Proceedings of the 2011 Winter Simulation Conference
S. Jain, R.R. Creasey, J. Himmelspach, K.P. White, and M. Fu, eds.

MODELING CYBER ATTACKS AND THEIR EFFECTS ON DECISION PROCESS

Erdal Cayirci

University of Stavanger
Electrical Engineering & Computer Science Dep.
Stavanger, 4036, NORWAY

Reyhaneh Ghergherehchi

University of Stavanger
Electrical Engineering & Computer Science Dep.
Stavanger, 4036, NORWAY

ABSTRACT

Cyber attacks are designed to affect human behavior by creating confusion and information overload. Although cyber attacks mainly aim to stimulate irrational behavior, there is limited work in the literature on modeling their human behavior effects. Instead most of the studies are focused on the simulation of attacks and technical solutions or counter measures to prevent, detect and recover from an attack. Taxonomies for attacks, attackers and human behavior effects of cyber attacks are provided, and the relation between cyber attacks and decision making process are modeled. Live simulation techniques for stimulating the expected behavior, specifically effects of cyber attacks on decision making are presented.

1 INTRODUCTION

Contemporary decision making process for most individuals and organizations depend on online information. Furthermore, the professional, individual and social life of many ordinary people is tied to networks and the information available in them. The infrastructure for these networks is typically the Internet. This much dependency to an open information source creates new opportunities for adversaries. Cyber incidents, where adversaries influence or control the communications and information systems for creating human behavior effect in their favor, have become common. Typically malwares, such as viruses, worms, trojan horses and botnets are used for attacking on:

- Availability: To reduce communications/computation capacity or to prevent the availability of information and communication systems
- Confidentiality: To compromise confidential information
- Privacy: To obtain detailed information about individuals and organizations
- Integrity: To create uncertainty about information

Cyber attacks and counter measures have been studied in the literature extensively for decades (Kotenko 2005, Stytz and Banks 2010). Numerous modeling and simulation tools are also available (OMNeT++ Community 2010, Cayirci and Marincic 2009) for simulating cyber attacks and counter measures. However, neither modeling and simulation nor training researchers have addressed human behavior effect of cyber attacks and their consequences enough.

Cyber attacks may create a situation worse than the time before the information age because decision makers under cyber attacks do not only tackle with the challenge of lack of information but also lose their trust of the available information under cyber attack. The implications and consequences of this phenomenon are serious. Therefore, practical solutions and procedures against it should be developed, tested and trained, which requires effective simulation tools and techniques.

In this paper we aim to relate cyber attacks and their human behavior effects systematically. Moreover, we present examples for practical techniques that can be used in training events to stimulate human behavior effect of cyber attacks. In Section 2, a taxonomy about cyber attacks and attackers is provided. The decision making process and its relations with cyber attacks are modeled in Section 3. Examples for simulating the effects of cyber attacks on decision making during operational and higher level exercises are introduced in Section 4. We conclude our paper in Section 5.

2 CYBER ATTACKS AND ATTACKERS

Security attacks can be categorized into two broad classes: passive and active attacks. Passive attacks, where adversaries do not make any emission, are mainly against data confidentiality. In active attacks malicious acts are carried out not only against data confidentiality but also integrity. Active attacks can also aim at unauthorized access and usage of the resources or the disturbance of the opponent's communications. An active attacker makes emission or an action that can be detected.

2.1 Passive Attacks

In passive attacks attackers are typically camouflaged, i.e., hidden, and tap the communication lines to collect data. Passive attacks can be grouped as eavesdropping and traffic analysis. Classified data can be eavesdropped by tapping the communication lines. Especially when the known protocols are used, and plain data (i.e., not encrypted) are transferred, an adversary can easily eavesdrop.

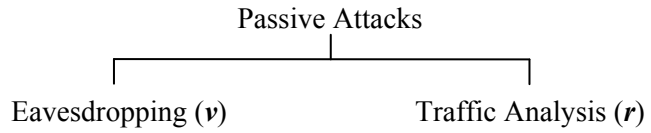

Figure 1: Passive attacks

Not only the content of data packets but also the traffic patterns may be very valuable for adversaries. For example, important information about the networking topology can be derived by analyzing the traffic patterns. Traffic analysis can also be used to organize attacks against anonymity. Adversaries can aim to detect the source of certain data packets, which may help localizing events and determining the weaknesses, capabilities, functions and owners of transferred data. Moreover, traffic patterns can pertain to the other confidential information such as the actions and the intentions.

2.2 Active Attacks

In an active attack an adversary actually affects the operations in the attacked network/information system. This effect may be the objective of the attack, and can be detected. For example, the networking services can be degraded or terminated as the result of the attack. Sometimes the adversary tries to stay undetected, and aims gaining unauthorized access to system resources or threatening confidentiality and/or integrity of the content in a network. We group active attacks into four classes as shown in Figure 2.

Adversary can physically damage hardware to terminate the nodes. This is a security attack that can be considered also in the domain of fault tolerance, which is the ability to sustain networking functionalities without any interruption due to node failures. When nodes are unattended and can be reached physically by the adversary, they can be attacked by tampering techniques, such as, microprobing, laser cutting, focused ion-beam manipulation, glitch attacks and power analysis (Cayirci and Rong 2009). Node tampering can help much in masquerading and denial of service attacks. Electromagnetic pulse (EMP) attacks are also among the threats that can be listed within physical security attacks. EMP is a short duration burst

of high intensity electromagnetic energy that can produce voltage surges, which can damage electronic devices within its range.

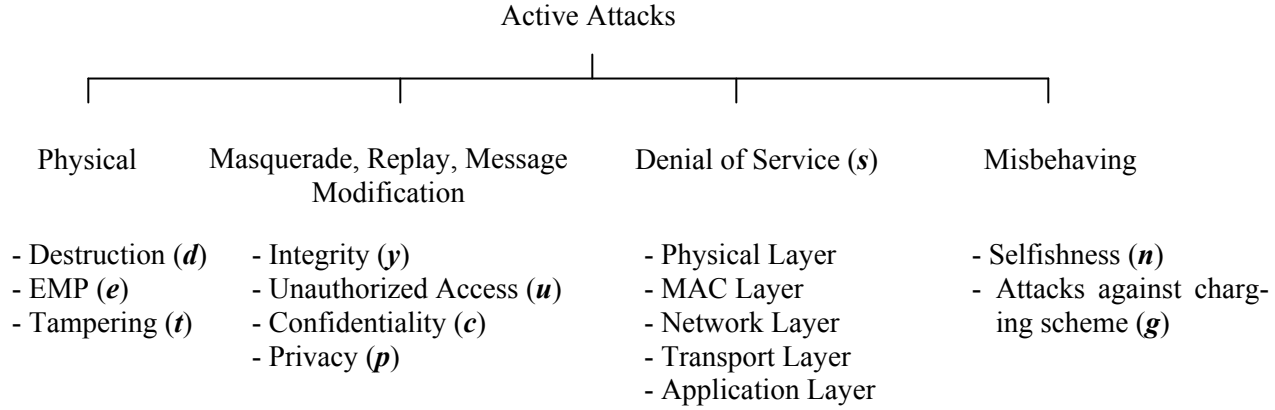

Figure 2: Active attacks

A masquerading node impersonates another node. Messages can be captured and replayed by the masquerading node. Finally, the content of the captured messages can be modified before being replayed. Various scenarios and threats can be developed based on these approaches. An adversary can masquerade for phishing, which means deceiving someone to make him/her give confidential information voluntarily. A malicious node that masquerades an authorized node can ask another node to give information about the passwords, keys, etc.

A Denial of Service (DoS) attack is mainly against the availability of network services. A DoS is defined as any event that diminishes network capacity to perform its expected function correctly or in a timely manner. A DoS attack is characterized by the following properties: malicious, disruptive and asymmetric. A DoS attack can be organized at any networking protocol layer (i.e., physical, MAC, network, transport and application layers).

Finally, misbehaving can also count as a cyber threat. A user of a system may misbehave to have unfair shares of the limited networking resources, i.e., selfishness. Another reason for misbehaving may be against the charging scheme not to pay for the services received.

2.3 Attackers

Similar to attacks, attackers can also be categorized according to many criteria (Cayirci and Rong 2009). Our classification of attackers is based on the characteristics shown in Figure 3: emission, location, quantity, motivation, rationality and mobility. First an attacker can be passive or active. Active attacks are carried out by active attackers, and passive attacks by passive attackers. An attacker can be an insider or an outsider. The attacker may learn all the cryptographic information owned by a compromised node when it is an insider. Therefore stealthy active attacks can be organized by the insider attackers. In other words an insider can be perceived as a legal entity inside the network. An outsider is typically not welcome to the network.

There may be a single attacker or multiple of them. When there are multiple attackers, they can collaborate with each other which can be considered as a more difficult case to defend against. An adversary carries out attacks with a motivation such as breaking confidentiality, integrity and privacy. This can be done also to gain an access to unauthorized resources. Attackers can attack also to hinder the operations of the other side. Selfishness, avoiding from payment or getting unearned rewards may be the other motivations. Needlessness, malfunctioning nodes or naïve users may also become a threat for an information system. However, needlessness is not the only reason for irrational attacks. An attacker may attack only to

attack and break a security system, and perceive this as a challenge to prove himself/herself. Therefore, some attacks are irrational where the results of these attacks may not be worth their cost. Rational attackers carry out their attacks to obtain something which is worth more than the cost of their attacks. Finally, attackers can be fixed or mobile. Detecting mobile attackers and defending against them are generally more difficult than defending against the fixed adversary.

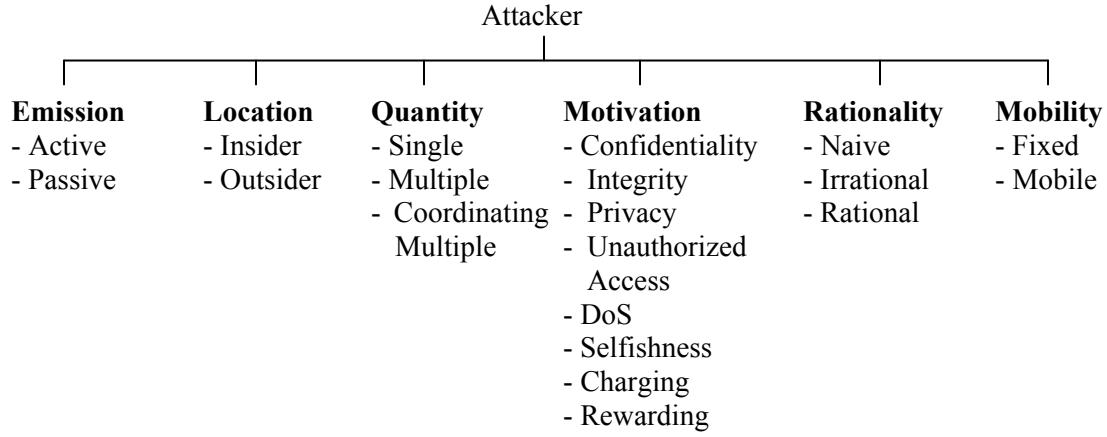

Figure 3: Classification of attackers

2.4 Malware

The tools for attacks are typically malwares. Four important classes of malware are listed below:

1. Virus: Viruses are embedded into the executable files (computer programs), and invoked when the executable is run. A virus can copy itself to other executables, and move as the executables are copied from one computer to the other. They can harm hardware and software or reduce the available capacities (i.e., fixed drive, memory, process) in the infected machines.
2. Worm: Worms are similar to viruses. The main difference between them is that worms are self propagating and self infecting, which means that they do not need to be embedded into another executable file.
3. Trojan Horse: Trojan horses are also similar to viruses. They are hidden in legitimate software, which are attractive and developed as a Trojan horse. When a Trojan horse is activated by a user, the adversary gains a point inside to organize its attacks.
4. Botnet: Botnets or bot armies are a set of more sophisticated malwares. They infect multiple machines, and coordinate their attacks started in many machines and collaborate with each other.

2.5 Human Behavior Effect of Attacks and Countermeasures

Since in this paper the human behavior effects of the cyber attacks are studied, we focus on the results of the attacks and counter measures rather than the techniques for attacking and counter measures. With this perspective, the results of the attacks can be modeled by using the following *cyber attack parameters*, which are assigned values from the unit interval of real numbers (i.e., R[0, 1]):

$\varphi_{Ii,\,k}$: The average integrity/accuracy of available information in information system (IS) i in time interval k

$\varphi_{Ci,\,k}$: The average integrity/accuracy of information transferred via communications channel (CC) i in time interval k

$\tau_{Ii,\,k}$: The average level of trust to the available information in IS i in time interval k
$\tau_{Ci,\,k}$: The average level of trust to the information transferred via CC i in time interval k
$\gamma_{Ci,\,k}$: The average availability of CC i in time interval k
$\gamma_{Ii,\,k}$: The average availability of IS i in time interval k
$\alpha_{i,\,k}$: The amount of information in IS i that needs to be transferred in time interval k
$\beta_{i,\,k}$: The capacity of CC i in time interval k

At first glance, these parameters seem to be related only integrity and availability. Since confidentiality and privacy issues effect the available communications capacities mainly because of the additional communications overhead incurred by cyber defense measures and therefore indirectly the decision making process, we do not define parameters directly related to confidentiality or privacy. However, their effects are included in parameters related to availability and trust.

Similar to the cyber attack parameters, the results of countermeasures can be modeled by using the following *cyber defense parameters*, which are also assigned values from the unit interval of real numbers (i.e., R[0, 1]):

$\mu_{Ii,\,k}$: The ratio between the detected compromised information and total compromised information in IS i in time interval k
$\mu_{Ci,\,k}$: The ratio between the detected compromised communications and total compromised communications in CC i in time interval k
$\rho_{Ii,\,k}$: The recovery level for the compromised information in IS i in time interval k
$\rho_{Ci,\,k}$: The recovery level for the compromised CC i in time interval k

The relation between the attacks and the cyber attack/defense parameters are formulized in Equations 5-14 based on an abstract network model depicted in Figure 4. Please note that the letter codes for the attacks are given in Figures 1 and 2. We do not directly relate the type of attacker with the cyber attack and defense parameters. Instead we use an abstract parameter called attack efficiency ε_a that represents the efficiency of an attacker. Similarly, we use another parameter ε_d that represents the efficiency of defender. Please note that we use Greek letters for cyber parameters, small Latin letters for the types of attacks, *f()* for "function of", and capital letters for the stages in decision making process. Please also note that the following notations are applied to all cyber attack/defense parameters:

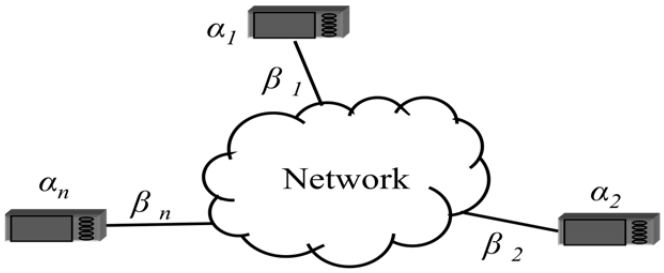

Figure 4: Network model.

$$\gamma_{Ci} = \sum_{k=1}^{z} \gamma_{Cik} \quad , \quad \gamma_{Ii} = \sum_{k=1}^{z} \gamma_{Iik} \quad , \quad \gamma_{i} = \sum_{k=1}^{z} \gamma_{Cik} + \sum_{k=1}^{z} \gamma_{Iik} \tag{1}$$

$$\gamma_{Ck} = \sum_{i=1}^{q} \gamma_{Cik} \quad , \quad \gamma_{Ik} = \sum_{i=1}^{q} \gamma_{Iik} \quad , \quad \gamma_{k} = \sum_{i=1}^{q} \gamma_{Cik} + \sum_{i=1}^{q} \gamma_{Iik} \tag{2}$$

$$\gamma_{C} = \sum_{i=1}^{q} \sum_{k=1}^{z} \gamma_{Cik} \quad , \quad \gamma_{I} = \sum_{i=1}^{q} \sum_{k=1}^{z} \gamma_{Iik} \tag{3}$$

$$\gamma = \sum_{i=1}^{q} \sum_{k=1}^{z} \gamma_{Cik} + \sum_{i=1}^{q} \sum_{k=1}^{z} \gamma_{Iik} \tag{4}$$

In Equations 1-4, q is the number of all IS or CC, and z is the total number of time intervals.

$$\mu_{Ii} \cong \varepsilon_d / \varepsilon_a \tag{5}$$

$$\mu_{Ci} \cong \varepsilon_d / \varepsilon_a \tag{6}$$

$$\rho_{Ii} \cong \varepsilon_d \cdot \mu_{Ii} \tag{7}$$

$$\rho_{Ci} \cong \varepsilon_d \cdot \mu_{Ci} \tag{8}$$

$$\varphi_{Ii} \cong \frac{1}{\varepsilon_a \cdot f(y,u,g)} \tag{9}$$

$$\varphi_{Ci} \cong \frac{1}{\varepsilon_a \cdot f(y,u)} \tag{10}$$

$$\tau_{Ii} \cong \frac{\rho_{Ii}}{\varphi_{Ii} \cdot \mu_{Ii} \cdot f(c,p,\varepsilon_d,\varepsilon_a)} \tag{11}$$

$$\tau_{Ci} \cong \frac{\rho_{Ci}}{\varphi_{Ci} \cdot \mu_{Ci} \cdot f(v,r,c,p,\varepsilon_d,\varepsilon_a)} \tag{12}$$

$$\gamma_{Ci} \cong \frac{\rho_{Ci}\tau_{Ci}}{f(d,e,t,s,n,\varepsilon_a) \cdot (1-\mu_{ci})} \tag{13}$$

$$\gamma_{Ii} \cong \frac{\rho_{Ii}\tau_{Ii}}{f(d,e,t,\varepsilon_a) \cdot (1-\mu_{Ii}) \cdot \gamma_{Ci} \cdot f(\beta_i,\rho_{Ci},\alpha_i,\rho_{Ii})} \tag{14}$$

3 MODELING THE EFFECTS OF CYBER ATTACKS ON DECISION MAKING PROCESS

Cyber attacks affect decision making process, and therefore the human/social behavior. Therefore, we focus on the decision making process and its relations with cyber attacks in this section. For decision making process (Bezerra et al. 1996; Ullman 2006), observe, orient, decide and act (OODA) loop (Brehmer 2005) is used in our model.

OODA under cyber attack is depicted in Figure 5. All decisions are based on observations of the environment. Observations provide decision makers with information about the evolving situation. That information may be obtained directly from an information source or coming from information systems where they have already been synthesized. Both cases are open to cyber attacks. Information in information systems and communication lines may be compromised. Feedback from own actions are also in-

put into the observation process. We can formalize the relation of the observation Stage O with cyber attack and defense parameters as in Equation 18, where *F* is the internal feedback from own actions, *I* is the information received from the environment and *S* is the synthesized information available in information systems:

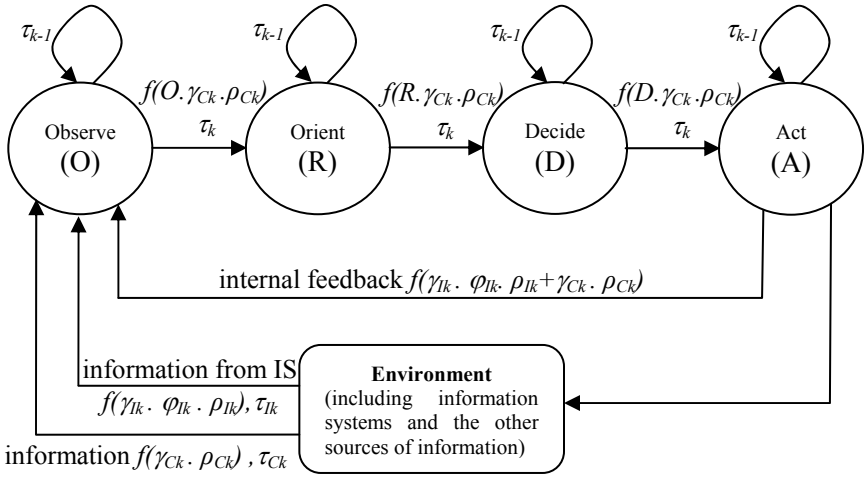

Figure 5: OODA under cyber-attack.

$$F_k \cong f(\gamma_{Ik} \cdot \varphi_{Ik} \cdot \rho_{Ik} + \gamma_{Ck} \cdot \rho_{Ck}) \tag{15}$$

$$I_k \cong f(\gamma_{Ck} \cdot \rho_{Ck} + \tau_{Ck}) \tag{16}$$

$$S_k \cong f(\gamma_{Ik} \cdot \varphi_{Ik} \cdot \rho_{Ik} + \gamma_{Ck} \cdot \rho_{Ck} + \tau_{Ik}) \tag{17}$$

$$O_k \cong f(F_k + I_k + S_k + \tau_{k-1}) \tag{18}$$

Orientation Stage R is the most important stage, where the decision makers analyze and synthesize the information provided by Stage O. In this stage, the trust to the integrity of the obtained information plays an important role beside all other parameters such as cultural traditions, genetic heritage and previous experience. There are two types of trust. One is coming from the detected integrity issues at the current decision interval, τ_k. The other is the experience about the integrity of the available information, τ_{k-1}. The relation between cyber attack/defense parameters and Stage R is given by Equation 19.

$$R_k \cong f(O + \gamma_{Ck} \cdot \rho_{Ck} + \tau_k + \tau_{k-1}) \tag{19}$$

In decision Stage D, the information analyzed and synthesized during Stage R is used to reach a decision. At this stage, the lower the available information level and the trust to the information, the higher the risk of irrational decision, because when the information is not available or trusted, counterproductive behavior due to emotional bias, expectation bias, cost fallacy, risk aversion bias and past fixation becomes more common. Please note that trust to information affects every stage in decision process again and again, and trust level is an important effect of cyber attacks.

$$D_k \cong f(R + \gamma_{Ck} \cdot \rho_{Ck} + \tau_k + \tau_{k-1}) \tag{20}$$

$$A_k \cong f(D + \gamma_{Ck} \cdot \rho_{Ck} + \tau_k + \tau_{k-1}) \tag{21}$$

At the final stage actions are taken based on the decisions made. During the execution of actions, new decisions can be taken based on evolving situation or previous decisions may be changed. As it is clear in Equations 18-21, decision making process is affected by cyber attacks and defense measures. By using the transient relations between attack/defense parameters and types of attacks, we can also see the relations of attack types with the various stages of decision making process.

4 TECHNIQUES FOR STIMULATING AND SIMULATING EXPECTED EFFECTS OF CYBER OPERATIONS

As shown in Figure 5, trust is the most important cyber attack parameter that affects every stage in decision making. The other important parameter is availability. In training events and exercises, it is possible to affect the trust and availability levels to create intended human behavior effect of cyber attacks by using simple techniques. We call these techniques as stimulation techniques (i.e., techniques that stimulate the human behavior effects of cyber attacks), and they should satisfy the following rules:

- The stimulation techniques should not hinder reaching the other training objectives. If training audience focus mainly on solving cyber security issues at the expense of reduced efficiency in other functions, or the communications and information systems (CIS) resources become too scarce, the other training objectives may not be exercised. This should be avoided.
- The stimulation techniques should not incur unreasonable cost or effort to implement.
- The stimulation techniques should be controllable. Exercise controllers/trainers should have the full control in reducing, intensifying or terminating them.

Many stimulation techniques that satisfy these rules can be designed. Three examples that can be used in military exercises are given below:

- Spurious tracks in recognized operational pictures: Spurious maritime and air tracks can be created in recognized air and maritime pictures. For example, additional air border violations may be created together with correct tracks (i.e., tracks that represent air border violations that actually happen according to the scenario of the exercise) in the recognized air picture. This reduces trust to the recognized air picture when the training audience needs it for making decisions and taking actions. The ratio between the true and false tracks, and the locations/timings for the tracks can be changed to control the trust level.
- Role play in response cells: Subordinates and superiors of training audience are represented as response cells in military command post exercises (Cayirci and Marincic 2009). Response cells may delay their actions and responses, and report the reason as the lack of availability in CIS resources due to cyber attacks.
- Compromised messages: Messages that represent compromised, replayed or changed messages can be produced by response cells. When the training audience request for clarification or take an action on the message, the message source denies the ownership of the message.

All these example scenarios can stimulate the effects of cyber attacks on trust and availability levels with negligible cost implications (i.e., the implementation of these scenarios does not require major effort or cost for exercise controllers), because they do not need the actual implementation of cyber attacks or defense measures. Moreover, there is no risk of losing the control of the incident. When actual attacks are implemented, attack may create an unexpected effect, which may risk reaching the other training objectives.

In many cases, the implementation of the actual attacks is not possible because of the security regulations. For example, software normally need to be accredited before being installed in a classified network. This typically requires a long accreditation process. Therefore, running software that simulates malware

in an operational network for a training event is not even an option for many cases. However, the intended effect of cyber attacks can be created on the training audience by using techniques that are similar to the ones explained above and do not require accreditation.

5 CONCLUSION

Cyber security has become more important issue for organizations and individuals that use on line information in decision process. Therefore modeling cyber attacks and defense measures are of interest for many individuals and organizations even if they are not maintaining classified data. There are two ways of simulating cyber threats during training events: simulating the threats and counter-measures or simulating the results of cyber attacks. Cyber attacks result in a human behavior effect that can be reduced by effective cyber defense measures. We present a set of cyber attack and defense parameters that can be used in defining human behavior effects of cyber attacks. The relations between cyber attacks and these parameters are also modeled. Trust and availability are two important cyber attack parameters that impact all the stages in decision making process. Therefore, the focus should be on them rather than on the actual attacks and defense measures especially when training military headquarters and civilian crises management centers. Simple scenarios that are practical and controllable can easily be developed and used for this purpose in exercises. Three examples are provided in Section 4. More scenarios can easily be designed. These scenarios do not require the actual implementation of attacks but simulate the results and effects of attacks and defense measures. Therefore, trainers and training event control staff can easily manage them in the correct level of intensity based on training objectives and the performance of training audience.

REFERENCES

Bezerra, S., Y. Cherruault, Y. Fourcade, and G. Verron. 1996. "A Mathematical Model for the Human Decision-Making Process." *Elsevier Mathematical and Computer Modelling* 24(10):21-26.

Brehmer, B. 2005. "The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control." In *Proceedings of the 10th International Command and Control Research and Technology Symposium The Future of C2.*

Cayirci, E., and D. Marincic. 2009. *Computer Assisted Exercises and Training: A Reference Guide*. Wiley and Sons.

Cayirci, E., and C. Rong. 2009. *Security in Wireless Ad Hoc and Sensor Networks*. Wiley and Sons.

Kotenko, I.V. 2005. "Agent Based Modelling and Simulation of Cyber Warfare between Malefactors and Security Agents in Internet." In *Proceedings of 19th European Simulation Multiconference.*

OMNeT++ Community. 2011. OMNeT++. Accessed March 22. http://www.omnetpp.org.

Stytz, M.R., and S. B. Banks. 2010. "Addressing Simulation Issues Posed by Cyber Warfare Technologies." In *SCS M&S Magazine. n(3).*

Ulman, D. G. 2006. *Making Robust Decisions: Decision Management for Technical, Business and Service Teams.* Trafford Publishing.

AUTHOR BIOGRAPHIES

ERDAL CAYIRCI graduated from Army Academy in 1986 and from Royal Military Academy, Sandhurst in 1989. He received his MS degree from Middle East Technical University, and a PhD from Bogazici University both in computer engineering in 1995 and 2000, respectively. He retired from the Army when he was a colonel in 2005. He was an Associate Professor at Istanbul Technical University, Yeditepe University and Naval Sciences and Engineering Institute between 2001 and 2005. Also in 2001, he was a visiting researcher for the Broadband and Wireless Networking Laboratory and a visiting

lecturer at the School of Electrical and Computer Engineering, Georgia Institute of Technology. He founded Genetlab in 2005. He is currently Chief, CAX Support Branch in NATO's Joint Warfare Center in Stavanger, Norway, and also a professor in the Electrical and Computer Engineering Department of University of Stavanger. His research interests include sensor networks, mobile communications, tactical communications, and military constructive simulation. Professor Cayirci has acted as an editor of the journals *IEEE Transactions on Mobile Computing, AdHoc Networks (Elsevier Science)* and *ACM/Kluwer Wireless Networks*, and has guest edited four special issues of *Computer Networks (Elsevier Science), AdHoc Networks (Elsevier Science)* and *Kluwer Journal on Special Topics in Mobile Networking and Applications (MONET)*. He received the "2002 IEEE Communications Society Best Tutorial Paper" Award for his paper titled "A Survey on Sensor Networks" published in the *IEEE Communications Magazine* in August 2002, the "Fikri Gayret" Award from Turkish Chief of General Staff in 2003, the "Innovation of the Year" Award from Turkish Navy in 2005 and the "Excellence" Award in ITEC 2006. He is also author of three textbooks, *Security in Wireless Ad Hoc and Sensor Networks, Computer Assisted Exercises: A Reference Guide* and *Near Field Communications: from Theory to Practice*, published by John Wiley & Sons. His email is erdal.cayirci@uis.no.

REYHANEH GHERGHEREHCHI is an MSc student in the Electrical Engineering and Computer Science Department at University of Stavanger. Her research interests include wireless communications and security in wireless communications. Her e-mail is r.ghergherehchi@stud.uis.no.