30} = 1$ or 100%. As can be seen, losing any single link will not affect the connectivity of the network, although it will reduce the systems redundancy (weakening the network to future attack). In contrast, the star topology has a density of $\frac{2\times5}{6(6-1)} = \frac{10}{30} = .33$ or 33%. The star network's 33% density is much more vulnerable to capability loss - every destroyed link will reduce the network's connectivity.

C. *Simulation Modeling of a Network*

To create our model, three different simulation software systems were considered: OPNET, NS3 and NETLOGO. OPNET [12] and NS3 [13], are discrete model simulators and are not preferred due to their inability to model behaviors of independent data packets. In comparison, the multi-agent based simulator, NETLOGO [14], provides the necessary functionality for modeling the behavior of an independent agent such as a virus on a network, or more importantly, the ability to track specific agents (such as files and packets) and their status as they move throughout a network. It is also the most user-friendly software of the three, as it contains a large library of sample models such as an example model demonstrating the spread of a virus on a network [15].

Our network model uses agent-based simulation in order to model the flow of information at the packet level with dictated behavior specific to an individual agent or group of agents. The advantage to using an agent-based, rather than a discrete-event, simulation model in this situation is that agent-based models focus on the relationship between entities from the bottom-up (such as at the packet level), rather than the entire system from the top-down. These agents are also autonomous, which allows for the assignment of simple rules to each agent set. With these rules, the agents can operate devoid of the need of an internal event queue, the foundation of discrete-event simulation, to dictate their behavior and can rely solely on their rule set and cognizance of pertinent information in order to perform an action at an instantaneous moment within the model [16]. The simulation models the following *agent set*s and properties:

- *Computers/Servers* – Occupy physical space on the network as nodes and have hard drives on which files are stored.
- *Hard drives* – Exist under the physical representation of computers and servers. They facilitate the propagation and storage of files.
- *Files* – Information stored on hard drives (which exist on computers and servers). Vary in type and size.
- *Packets* – Formatted data subunit into which files are broken down at origin nodes for network travel and then reassembled from at destination.
- *Links* – Pathways through which network travel of packets occurs.
- *Routers* – Intermediate points along a packet's route of travel along a network path that directs them towards their destination nodes.

Organic to the simulation model is an interface allowing the user to create a network in one of three configurations, attack that network, and monitor network statistics throughout the course of a simulation run. Specific functions include:

- Network *Topology* Selection – Complete Hybrid (Mesh), Limited Hybrid (Mesh), or Star
- Network Structure/Functionality Options – Number of Computers per Router, Network Traffic Load, & Server Exchange Rates
- An interface to allow the user to launch confidentiality attacks within the network. Efforts to create an interface for user-controlled integrity attacks are underway.
- The ability for the user to dynamically destroy specific network entities (such as nodes, routers, servers, or links) during a simulation run in order to model an availability attack.
- Monitoring graphics, such as depicted in Fig. 4, which allow the user to view and assess traffic as a network administrator would.

IV. RESULTS

The resulting simulation provides the opportunity to test how various network configurations, topologies, and security protocols respond to cyber attacks launched from within the network. One example of such an attack is the confidentiality attack known as the WikiLeaks scandal, during which Army Private First Class Bradley Manning was charged with copying "more than 250,000 diplomatic cables between March 28 and May 4, 2010" from restricted computer systems [17].

The simulation model creates an environment for user-controlled confidentiality attacks within the network through an interface that allows the user to access and download information stored on various locations throughout the network. The established network monitoring protocols automatically track and record traffic flow across all links. Fig. 4 below graphically represents the load across various links to specific nodes. Through detailed monitoring throughout the progression of a simulation run, it is possible to identify nodes with an abnormally large amount of traffic being routed to them. A traffic level that exceeds a normal threshold is indicative that a certain node could be perpetrating a confidentiality attack (or could indicate a user with a legitimate need for a large amount of information).

Unfortunately, the signal that corresponds with the attacking computer also shows that some volume of information has already been lost. The simulation can track the different types of files that were compromised and then calculate the resulting value loss using Equation (2). An example of such a calculation is provided in Table I, in which there was a 68% network loss. This model allows the user to test security thresholds in order to determine the ideal tradeoff between network security and network usability (due to false alarms, etc).

We can also simulate an availability attack through the user interface which allows links, routers, and computers on the network to be destroyed dynamically as the simulation

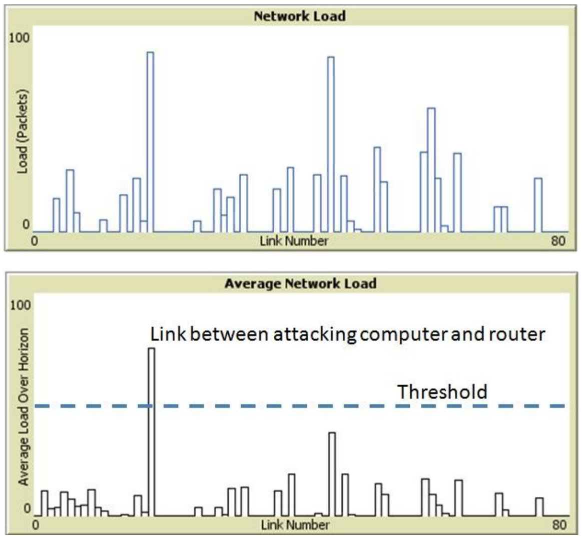

Fig. 4. Traffic monitors during a confidentiality attack. Link 17 shows *current traffic* that is within the range of other observed network traffic signals. However, *average traffic* over this link is much higher than all other computers and is much higher than the threshold for unusual activity. In a similar manner, thresholds can also be added to the current network load monitor (on top) to illustrate the maximum carrying capacity of the network, providing an opportunity to identify when the network is becoming overloaded.

progresses. Referencing Fig. 2, suppose that during an availability attack, the central router (JNN satellite link) was destroyed. One can see that, in this configuration, all information stored on the Brigade C2 servers becomes immediately unavailable (a dramatic loss in *V*, information value, ensues) but that the majority of the unit is still connected as a large *component*. In this case, the battalions can still communicate, but only by using lower-bandwidth CPN links (shown as green links in Fig. 2). The network monitors, such as those in Fig. 4, illustrate the corresponding shift in traffic to the lower bandwidth links. Using the value methodology discussed previously, the simulation model dynamically tracks:

- How much of the network is connected (Eq. 3)
- How much information value is still available on the network (Eq. 4)
- If the network is currently overloaded (Fig. 4)
- How vulnerable the remaining network is to future attack (Eq. 5)

This model therefore provides the opportunity to test the robustness of a configuration for a particular tactical network under various forms of attack prior to expending resources in building it.

V. Future Work

Future development of the model will include the integration of viruses and worms that have the ability to propagate through the network. Currently, network attacks are simulated by a human user interacting with the simulation model to launch attacks. An enhanced user interface to implement attacks and make further changes to organization-specific network topologies and security protocols will also be added. In order to provide a more detailed analysis of the user-defined security protocols, a HID system will also be created to complement the already established NID system within the model.

The last development for this simulation would be the validation of the model within a client's propriety environment. We have not yet validated the model to a specific military network as proprietary information on bandwidth, specific security protocols, and system performances are controlled for security purposes. Rather, this model provides a methodological approach and general template which could be easily adapted to a specific network's topology, structure, bandwidth, and security protocols using the provided simulation model user interface.

References

[1] Wilson, C. "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress." *CRS Report for Congress*. (2003) http://www.fas.org/irp/crs/RL32114.pdf

[2] Gady, Franz-Stefan. "The Cyber Fortress Mentality." *Foreign Policy Journal,* (2010) http://www.foreignpolicyjournal.com/2010/11/25/the-cyber-fortress-mentality/

[3] Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." *Center for Strategic & International Studies*. (2002) http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

[4] BBC News. "Stuxnet worm hits Iran nuclear plant staff computers" (2010) http://www.bbc.co.uk/news/world-middle-east-11414483 (accessed December 2, 2010)

[5] Kristoff John. *Botnets*. Evanston, IL. http://www.nanog.org/meetings/nanog32/presentations/kristoff.pdf (accessed December 2, 2010)

[6] FM 6-02.60. Tactics, Techniques, and Procedures for the Joint Node Network. Department of the Army, 2006.

[7] Windows Security. "IDS Part 1". http://www.windowsecurity.com/articles/Intrusion_Detection_Systems_IDS_Part_I__network_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture.html

[8] Parnell Gregory S, Driscoll Patrick J, Henderson Dale L. (2008). *Decision Making in Systems Engineering and Management*. Hoboken, NJ.

[9] ComputerHope. "Star Topology". http://www.computerhope.com/jargon/s/startopo.htm

[10] ComputerHope. "Mesh Topology". http://www.computerhope.com/jargon/m/mesh.htm

[11] Faust, Katherine and Wasserman, Stanley. "Social Network Analysis Methods and Applications." (1994)

[12] "KeyFeatures" http://www.opnet.com/solutions/network_rd/modeler.html (accessed December 2, 2010

[13] "What is NS-3?" http://www.nsnam.org/docs/ns-3-overview.pdf (accessed December 2, 2010)

[14] Wilensky, U. (1999). NetLogo http://ccl.northwestern.edu/netlogo/ Center for Connected Learning and Computer-Based Modeling. Northwestern University, Evanston, IL. (accessed December 2, 2010)

[15] Stonedahl, F. and Wilensky, U. (2008). NetLogo Virus on a Network Model. http://ccl.northwestern.edu/netlogo/models/VirusonaNetwork. Center for Connected Learning and Computer-Based Modeling. Northwestern University, Evanston, IL.

[16] Learmonth, G.P. "Chapter 2: Agent Based Modeling and Simulation." *Lecture Notes for Systems 681: Modeling and Simulation of Complex Systems.* University of Virginia. (Fall 2007).

[17] Savage, Charlie. "Soldier Faces 22 New WikiLeaks Charges." *The New York Times*. (2011) http://www.nytimes.com/2011/03/03/us/03manning.html