A Characterization of Cybersecurity Simulation Scenarios

Hamdi Kavak
Dept. of Modeling, Simulation & Visualization Engineering
Old Dominion University
1300 Eng. & Comp. Sciences
Norfolk, VA 23529, USA
hkava001@odu.edu

Jose J. Padilla
Virginia Modeling Analysis & Simulation Center
Old Dominion University
1030 University Boulevard
Suffolk, VA 23435, USA
jpadilla@odu.edu

Daniele Vernon-Bido
Dept. of Modeling, Simulation & Visualization Engineering
Old Dominion University
1300 Eng. & Comp. Sciences
Norfolk, VA 23529, USA
Dvern001@odu.edu

Ross J. Gore
Virginia Modeling Analysis & Simulation Center
Old Dominion University
1030 University Boulevard
Suffolk, VA 23435, USA
rgore@odu.edu

Saikou Y. Diallo
Virginia Modeling Analysis & Simulation Center
Old Dominion University
1030 University Boulevard
Suffolk, VA 23435, USA
sdiallo@odu.edu

ABSTRACT
The rate and sophistication of cyber-attacks are ever increasing forcing organizations to test their systems and assess their risks for specific situations (e.g., data breach). Simulation is an emerging field in testing and assessing cybersecurity risk as it allows modeling cyber systems, their interdependencies, and interactions between cyber systems and people who are using, policing, and even attacking these systems. With cybersecurity scenarios, we help describe and formulate these complex interdependencies and relationships. In this paper, we first characterize cybersecurity scenarios along (1) the nature of cyber systems with considerations for design and (2) the type of actor with considerations of abilities. This characterization provides a more clear distinction compared to military oriented LVC (Live-Virtual-Constructive) simulation characterization. We then review examples from the literature based on our characterization. According to our review, we note that cyber system representation has been widely explored while actor representation is often realized at the technical-level dismissing social and cognitive aspects. Thus, we believe that paying more attention to social and cognitive aspects of actor representation, especially as developing general-purpose tools, will benefit the modeling and simulation community.

Author Keywords
Cybersecurity; simulation for cybersecurity; cyber system representation; actor representation

ACM Classification Keywords
I.6 SIMULATION AND MODELING

1. INTRODUCTION

Advancements in communication and information technologies have connected the world in a way that physical presence is no longer a requirement. It is possible nowadays to accomplish daily tasks such as buying/selling stocks online or to accomplish critical missions such as remote military operations. While these advancements eased the way we do tasks, they also create opportunities for cyber criminals to access, control, modify, or even destroy cyber systems and data on cyber systems. Failure in securing them may become not only financially costly [51], but also risky for national security [13].

As a part of security assessment, organizations test their cyber systems and assess their risks. A cyber system can be tested through evaluating the security measures of individual components and the overall system against potential cyber-attacks. For instance, vulnerabilities of a system can be tested using port-scanning tools. Risk assessment of a cyber system, on the other hand, helps identify critical parts of the system to plan and prioritize resources during crises and/or emergencies. In this respect, US National Institute of Standards and Technology developed a Cybersecurity Framework for guiding risk assessment and planning activities for institutions [38]. It is important to note that system users and security personnel are considered as integral parts in both testing and risk assessment due to the fact that human factors play a significant role in cybersecurity incidents [24].

One way to approach the above testing and risk assessment would be to use actual working system. In this case, security assessment results should be very close to what could happen in a real incident; however, it is often the case that assessing security on real system is not only unreasonable but also dangerous. For instance, SCADA systems are not tolerant to interruptions, thus testing on a real SCADA system might yield threatening outcomes. Instead of testing on the actual system, organizations create

CNS 2016, April 03 - 06, 2016, Pasadena, CA, USA

representative systems to conduct security assessments in a safer way.

Simulation is a cost-effective and often flexible way of creating a representative system with its interdependencies and relationships, which can be studied through execution of scenarios. However, not all scenarios are created equally and, in fact, not all simulation scenarios include only simulated elements. Thus, we need a way to characterize these differences. One common characterization is live virtual constructive (LVC) simulation.

LVC [12] in cybersecurity context, as introduced in [9], characterizes cyber systems by their type of representation:

- Live (cybersecurity) simulation: Real actors (in a testing/assessment scenario) interact with physical systems of real computers connected to real, and usually isolated, networks.
- Virtual (cybersecurity) simulation: Real actors (in a testing/assessment scenario) interact with emulation/simulation of networks or emulation/simulation of actors interacts with real and usually isolated, networks.
- Constructive (cybersecurity) simulation: Simulated/emulated actors (in a testing/assessment scenario) interact with emulation/simulations of networks.

This LVC terminology is used, especially in the military domain, as it provides an umbrella for the different types of systems that can be used jointly or separately. In other words, it tells us about the nature of the simulation for cybersecurity. We will further explore this nature as one of two potential cybersecurity simulation dimensions.

2. CHARACTERIZATION OF CYBERSECURITY SIMULATION SCENARIOS

In the cybersecurity simulation context, we define scenario as a description of an existing or potential cyber incident. These descriptions vary of course depending on the incident to be described and the purpose of making the scenario such as policymaking or testing network resilience. As researchers, we are interested in this characterization as it increases our understanding of how simulation is, and can be, applied in cybersecurity context. In addition, a clear characterization with enough detail would (1) provide a common terminology in scenario description facilitating communication among the community and (2) classify the literature in identifying emphasized and overlooked study areas. Thus, we first aim at finding elements that can be included in a typical cybersecurity scenario.

A cyber-attack against the security company RSA (https://www.rsa.com) back in 2011 is a typical cyber incident example, which helps us derive scenario elements.

"[T]he attacker sent two different phishing emails over a two-day period…to two small groups of employees… The email subject line read '2011 Recruitment Plan'. This was intriguing enough for one of the employees to actually pull the email out of their Junk Box and double-click on the email attachment… The [attached] spreadsheet contained a zero-day exploit that installs a backdoor through Adobe Flash vulnerability (CVE-2011-0609)… The attacker first harvested access credentials from the compromised users … performed privilege escalation on non-administrative users in the targeted systems, and then moved on to gain access to key high value targets, which included process experts and IT and Non-IT specific server administrators… The attacker then used FTP to transfer many password protected RAR files from the RSA file server to an outside staging server… RSA detected this attack in progress" [44].

Considering this incident as a scenario, we can infer a list of broad scenario elements as follows.

- An attacker
- Users that the attacker targets initially
- A cyber system and data that the attacker targets
- System security personnel that detects the incident
- Interactions between the attacker, users, the system and the security personnel
- A wide network infrastructure that facilitates connection between cyber systems and people.

The above elements can be categorized under two groups: cyber systems (including data and wide network infrastructure), as observed in LVC systems, and actors (attacker, user, and system security personnel).

2.1. Cyber System Characterization

A cyber system, in a typical scenario, is described as a network of information systems involving nodes (workstations, printers etc.), routers, applications servers, databases, etc. We often assume that data are part of cyber systems as well. For instance, a stock market exchange system is a cyber system; it is a networked system containing data with thousands of computers serving thousands of customers online. When we study systems through scenarios, representations of cyber systems (i.e., *representative systems*) are preferable to work with, as it is neither reasonable nor safe to execute a scenario on a real working cyber system. It is not a requirement but it is advantageous that these representative systems are constructed using general-purpose network development environments. For instance, the US Army has recently built a cybersecurity training center in order to provide a general-purpose training environment for soldiers [47]. Being general-purpose, these environments are cost-effective as they allow reuse of the same system for wide range of tasks. However, not all general-purpose environments are made equal. Based on the purpose of the scenario, cyber systems are usually represented as physical, emulation, and

simulation, which can be approximated to live, virtual and constructive respectively.

Physical (actual) means that a representative system is built using physical hardware, devices, and software. There are certain advantages and disadvantages on setting a physical environment. On the one hand, physical environment allows setting up networks that are as close as possible to an actual cyber system (or its scaled down version) because all the elements of the network, in principle, can be identical to the actual cyber system. On the other hand, it comes with challenges such as hardware cost [32].

When using emulation, as an approach, some part (or whole) of the cyber system is represented and mimicked using surrogate systems called emulators [20, 35]. In other words, emulators act in place of a real device as a part of a representative system and are usually realized as software [21, 41]. Representing hardware as software might provide flexible environment to construct computer networks [41]. As such, real software applications, on network nodes, will still be able to run on (partly) emulated network.

Although sometimes confused with emulation, a simulation approach is different in several aspects. Simulation makes a constructive representative model of the actual cyber system. In this case, some details of actual cyber system might be abstracted out. It is, for instance, possible to see a network simulation without capabilities of transmitting full-stack of network protocol data. This is advantageous, as simulations often do not require as much of computational resources when compared to emulation and physical solutions. As a result, it is cost effective [32] and becomes easier to scale to a large number in network size [7]. Lastly, given the same parameters (including the seed value for pseudo-random number generators), simulations "always execute in exactly the same way" [35, p. 2684] which makes them suitable if repeatability is of concern. The disadvantage with simulation as the representative system is that it is often not possible to run real software [8].

In the context of cyber system representation, LVC means that an environment/tool involves physical, emulation, and simulation in the same construct. As such, the benefits of each type are expected to improve the mix: scalability can be achieved with a simulation, fidelity with an emulation and flexibility with either. Fidelity, scalability, and flexibility then are considerations for type selection in scenario construction and can be treated as a scale of values such as low, medium, or high.

Feinstein and Cannon [17] define fidelity as "the level of realism that a simulation presents to the learner" (p.426). While the definition is subjective, it could be tied to the level of detail in the representative system. In other words, a cyber system representation that provides higher detail of the system has higher fidelity. In network development environments, it is often the case that physical systems have the highest fidelity [25].

Scalability is the ability of rapidly increasing the size of a network. It is sometimes associated with the availability of computing resources but network development environment should facilitate increasing the size without significant effort. Simulations are quite advantageous in terms of scalability as system components are constructive and lightweight while physical systems are the least advantageous [25].

Flexibility is the ability of rapidly repurposing the environment for another use case. Simulations are quite flexible while physical systems are challenging.

2.2. Actor Characterization

Actor representation, despite the evidence of the role of humans in cyber incidents [24], has been explored in a limited matter. This could be due to the complexity of simulating humans along the behavioral and cognitive lines relevant to the cybersecurity community. Currently, actors are represented by real people or by simulated entities. It depends on the purpose of the study and other constraints when making decision to use real people or simulated entities. Cases show that when actors are represented as real, they role-play a certain actor in a scenario. Cyber ShockWave [5] is an event that attempts to simulate series of cyber-attacks against critical infrastructures. Actors, in this case, role-play government officials that advise the president. [18] also reports a similar experimentation with a business-oriented context. However, these scenarios are costly and require large number of people's participation and physical presence for several days. Our focus here is on characterizing simulated entities as they make scenarios flexible and economical without active human participation (If needed, though, it would still be possible to add real actors as part of the characterization). Here we characterize actors based on their *type* with considerations for social, technical, and cognitive *abilities*.

We consider using the term *type* for showing the variety of different group of people that might be involved in a typical cybersecurity simulation scenario. In this case, types of actors we identified are *attackers*, *system security personnel*, *users*, and *insiders*.

Attacker is a vague term because it is actually an unknown party in majority of cyber incidents. In this sense, an attacker may be an individual, a group, or a state-funded organization. Because of this vagueness, it is often the case that attackers are not explicitly represented in cybersecurity simulation scenarios. Rather, their actions to the cyber system are scripted [22].

A system security individual is an employee who monitors cyber system's security and protects it against unauthorized access and other intrusions. Typical system security personnel have higher-level access to system resources than regular system users and are often knowledgeable and well-trained professional. Their representation in a scenario

might be crucial as described in [44] case where early detection of an attack prevented greater damage.

Users are often employees that have access to the cyber system at a low level. While they have low-level privileges – as seen in RSA case – their mistakes might be costly as attackers use them as an entry point to the system before elevating their privileges; that is the reason why system users are one of the listed actor types in our characterization.

Among the four types, insider is probably the most ambiguous one because it involves characteristics of the other three types. Insiders are similar to system users as they have access to the system through legitimate work. They are similar to security personnel as they usually have knowledge, skills, and resources. They are also similar to attackers as they access the system for illegitimate gain [52]. Their capabilities may help them thwart detection [34]. While other actor types seem like constant categories, insider studies may involve a simulated entity changing their type along the simulation (e.g., a system user turning to an insider).

Considering four types of actors, it is a fact that not all actors in real world have same abilities at the same level. These cases need to be captured in cybersecurity scenarios too. In this respect, we consider *social*, *cognitive*, and *technical* abilities of actors in our characterization.

Social ability of an actor refers to being able to communicate and interact with other actors. Importance of social ability comes from the fact that it can facilitate a means to model non-linear dynamics of interactions. For instance, people in a work group in an organization might behave quite differently when social ability exists. In actors, social abilities are often represented using multi-agent frameworks.

Cognitive ability, according to Bernstein et al. [4], "is the capacity to perform higher mental processes of reasoning, remembering, understanding, and problem solving". In actor representation, by cognitive ability we mean deliberate decision-making based on a cognitive model such as Belief-Desire-Intention (BDI).

Technical ability of an actor is a skillset facilitating to execute certain actions such as conducting a cyber-attack. Realization of this skillset differs based on the purpose identified in the cybersecurity simulation scenario. In some instances, skillset might be realized using a simple Boolean variable. However, in some instances, realizing a skill might require operating real software.

3. CYBER SYSTEM REPRESENTATION EXAMPLES

In order to create scenarios that capture cyber systems and actors, tools are required. We describe a sample of tools that vary along emulation and simulation lines representing cyber systems, which are those of interest for this community. Actor representations are given in section 4.

3.1. Simulators

Simulators for representing cyber vary from general-purpose simulation tools to those focused on the creation of networks and the evaluation of varied cyber-attacks like denial of service. Some of the ones used, based on the literature are:

- General-purpose simulation software includes those for discrete-event or agent-based simulations. [29] use Arena to construct a representative network system and intrusion detection system that is able generate simulated attacks. Their model consists of hosts and links between hosts but with no detailed representation of hosts or traffic, thus their model fidelity is low. Authors do not report about model scalability or flexibility.
- NS-3 [39] is an open source discrete-event network simulation tool. Main function of the tool is to provide a programming environment where users can develop network models using python or C++ languages. While requiring programming expertise, it allows flexible development, highly scalable system, and relatively good fidelity in network representation.
- OMNET++ [48] is an open source discrete-event simulation tool that aims at simulating computer networks (hosts, routers, protocols, links etc.). With the extension of INET framework, it can generate high fidelity virtual traffic and its GUI makes it easier to identify network settings. [25], for instance, uses OMNET++ (with INET) as the infrastructure to model a computer network and uses this network to analyze distributed denial of service (DDoS) attack and defense mechanisms based on a multi-agent framework.
- OPNET is a commercial, general-purpose, simulated-based network development and testing tool, which is currently named as SteelCentral [42]. While it is essentially a network simulator, its capabilities such as providing an extensible wide range of network elements and realistic network traffic generation make it a good candidate for cybersecurity simulation. Various studies use OPNET as their basis for network generation and experimentation (e.g., [31, 46, 53]).

3.2. Emulators

Emulators, as they provide better fidelity compared to simulators, have been used extensively in the literature. Here we review some of the notable ones.

- Emulab [16] is a network testbed[1] facility and software system developed at University of Utah. Emulab allows users generate computer networks with a desired

[1] The term testbed refers to an instance of a system under test (SUT) that satisfies all the properties of SUT for a particular purpose. Thus, a system can be a testbed for one study while it might not be a testbed for another study. See [20] for the definition and [32] for properties of testbeds.

topology based on NS2 script syntax. With this scripting support, Emulab provides highly flexible environment that can create and destroy relatively large-scale models in short periods. In Emulab, computer nodes are realized as virtual computers such as FreeBSD, Linux, and Windows and network devices such as routers are emulated in the system. Thus, Emulab models have high fidelity. Emulab facilitates multiple physical machines providing mid-level scalability capabilities. The main purpose with Emulab is to provide a software and experimentation environment for general-purpose computer networks research rather than mere cybersecurity experimentation.

- The DETER project [2], on the other hand, utilizes Emulab in a cybersecurity testbed called DeterLab. The DETER project aims at providing tools and capabilities for easy-to-handle cyber security experimentations with built-in scenario development and data collection mechanisms. In other words, by keeping all advantages of Emulab, DeterLab provides additional tools and capabilities to conduct cybersecurity experiments. Different from Emulab, DeterLab facilitates creation of multi-resolution network elements that provides variable fidelity and increases scalability of the system. Access to both Emulab and Deterlab are subject to approval of a cybersecurity project in their respective project websites.
- GENI [3] is a facility, similar to DETER, allowing researchers to explore new networking technologies. The difference from DETER is that GENI relies on highly distributed network environment and allow low-level programmability of network. That is, when used in cybersecurity context, it can provide more flexible but complicated environment compared to DETER. Accessing GENI is directly open to select universities in the US while others might need to fill an application.
- Minimega [36] is a tool from Sandia National Labs that can launch and manage massive number of virtual machines connected through a virtual network. Thus, it is an emulation technology. Advanced capabilities of Minimega are high scalable with the ability of running on a cluster, high flexible, fast and lightweight, and additional tools to make virtual machine management even easier. Like other emulation-based tools, fidelity of Minimega is also high. While it has not been used in a scholarly cybersecurity study, Minimega is a great candidate in that realm.
- Netkit [40, 41] is an emulation-based network environment with a capability to setup high fidelity computer networks involving devices such as switches, routers, firewalls and tools such as DNS servers, HTTP servers with a desired topology based on a configuration providing flexibility. The main goal of Netkit is integrating various open source software (e.g., User-Mode Linux [10]) rather than building them from scratch. While Netkit was originally built for network education, it has tools such as snort, IPsec, RADIUS to experiment cyber-attacks as pointed out in [40]. Limitations of Netkit are that it can only run on a single machine and lacks support for Windows/Mac-based nodes.
- Mininet [30] is similar to Netkit, allowing researchers develop emulated computer networks on a single computer. The difference is that Mininet aims at making this process research-friendly allowing deploying generated network description on testbeds, support different protocol stacks, and share with collaborators. Despite its network research orientation, Mininet has been used in cybersecurity research [14].

3.3. LVC and Others

LVC type of cyber systems are actually getting popular as they provide advantages of physical, emulator, and simulators in the same environment. However, as they are costly to build, only few well-known institutions (e.g., Sandia National Lab) are able to develop advanced LVC cyber security experimentation environments.

Emulytics [32] is a platform from Sandia National Lab providing cybersecurity training and testing capabilities. Emulytics blends physical computers, emulated, and simulated components in making large-scale computer networks. Thus, Emulytics is LVC in nature. Defining characteristics of Emulytics is that it allows high fidelity and scalable environment with a large number of network devices and nodes running real operating systems on virtual machines. Developed for training and testing, Emulytics is flexible in creating and destroying large-scale models. While currently only available for internal use, Sandia National Lab might release the system as open source software in the future as they did with Minimega [36] .

Apart from tools above, there are others developed for internal use in military facilities or educational institutions. SIMTEX (Air Force Simulator Training and Exercises) is a network environment used by US Air Force branches with capabilities such as simulation of the Internet [23]. SAST is a cyber-attack training environment developed for US Air Force with capabilities such as background traffic generation [50]. LARIAT (the Lincoln Adaptable Real-time Information Assurance Testbed) is a network emulation/simulation testbed [33, 43]. It is a sophisticated environment capable of generating large-scale computer networks that can mimic user behavior and evaluation of attack behavior.

4. ACTOR REPRESENTATION EXAMPLES

Compared to variety of cyber system representation examples given in section 3, actors are not considered as much. In large number of studies (e.g., [1, 11, 19, 37]) actor representation is implied by mentioning attack occurrence without mentioning the attacker. Here we review studies that explicitly mention the existence of actor types with technical, social, and/or cognitive abilities.

4.1. Actors with Technical and Social Abilities

A common trend in explicit actor representation appears to be scripted behaviors or predefined actions facilitating technical details of an attack. For instance, [49] develop an LVC framework involving user behavior models of security personnel and attackers. According to an example scenario they present, attackers execute timed pre-defined actions in a DDoS scenario. Security personnel in that scenario have also similar capabilities. Along the same line, [22] introduce attackers and security personnel representations executing actions based on game-theoretic and probability-based search techniques in decision-making process. Just recently, authors in [45] represent and simulate attackers and security personnel based on game theory and attack/defend-based graphs. All three examples in common explicitly mention representations of attackers and security personnel with just technical abilities.

In series of papers [25-27], authors develop agent-based models to represent a team of attacker actors and a team of security personnel actors with communication abilities. In addition to technical abilities, these teams have social and adaptive behaviors. These papers describe their tool that facilitates mechanisms for attack and defense and do not have a substantial example how they would work in a real cybersecurity simulation scenario. It is important to note that while they can communicate, authors present these actors more like a computational algorithmic entity rather than representing real system security teams or attacker teams. Nevertheless, technical and social abilities in representing actors have somehow found their way in the literature.

4.2. Actors with Cognitive Abilities

Cognitive abilities, according to our research, have been only investigated in a handful of papers. [15] introduce a cognitive model simulating security personnel's behavior and learning abilities and an attacker with technical abilities with patient or impatient strategies. In this model, they test success of security personnel based on various experience and risk tolerance level against attackers. They conclude that when attacker is impatient, risk-averse and experienced security personnel improve their detection rate while the same not the case for patient attackers. While the scope of their scenario is limited with only two factors involved, the model provides an interesting finding that is not commonly seen in earlier examples.

The idea of providing cognitive abilities to actors is also considered in [6] where they conduct a cybersecurity scenario to simulate system users during a cyber-attack. In this scenario, system users are represented as BDI agents accomplishing their routine tasks operating on real software and communicating with each other. When the cyber-attack is simulated, the model captures the changes in user resiliency, communication patterns, and task accomplishment. Having all three (social, cognitive, and technical) abilities, their model suggests that team organization and finding alternative plans when resources are attacked stabilizes the situation. In other words, like the previous study [15], model results propose some planning suggestions that are not very likely to be gathered when explicit actor representation with social, cognitive, and technical abilities are not present.

The above two examples are ad-hoc solutions to experiment for a particular scenario. Just recently, Deter Project included a module called DASH (Deter Agents Simulating Humans) in their experimentation environment. This module facilitates a means for developing agents (within DeterLab) representing humans with cognitive and technical abilities. The importance of this approach is that this module is developed as a general-purpose tool that can be used in variety of cases similar to those in cyber system representation examples. In fact, it has already been used in a study such as [28] to create cognitive constructs for evaluating password policies from user perspective.

5. CONCLUSION

In this paper, we characterized a typical cybersecurity simulation scenario based on two elements: cyber systems and actors. Cyber systems were described by their nature with considerations for design while actors were described based on their type with considerations of abilities. With this characterization, we are able to differentiate not only different types of models but also classify the examples from the literature. Just considering general-purpose cyber system representation tools (ignoring ad-hoc cyber system representation approaches), we were able to identify a number of tools cutting across our characterization scale. When it comes to actor representation, however, we found large number of studies focusing on attacker and security personnel with their technical-only abilities. This may suggest modeling and simulation scholars have understudied cognitive and social actor research on system users and insiders. We believe that modeling and simulation community dealing with cybersecurity area need to pay more attention on development of general-purpose actor behavior development tools. These tools, when combined in popular general-purpose and open-source cyber system development tools, may diminish the burden of integration and attract the community on contributing their particular actor models.

ACKNOWLEDGMENT

This material is based on research sponsored by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)) under agreement number FAB750-15-2-0120. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

DISCLAIMER

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily

representing the official policies or endorsements, either expressed or implied, of the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)) or the U.S. Government.

REFERENCES

1. AlMajali, A., Viswanathan, A., & Neuman, C. Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack. *Proceedings of 5th ACM USENIX Workshop on Cyber Security Experimentation and Test*. Usenix (2012).
2. Benzel, T. The science of cyber security experimentation: the DETER project. *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM (2011), 137-148.
3. Berman, M., Chase, J. S., Landweber, L., Nakao, A., Ott, M., Raychaudhuri, D., ... & Seskar, I. GENI: A federated testbed for innovative network experiments. *Computer Networks*, *61* (2014), 5-23.
4. Bernstein, D. A., Penner, L.A., Clarke-Stewart, A., & Roy, E. J. *Psychology (6th ed.)* Houghton Mifflin Company, Boston, MA, USA, 2003.
5. Cyber ShockWave, Simulation report and findings. http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Final%20Cyber%20Brochure.pdf. As of 05 January 2016.
6. Blythe, J., Botello, A., Sutton, J., Mazzocco, D., Lin, J., Spraragen, M., & Zyda, M. Testing Cyber Security with Simulated Humans. *Twenty-Third IAAI Conference*. AAAI Press (2011).
7. Calheiros, R. N., Netto, M. A., De Rose, C. A., & Buyya, R. EMUSIM: an integrated emulation and simulation environment for modeling, evaluation, and validation of performance of cloud computing applications.*Software: Practice and Experience*, *43*, 5 (2013), 595-612.
8. Chertov, R., Fahmy, S., & Shroff, N. B. Fidelity of network simulation and emulation: A case study of tcp-targeted denial of service attacks. *ACM Transactions on Modeling and Computer Simulation*, *19*, 1 (2008), 4.
9. Damodaran, S. K., Couretas, J. M., & Allen, B. Cyber Modeling & Simulation for Cyber-Range Events. *Summer Simulation Conference*. Society for Modeling & Simulation International (2015), 529–536.
10. Dike, J. *User mode linux (Vol. 2)*. Prentice Hall, 2006.
11. Dini, G., & Tiloca, M. A Simulation Tool for Evaluating Attack Impact in Cyber Physical Systems. *Modelling and Simulation for Autonomous Systems: First International Workshop, MESAS 2014, Revised Selected Papers* (Vol. 8906). Springer (2014), 77-94.
12. DoD. Modeling and Simulation (M&S) Glossary. http://www.msco.mil/documents/_4_Final_Glossary.pdf As of 05 January 2016.
13. DoD Cyber Strategy. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. As of 05 January 2016.
14. Dong, X., Lin, H., Tan, R., Iyer, R. K., & Kalbarczyk, Z. Software-defined networking for smart grid resilience: Opportunities and challenges. *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, ACM (2015), 61-68.
15. Dutt, V., Ahn, Y. S., & Gonzalez, C. Cyber situation awareness modeling detection of cyber attacks with instance-based learning theory. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *55*, 3 (2013), 605-618.
16. Emulab - Network Emulation Testbed Home. https://www.emulab.net. As of 05 January 2016.
17. Feinstein, A. H., & Cannon, H. M. Constructs of simulation evaluation. *Simulation & Gaming*, *33*, 4(2002), 425-440.
18. Gallaher, D. Cyber simulation lessons learned. https://drive.google.com/file/d/0B5sfMkarqtvUVmRVcnFIZDBKVUU/view?pli=1. As of 05 January 2016.
19. Genge, B., Fovino, I. N., Siaterlis, C., & Masera, M. Analyzing cyber-physical attacks on networked industrial control systems. *Critical Infrastructure Protection V*. Springer (2011), 167-183.
20. Göktürk, E. A stance on emulation and testbeds, and a survey of network emulators and testbeds. *21st European Conference on Modelling and Simulation*, (2007).
21. Guruprasad, S., Ricci, R., & Lepreau, J. Integrated network experimentation using simulation and emulation. *Testbeds and Research Infrastructures for the Development of Networks and Communities, Tridentcom*, IEEE (2005), 204-212.
22. Hamilton, S. N., & Hamilton W. L. Adversary Modeling and Simulation in Cyber Warfare, *International Federation for Information Processing*, Springer (2008), 461–75.
23. Harwell, S. D., & Gore, C. M. Synthetic Cyber Environments for Training and Exercising Cyberspace Operations. (2013). *M&S Journal*, 8, 2(2013), 36-48.
24. IBM Cyber Security Intelligence Index (2015).
25. Kotenko, I. Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security. *4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*.IEEE (2007), 614-619.
26. Kotenko, I. Agent-Based Modelling and Simulation of Network Cyber-Attacks and Cooperative Defence

Mechanisms. *Discrete Event Simulations*. (2010), 223–46

27. Kotenko, I., & Ulanov, A. (2007). Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. *Autonomous Intelligent Systems: Multi-Agents and Data Mining*, Springer Berlin Heidelberg (2007), 212-228.
28. Kothari, V., Blythe, J., Smith, S. W., & Koppel, R. Measuring the security impacts of password policies using cognitive behavioral agent-based modeling. *Proceedings of the Symposium and Bootcamp on the Science of Security*. ACM (2015).
29. Kuhl, M. E., Kistner, J., Costantini, K., & Sudit, M. Cyber attack modeling and simulation for network security analysis. *Proceedings of the 39th Conference on Winter Simulation*, IEEE Press (2007), 1180-1188.
30. Lantz, B., Heller, B., & McKeown, N. A network in a laptop: rapid prototyping for software-defined networks. In *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, ACM (2010).
31. Leeuwen, B., Urias, V., Eldridge, J., Villamarin, C., & Olsberg, R. Performing cyber security analysis using a live, virtual, and constructive (LVC) testbed. *Military Communications Conference*, IEEE (2010), 1806-1811.
32. Leeuwen, B. V., Urias, V., Stout, W., & Wright, B. Emulytics at Sandia National Laboratories. *MODSIM World 2015*, 1–10.
33. Lincoln Laboratory https://www.ll.mit.edu/mission/cybersec/CSA/CSA-projects.html. As of 05 January 2016.
34. Maasberg, M., Warren, J., & Beebe, N. L. The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits. *48th Hawaii International Conference on System Sciences (HICSS)*, IEEE (2015), 3518-3526.
35. McGregor, I. The relationship between simulation and emulation, *Proceedings of the Winter Simulation Conference*, IEEE (2002), 1683-1688.
36. Minimega. http://minimega.org. As of 05 January 2016.
37. Moskal, S., Wheeler, B., Kreider, D., Kuhl, M. E., & Yang, S. J. Context model fusion for multistage network attack simulation. *Military Communications Conference (MILCOM)*, IEEE (2014), 158-163.
38. NIST Framework for Improving Critical Infrastructure Cybersecurity. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. As of 05 January 2016.
39. NS-3. https://www.nsnam.org. As of 05 January 2016.
40. Pizzonia, M., & Rimondini, M. Netkit: network emulation for education. *Software: Practice and Experience*. Wiley (2014).
41. Rimondini, M. Emulation of computer networks with Netkit.*Dipartimento di Informatica e Automazione, Roma Tre University*, (2007).
42. Riverbed http://www.riverbed.com/about/news-articles/press-releases/riverbed-to-acquire-opnet-technologies-inc.html. As of 05 January 2016.
43. Rossey, L. M., Cunningham, R. K., Fried, D. J., Rabek, J. C., Lippmann, R. P., Haines, J. W., & Zissman, M. Lariat: Lincoln adaptable real-time information assurance testbed. *Aerospace Conference Proceedings*, IEEE (2002).
44. RSA FraudAction Research Labs. https://blogs.rsa.com/anatomy-of-an-attack. As of 05 January 2016.
45. Rybnicek, M., Tjoa, S., & Poisel, R. Simulation-Based Cyber-Attack Assessment of Critical Infrastructures. *Enterprise and Organizational Modeling and Simulation*, Springer (2014), 135-150.
46. Sakhardande, R R. *The use of modeling and simulation to examine network performance under denial of service attacks*. ProQuest, 2008.
47. Solivan, D. A. Communications-Electronics Command cyber training range launches. http://www.army.mil/article/150996/Communications_Electronics_Command_cyber_training_range_launches. As of 05 January 2016.
48. Varga, A. The OMNeT++ discrete event simulation system. *Proceedings of the European simulation multiconference*, 2001.
49. Varshney, M., Pickett, K., & Bagrodia, R. (2011, November). A live-virtual-constructive (LVC) framework for cyber operations test, evaluation and training. *MILITARY COMMUNICATIONS CONFERENCE, 2011*, IEEE (2011), 1387-1392.
50. Wabiszewski Jr, M. G., Andel, T. R., Mullins, B. E., & Thomas, R. W. Enhancing realistic hands-on network training in a virtual environment. *Proceedings of the 2009 Spring Simulation Multiconference*, Society for Computer Simulation International (2009).
51. WEF Risk and Responsibility in a Hyperconnected World. World Economic Forum Insight Report in collaboration with McKinsey & Company. http://reports.weforum.org/hyperconnected-world-2014/wp-content/blogs.dir/37/mp/files/pages/files/final-15-01-risk-and-responsibility-in-a-hyperconnected-world-report.pdf. As of 05 January 2016.
52. Willison, R, and Siponen, M. Overcoming the insider: Reducing employee computer through situational crime. *Communications of the ACM*. 52, 9 (2009), 133-137.
53. Zhou, M., and Sheau-Dong L.. A Frequency-based approach to intrusion detection. *Proc. of the Workshop on Network Security Threats and Countermeasures*, 2003.