Proceedings of the 2019 Winter Simulation Conference
N. Mustafee, K.-H.G. Bae, S. Lazarova-Molnar, M. Rabe, C. Szabo, P. Haas, and Y-J. Son, eds.

SIMULATION FOR CYBER RISK MANAGEMENT – WHERE ARE WE, AND WHERE DO WE WANT TO GO?

Sachin Shetty

Virginia Modeling, Analysis and Simulation Center
Old Dominion University
1030 University Blvd
Suffolk, VA 23435, USA

Indrajit Ray

Department of Computer Science
Colorado State University
1873 Campus Delivery
Fort Collins, CO 80523, USA

Nurcin Ceilk
Michael Mesham

Department of Industrial Engineering
University of Miami
1320 South Dixie Highway
Coral Gables, FL 33146, USA

Nathaniel Bastian

Army Cyber Institute
Unidted States Military Academy
2101 New South Post Road
West Point, NY 10996, USA

Quanyan Zhu

Department of Electrical and Computer Engineering
New York University
70 Washington Square Sout
New York, NY 10003, USA

ABSTRACT

There is a dearth of simulation environments that conduct a comprehensive cyber risk assessment and provide insights that are accessible for decision makers and operational folks. During the Winter Simulation Conference 2019, a group of experts will discuss the challenges and opportunities for developing simulation platforms for cyber risk management. The panel will focus on issues with integrating technologies into simulation platforms, loss of fidelity due to lack of access to cyber datasets and complexity involved in representing cyber-physical systems. This paper is a collection of position papers of the participating experts supporting their viewpoints that will be captured in the panel discussion.

1 INTRODUCTION

Critical infrastructures such as, power grid, oil and gas refineries, and water distribution are characterized by complex technological networks, and its cyber-physical interconnectivity presents a "surface" for cyber attacks. The potential for disruptions in these critical infrastructures can be attributed to the dependence and the vulnerability of the networks interconnecting the physical plants and control centers. There is a need for deeper insights into cyber risks to critical infrastructures. Researchers and practitioners have proposed data driven cyber risk assessment platforms that provide insights into factors that increase cyber risk. However, for critical infrastructure, it is not practical to allow assessment tools to gain direct access

to mapping and collecting information on the cyber infrastructure. Simulation platforms provide a safe and practical means to gain insights about cyber risk to critical infrastructure without impacting operational resilience.

However, there is a dearth of simulation platforms for cyber risk management that can provide quantitative insights into the operational resilience and development of an cyber defense remediation plan. It is highly unlikely to gain direct access to data from operational environments. Instead, a simulation environment that characterizes the impact of exploiting attack surfaces in cyber environments would be applicable and provide useful quantifiable risk metrics which can be useful for decision support systems and eventually help formulate an informed mitigation plan.

The paper is organized as follows. Section 2 provides the opportunities and challenges in developing simulation platforms for cyber risk management. Section 3 presents the need to develop hybrid simulation platforms for critical infrastructure risk assessment. Section 4 presents challenges posed by adversarial machine learning in developing trusted simulation environments for cyber risk assessment. Section 5 describes the advantages of using game theoretic based models for cyber risk management. Finally, in Section 6 we conclude.

2 SIMULATION FOR CYBER RISK MANAGEMENT (NURCIN CELIK AND MICHAEL MESHAM)

2.1 Position Statement

Cyber risk management is a fast pace and complex field, requiring autonomous real-time decision capabilities. To achieve this, intelligent and adaptive systems incorporate simulation to become capable of evaluating a multitude of possible system configurations to determine which is most effective for a given investment level.

2.2 Detailed Description

The overarching goal of the governing body is to improve the system's situational awareness, threat assessments, and allocation of resources. However, all simulations face a similar resources constraint in terms of memory, processing power, and battery life (Kim and Mosse, 2008). These resources ultimately determine the computation and execution time necessary for a simulation to be performed (Celik at al. 2010) as well as its resultant accuracies.

While simulation continues to advance as the state of the art, further refinement is necessary. Simulation continues to race against the clock to deliver accurate results in a timely manner for the data to update. With cyber risk management, time is particularly limited due to the consistently changing cyber environment and speed of attacks. The computation and execution time is determined by the number of runs necessary to reach the desired fidelity. Each run in a simulation tests a different system configuration and determines the effectiveness. If each configuration were tested every time the computation and execution time would exceed the limited time to react, so simulations must be selective in which runs are performed.

Cyber risk management encounters certain unique challenges with the parameters inputted and vast complexity of the problem. First, the simulation must account for all possible exploits and cyber-attack methods with new ones developing each day (Musman and Turner 2018). Second, numerous attack paths must be considered, and the fact that multiple components could be compromised at one time and seemingly, non-critical cyber components can be exploited to bypass security controls (e.g., Stuxnet and Slammer worm) (Musman and Turner 2018). Finally, the behavior of the attacker must be taken into account as each action the defender takes to improve the system's security will lead the attacker to take a corresponding action most promising to the attack (Musman and Turner 2018).

Many uncertainties encountered in cyber risk management can be improved through dynamic and adaptive simulation. Previous work on simulation has potential applications in cyber risk management. Dynamic-Data-Driven Application Systems (DDDAS) (Darema 2004) were originally applied to supply

chain systems (Celik et al. 2010) to adaptively adjust the fidelity of the simulation model against the available computational resources. This was done by incorporating dynamic data into the executing model, which steers the measurement process for selective data update (Celik et al. 2010). DDDAS was further refined to operate on a large scale with Dynamic-Data-Driven Adaptive Multi-Scale Simulations (DDDAMS) (Celik and Son 2012). DDDAMS runs similar to DDDAS, but with a novel selection algorithm based on a sequential Monte Carlo method embedded into the DDDAMS to enable its ideal fidelity selection given large data sets (Celik and Son 2012). Later on, DDDAS was also applied to the automated control in microgrids, facing similar challenges, requiring split second decisions, as those encountered with cyber risk management. DDDAS incorporated a multiobjective optimization algorithm to significantly accelerate the real time computation of the resource allocation, and control decision to optimize the operational cost, energy surety, as well as emissions per MW (Thanos et al. 2017). Overall, the combination of DDDAS and the multiobjective optimization algorithm significantly reduced computation time by 50.38% $\pm$11.09% without compromising quality of the solutions in comparison to a plain optimization problem (Thanos et al. 2017).

The correlation of these recent research on DDDAS to cyber risk management is also strong. The work by (Mesham and Celik 2019) highlights heterogeneous systems addressing the interconnectedness of cyber components and physical components, as cybersecurity and physical security become increasingly interdependent. Their proposed data-driven adaptive simulation framework would enable managers to simulate and evaluate the effectiveness of the integration of physical and cyber securities in complex systems.

Simulation platforms provide cyber risk management an edge by enabling defenders to prepare for a possible attack. Through simulation, systems can assess and discover vulnerabilities to properly prioritize and allocate investment for improvements. Simulation makes this possible by simultaneously evaluating a variety of different system configurations to determine which is most effective for the given resources. This process enables the measurement of the relative improvement of changes (e.g., new information and communication technology (ICT) and different protocols) to the overall system. Knowing the effectiveness of improvements is vital to prioritizing investment for the efficient allocation of resources to address the most pressing threats. Running through simulations to see how attacks play out provides insight into the attacks most likely to occur, to then establish response procedures to minimize the consequences of a successful attack. Simulation can then also evaluate the effectiveness of the procedures put in place to help further refine them to minimize potential impacts to the system. The most captivating ability of simulation, however is the capability to autonomously make real-time decisions without human intervention. This ability allows simulation to surpass human capabilities opening new frontiers. Dynamic simulation is attempting to take this further as it overcomes the challenge of incorporating dynamic data into the executing model similar to DDDAS and DDDAMS (Thanos et al. 2017).

Simulation still faces serious challenges and drawbacks in regard to heterogenous systems, data for testing, simulation parameters, and resource limitations. Heterogenous systems pose a growing problem as systems become more complex as both cyber and physical aspects of security are intertwined. Cybersecurity measures can be easily bypassed if physical access to the system can be gained, and physical security relies on networked electronics (e.g., surveillance, access control, and communication) to protect the facility. The increasing use of ICT systems has introduced a new paradox as the more ICT systems are used, the more opportunities there are for intrusions by external and internal malicious actors (Mesham and Celik 2019). All the physical devices that contribute to the secure functioning of a system are vulnerable to become tools for an attack. Most maintenance services on ICT systems are performed remotely, opening a possibility for attack. ICT systems also pose a challenge integrating new ones into an existing simulation environment.

A key requirement to testing a system's performance is data to run, but this has become a particular challenge in cyber risk management. A lack of data for testing simulations exists as no one wants to potentially compromise real, critical data. Simulating realistic data creates another challenge in itself as the data must produce both alerts of an intrusion and a control group appearing as normal data (Kuhl et al. 2007). The method can be very tasking on computational resources and faces accuracy limitations in

comparison to realistic data. Cyber risk management also struggles with the parameters inputted into the simulation model as previously mentioned. Simulation relies on a database of all the presently known threats, but this is continuously changing as new and innovative threats and attack methods emerge each day. Some unknown threats already in place may even be missed since many attacks lie in wait. Finally, the simulation model must predict the attacker's behavior, which can be a particularly difficult endeavor as humans can be highly irrational.

The development of a generic simulation framework could be the ultimate benefit to reduce the effort and cost of deployment, testing, and maintenance of systems. This generic framework could support the effective use of existing software, rapid introduction and integration of new standards, protocols and software platforms through the support of a consistent development environment (Kim and Mosse 2008). However, this feat may also prove our greatest challenge as current options available require tremendous effort to adapt to different users' development environments (Kim and Mosse 2008). Generic solutions are often thought not to be useful for most applications, because the generality is typically associated with "not-specific enough" to be ready for use (Kim and Mosse 2008). Most solutions available restrict the development environment and reduce flexibility of design by enforcing the use of a specific software platform and tightly-coupled tools (Kim and Mosse 2008). This is often attributed to legacy software (e.g., wired communications software) integration with new sensor applications, cost issues that require optimizing resources (e.g., memory and communications), and modifiability requirements to enable adding and adapting various requirements easily (Kim and Mosse 2008). Heterogeneity and scalability also introduce challenges due to the level of complexity of the combination of components with the requirement of modeling external resources (e.g., light, temperatures, and signals).

3 HYBRID SIMULATION PLATFORM FOR CYBER RISK MANAGEMENT (SACHIN SHETTY)

3.1 Position Statement

Critical infrastructures are complex systems and there is lack of visibility for the underlying interconnections and message communications due to heterogeneous nature of the system. There is a need to develop a simulation platform that can assist to assess the security posture without impacting the operations and provide quantitative cyber risk metrics that would influence prioritized mitigation plan. Instead, a hybrid simulation environment that characterizes both the cyber and physical environments would be applicable and provide useful cyber risk metrics.

3.2 Detailed Description

The cyber-physical interconnectivity in most critical infrastructures presents an attack surface that has the potential to be exploited by adversaries. For example, exploitation of vulnerabilities in cyber infrastructure interconnecting physical plants and control centers can cause catastrophic damage. Researchers and practitioners will not be able to access data from operational environments to develop the simulation platform. There is a need to develop a simulation platform that can assist to assess the security posture without impacting the operations and provide quantitative cyber risk metrics that would influence prioritized mitigation plan. Researchers and practitioners will not be able to access data from operational environments to develop the simulation platform. Instead, a hybrid simulation environment that characterizes both the cyber and physical environments would be applicable and provide useful cyber risk metrics.

The critical question is how the proposed simulation platform would provide cyber risk metrics that would lead to informed decision making. The availability of the cyber risk metrics would provide guidelines and directions in the different stages of Cyber Physical Systems (CPS) operations (e.g., design process, monitoring, recovery, etc.) and ensure the overall security by pointing to the improvement areas with essential recommendations. Including the physical processes and cyber-physical interconnectivity in the

simulation platform would be a big challenge, because of system connectivity changes based on the application area. Depending on expected level of expected fidelity, physical and cyber-physical components can be represented into the simulation platform. It is also possible to add multiple simulation modules where each module would serve specific application area (such as smart grid, oil and gas, etc.). Following are the challenges with developing hybrid simulations for Cyber risk management

There is a need to balance the details in representing the components underpinning the cyber and physical infrastructure. A careful examination of the NIST Industrial Control Systems Reference Defense in Depth architecture reveals that not all attacks in the cyber layers leads to an attack on the physical layer. For instance, if the attack results in disconnecting the corporate network and does not impact the substation, then this type of attack need not be included in the simulator. The focus should be on the attack surfaces that lead to impacting the physical plant. The state-of-the art efforts in simulating exploitability and impact of attacks on critical infrastructure focus on failures induced by physical faults (Kinney et al. 2005). Physical attacks are deterministic in nature and due to the selective nature the impact on the target physical system or potential of cascading events have no parallels to cyber-attacks. The timing of physical attack are typically precise, which is not a case in cyber attacks. The recovery process after physical and cyber attack have divergent timelines. In order to develop a hybrid simulator, the aforementioned issues need to be addressed such that the prominent and impactful attack surfaces are represented.

The development of the hybrid simulation environment would benefit form a formal cyber resilience modeling framework. (Tierney and Bruneau 2007), proposed a R4 framework for disaster resilience across the Technological, Organizations, Societal and Environmental (TOSE) dimensions. The R4 framework comprises of Robustness (Ability of systems to function under degraded performance), Redundancy (identification of substitute elements that satisfy functional requirements in event of significant performance degradation), Resourcefulness (initiate solutions by identifying resources based on prioritization of problems), and Rapidity (ability to restore functionality in timely fashion). A hybrid simulation framework that will allow measurement of the R4 across the TOSE dimensions for cyber physical systems will address the diverse perspectives needed to characterize cyber risk (Haque et al 2018). The ability to characterize the interplay between the diverse TOSE dimensions will be crucial. The hybrid simulation framework is only effective if it provides useful insights to not only the technology stakeholders, but also, decision makers, who would like to utilize the outputs from the simulations to develop informed decision support systems.

The purpose of developing the hybrid simulation framework has to go beyond providing quantifiable cyber risk metrics and lead to an actionable mitigation plan. The mitigation strategies should be applicable across the TOSE dimensions. The mitigation strategies they are typically dependent on the cyber component are not amenable to generalized mitigation plans that also factor in organizational, societal and environmental perspectives. However, the organization policies and physical systems do not undergo changes at the rapid pace at which cyber technologies evolve. Physical systems follow laws of physics that can be leveraged to find out if the physical systems can operate at an acceptable capacity. The inertia property provides the latitude to operate even under loss of cyber information. Within the hybrid simulation framework, it will be beneficial to observe to what extent cyber attack can be withstood, if the physical system can tolerate loss of signals. The simulation framework should be able to answer questions on detection (when should we drop), fault isolation (what should be drop), recovery (how soon can we recover to known good state).

4 USING SIMULATION TO TACKLE THE CHALLENGE OF ADVERSARIAL MACHINE LEARNING (NATHANIEL D BASTIAN)

4.1 Position Statement

Machine learning techniques have the ability to automate cyber risk assessment processes. However, the susceptibility of machine learning algorithms to adversarial manipulation will require simulation techniques

to tackle the challenge of adversarial machine learning in cybersecurity, which serves as a best practice for cyber risk management.

4.2 Detailed Description

Machine learning capabilities have recently been shown to offer astounding ability to automatically analyze and classify large amounts of data in complex scenarios, in many cases matching or surpassing human capabilities. However, these same machine learning algorithms have been shown to be vulnerable to adversarial manipulation through systematic modification of features, which is also known as adversarial examples. In general, these adversarial attacks often take three forms: a) data poisoning attacks inject incorrectly or maliciously labeled data points into the training set so that the algorithm learns the wrong mapping, 2) evasion attacks perturb correctly classified input samples just enough to cause errors in classification, and 3) inference attacks which repeatedly test the trained algorithm with edge-case inputs in order to reveal the previously hidden decision boundaries. These adversarial machine learning attacks in the domain of cybersecurity can cause the algorithms to misbehave or reveal information about their inner workings, which poses significant cyber risk that needs to be managed.

Within the cybersecurity domain, machine learning algorithms are frequently used for malware detection and as part of intrusion detection systems (IDS). For malware detection, machine learning based algorithms extract features from programs and use a classification model to classify programs between benign and malware. Most of these algorithms are integrated into an antivirus software, making it difficult for malware authors (i.e., adversaries) to know which classifier a malware detection system uses and the underlying parameters of the classifier. However, these adversaries can figure out what features a malware detection algorithm uses and can manually modify them, for example, by changing some API names in the import directory table (Hu and Tan 2017). For IDS, machine learning based algorithms are essential to detect and defend network attacks, as the objective of these algorithms is to classify the network traffic records between normal and malicious. However, adversaries attempt to deceive these machine learning algorithms by using adversarial malicious network traffic examples to deceive and evade the IDS (Lin et al. 2018).

Protection against adversarial machine learning attacks include techniques that cleanse training sets of outliers in order to thwart data poisoning attempts, and methods that sacrifice up-front algorithm performance in order to be robust to evasion attacks. As machine learning based artificial intelligence (AI) capabilities become incorporated into facets of everyday life, including protecting cyber assets, the need to understand adversarial machine learning and address it becomes clear. Poisoning attacks that inject incorrectly labeled malicious traffic or data can be leveraged by the adversary to enable their attacks to go undetected, while data evasion attacks can be used to cause false classification of benign traffic as malicious thereby eliciting a defense response. If machine learning based AI is to succeed in helping cybersecurity, it must be secure and robust to adversarial attacks itself.

Therefore, in order to ensure effective cyber risk management to protect against the threat of these adversarial machine learning attacks, many proactive defense strategies have been developed to serve as countermeasures for adversarial examples. These proactive strategies make machine learning based algorithms within the cybersecurity domain more robust. One such proactive strategy is known as adversarial training, which entails training classification models with adversarial examples to make the machine learning algorithm more robust. These adversarial examples must be generated and injected into the training data set (Yuan et al. 2019). While there are many different approaches for generating adversarial examples, small perturbations are commonly used in practice. Recall that adversarial examples are designed to be close to the original samples and imperceptible to a human, which causes performance degradation of machine learning algorithms compared to that of a human.

In order to generate adversarial examples for use in the training data, simulation methods can be used quite effectively as a perturbation scheme. In the case of malware detection, for example, the development, training and evaluation of machine learning algorithms using a stochastic simulation-based perturbation scheme of the training data along with a stacking ensemble method led to malware classifiers robust to

adversarial conditions without significantly degrading the model's classification accuracy (Devine and Bastian 2019). As a result, simulation techniques can be effectively used to tackle the challenge of adversarial machine learning in cybersecurity, which serves as a best practice for cyber risk management.

5 GAME THEORETIC METHODS FOR CYBER RISK MANAGEMENT (QUANYAN ZHU)

5.1 Position Statement

Game theory based modeling framework provides ability to quantify the interactions between attackers and defenders, which leads to development of quantitative metrics for cyber risk assessment. The threat of adversarial machine learning can be addressed by incorporating game theoretic methods in simulation techniques to facilitate quantifying cyber risk measures in a resilient fashion.

5.2 Detailed Description

The increasingly sophisticated information and communication technologies (ICTs) today have made systems and devices highly connected more than ever before. The complexity of large-scale systems and their ubiquitous connectivity have created new challenges for cybersecurity risk management. One critical example is the cyber-physical systems, where the integration of the ICTs with the physical systems such as power plants, vehicles, and manufacturing systems has increased operational efficiency but exposed them to cyber vulnerabilities. Lessons from recent attacks such as Stuxnet, Duqu, and Triton have indicated a new class of attacks called advanced persistent threats (APTs), where attackers can gain unauthorized access to a network and remain undetected for a long period of time. Attackers can leverage sophisticated techniques to target a specific asset. Traditional security solutions using cryptography, which relies on the secrecy of cryptographic keys, are no longer sufficient for APTs. Hence, managing cybersecurity risks is critical to protect targeted assets in the network and mitigate the impact of the attacks if they become successful.

The first challenge of cyber risk management is to quantify risk measures for the system. Game theory recently has become a natural framework to provide a quantitative model to capture the interactions between attackers and defenders. The rich literature on game-theoretic methods has offered a variety of frameworks to model different security contexts. For example, Stackelberg games have been used to study the leader-and-follower-type of security interactions in which the follower can observe and respond to the action of the leader, e.g., (Pawlick and Zhu 2016; Zhu and Başar 2013; Zhu et al. 2010a, Zhu et al. 2012b; Zhu et al. 2012c, Zhu et al. 2012d, Zhu et al. 2013e; Zhu et al. 2013f; Clark et al. 2012). The two-stage interaction game can be extended to dynamic games to model multiple rounds of strategic interactions of the attacks and defense across different layers of the system, e.g., (Zhu et al. 2010g; Zhang and Zhu 2017c; Huang and Zhu 2018b; Huang and Zhu 2018a; Pawlick et al. 2015; Farhang et al. 2014; Zhu and Başar 2009; Zhu et al. 2010h; Zhu et al. 2010i). The games of incomplete information are a class of games that can capture the asymmetric information between players and have been used to study cyber deception and counter-deception, e.g., (Pawlick et al. 2018; Zhang and Zhu 2017c; Horák et al. 2017; Pawlick et al. 2017; Pawlick and Zhu 2015; Zhuang et al. 2010). The network games offer frameworks that deal with security risks over networks, which have been used together with attack trees and graphs to model cyber risks for enterprise networks, critical infrastructures, and massive IoT systems, e.g., (Xu and Zhu 2017b; Xu and Zhu 2017a; Xu and Zhu 2016; Xu and Zhu 2015; Huang et al. 2017; Chen et al. 2017; Miao et al. 2018; Yuan et al. 2013). The analysis of the equilibrium of the games provides a quantitative prediction of the security outcomes of the game model, which leads to a method to assess long-term risks of the network system.

With the quantitative measures of security, game theory makes security manageable beyond the strong qualitative assurances of cryptographic protections. Extending this approach to mechanism design provides system designers freedom to shift the equilibrium and the predicted outcomes toward ones that are favored by the defender or the system designer via an elaborate design of the game structure. One example is

the design of proactive defense to have a built-in security mechanism to increase the cost of attacks and equip with preventive responses. These preventive responses make attackers less impactful when they reach their targets. In (Huang and Zhu 2018b), it has been shown that such preventive measures can be implemented across multiple layers of the system to protect the targeted asset by holistically taking into account interconnections and interdependencies among these layers.

Another key application of mechanism design is cyber insurance. Cyber insurance is an important tool in risk management to transfer risks. Complementary to the technological solutions to cybersecurity, cyber insurance can mitigate the loss of the targeted system and increase the resiliency of the victim by enabling quick financial and system recovery from cyber incidents. Such a scheme is particularly helpful to small and medium-size infrastructure systems that cannot afford a significant investment in cyber protection. In (Zhang et al. 2017), a principal-agent game-theoretic model has been introduced to capture the interactions between one insurer and one user. The insurer is deemed as the principal who does not have incomplete information about the user's security policies. The user, which refers to the infrastructure operator or the customer, implements his local protection and pays a premium to the insurer. The insurer designs an incentive compatible insurance mechanism that includes the premium and the coverage policy, while the user determines whether to participate in the insurance and his effort to defend against attacks. The mechanism design approach establishes an attack-aware cyber insurance model and addresses economic and security issues in one holistic framework.

Game-theoretic methods have been promising framework to address many emerging applications such as adversarial machine learning (Zhang and Zhu 2017b; Zhang and Zhu 2017a; Zhang and Zhu 2016; Zhang and Zhu 2015; Zhang and Zhu 2018), cross-layer cyber-physical security (Miao et al. 2018; Pawlick and Zhu 2017c; Chen and Zhu 2017; Zhu and Basar 2015; Xu and Zhu 2017b), cyber deception (Pawlick et al. 2018; Zhang and Zhu 2017c; Horák et al. 2017; Pawlick et al. 2017; Pawlick and Zhu 2015; Zhuang et al. 2010), moving target defense (Zhu and Başar 2013; Jajodia et al. 2011; Maleki et al. 2016), critical infrastructure protection (Chen et al. 2017; Rass et al. 2017; Huang et al. 2017; Pawlick and Zhu 2017b; Chen and Zhu 2016; Hayel and Zhu 2015; Huang and Zhu 2018a), adversarial machine learning (Zhang and Zhu 2018; Wang and Zhu 2017; Zhang and Zhu 2017b; Pawlick and Zhu 2016; Pawlick and Zhu 2017a), insider threats (Casey et al. 2016; Casey et a1. 2015). The diverse methodologies from game theory that includes games of incomplete information, dynamic games, mechanism design theory offer a modern theoretic underpinning of a science of cybersecurity for risk management.

6 DISCUSSION

The expert position papers compiled in this contribution address modeling and simulation challenges that need to be addressed for cyber risk management. The position papers address challenges in developing the simulation platform that can provide cyber risk assessment by balancing fidelity, accuracy and complexity. The panelists are in agreement that the cyber risk management field is constantly evolving and there is a need for autonomous real-time decision capabilities. The position paper starts by providing the benefits of a simulation platform that is capable of evaluating diverse configurations with the goal to improve system's situational awareness, threat assessments, and allocation of resources. The benefit of a simulation platform would lead to reduction in effort and cost of deployment, testing, and maintenance of systems by effective use of existing environment resources. We also discussed the need for assessing cyber risk for critical infrastructure will result in differentiating between high and low impact cyber attacks. The necessity to agree on a unifying formalism to allow for standardized cyber risk assessment for critical infrastructure is a common theme, but there is no consensus on how to accomplish this. We need to address challenges with cyber risk modeling, achieving right balance between fidelity and actionable intelligence and ensuring trust in the simulation processes to realize the formalism. The use of machine learning models for cyber threat assessment provides meaningful insights into risk metrics and mitigation plans. However, the threat of adversarial attacks on the machine learning model building process has the potential to impact the integrity of the risk metrics and result in incorrect mitigation plans. There is a need for simulation techniques can be effectively used to tackle the challenge of adversarial machine learning in cybersecurity that can lead to

best practices for cyber risk management. Finally, the need for quantitative metrics for cyber risk assessment requires game theoretic based methods. These methods have the ability to provide the metrics in presence of adversarial attacks.

The contributions from the Modeling & Simulation (M&S) domain can significantly benefit the development of simulation environments for cyber risk assessment. The panelists agree that we need to conduct research in this direction and disseminate research results in the cyber and M&S communities that would lead to increase in interdisciplinary contributions.

ACKNOWLEDGMENTS

The work was supported in part by the Air Force Office of Scientific Research under award FA9550-18-1-0075 and the Office of the Assistant Secretary of Defense for Research and Engineering under award FA8750-15-2-0120

REFERENCES

Hu, W. and Y. Tan. 2017. "Generating adversarial malware examples for black-box attacks based on GAN". *arXiv preprint arXiv:*1702.05983.

Lin, Z., Y. Shi, and Z. Xue. 2018. "IDSGAN: Generative Adversarial Networks for Attack Generation against Intrusion Detection". *arXiv preprint arXiv:*1809.02077.

Yuan, X., P. He, Q. Zhu, and X. Li. 2019. "Adversarial Examples: Attacks and Defenses for Deep Learning". *IEEE Transactions on Neural Networks and Learning Systems* 30(9):2805-2824.

Devine, S. and N. Bastian. 2019. "Intelligent Systems Design for Malware Classification under Adversarial Conditions". *Unpublished bachelor's thesis*, U.S. Military Academy, West Point, NY.

Mesham, M. and N. Celik. 2019. "Cybersecurity Assessment of Power Plants using Data-Driven Simulations". working paper.

Celik, N., S. Lee, K. Vasudevan, and Y.-J. Son. 2010. "DDDAS-based Multi-Fidelity Simulation Framework for Supply Chain Systems". *IIE Transactions* 42(5): 325-341.

Celik, N. and Y.-J. Son. 2012. "Sequential Monte Carlo-based Fidelity Selection in Dynamic-data-driven Adaptive Multi-scale Simulations". *International Journal of Production Research* 50(3): 843-865.

Darema,F. 2004. "Dynamic Data Driven Applications Systems: A New Paradigm for Application Simulations and Measurements". *International Conference on Computational Science (ICCS), LNCS*, June 6th – 9th, Krakow, Poland, 662–669.

Kim, J. E. and D. Mosse. 2008. "Generic Framework for Design, Modeling and Simulation of Cyber Physical Systems". *SIGBED Reviews* 5(1): 1-2.

Kuhl, M. E., J. Kistner, K. Costantini, and M. Sudit. 2007. "Cyber Attack Modeling and Simulation for Network Security Analysis". In *Proceedings of the 39th conference on Winter Simulation Conference*, edited by J. D. Tew, 1180-1188, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Musman, S. and A. Turner. 2018. "A Game Theoretic Approach to Cybersecurity Risk Management". *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology,* 15(2): 127-146.

Thanos, A. E., M. Bastani, N. Celik, and C. Chun-Hung. 2017. "Dynamic Data Driven Adaptive Simulation Framework for Automated Control in Microgrids". *IEEE Transactions on Smart Grid* 8(1): 209-218.

Tierney, K. and M. Bruneau. 2007. "Conceptualizing And Measuring Resilience: A Key to Disaster Loss Reduction". *TR News* 250.

Haque, M., G. De Teyou, S. Shetty, and B. Krishnappa. 2018. "Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights". *IEEE International Conference on Intelligence and Security Informatics (ISI)*, November 8th – 10th , Miami, FL, USA, 25-30.

Casey, W., J. A. Morales, E. Wright, Q. Zhu, and B. Mishra. 2016. "Compliance Signaling Games: Toward Modeling the Deterrence of Insider Threats". *Computational and Mathematical Organization Theory* 22(3):318–349.

Casey, W. A., Q. Zhu, J. A. Morales, and B. Mishra. 2015. "Compliance Control: Managed Vulnerability Surface in Social-Technological Systems via Signaling Games". In *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*, October 12th – 16th , Colorado, Denver, USA, 53–62.

Chen, J. C. Touati, and Q. Zhu. 2017. "A Dynamic Game Analysis and Design of Infrastructure Network Protection and Recovery". *ACM SIGMETRICS Performance Evaluation Review* 45(2):128.

Chen, J. and Q. Zhu. 2016. "Interdependent Network Formation Games with an Application to Critical Infrastructures". In *American Control Conference (ACC),* July 6th – 8th, Boston, MA, 2870–2875.

Chen, J. and Q. Zhu. 2017. "Security As A Service for Cloud-Enabled Internet of Controlled Things Under Advanced Persistent Threats: A Contract Design Approach". *IEEE Transactions on Information Forensics and Security* 12(11):2736–2750.

Clark, A., Q. Zhu, R. Poovendran, and T. Bas¸ar. 2012. "Deceptive Routing in Relay Networks". In *Decision and Game Theory*

for Security, edited by Grossklags J., Walrand J. GameSec, 171-185. New York: Springer.

Farhang, S., M. H. Manshaei, M. N. Esfahani, and Q. Zhu. 2014. "A Dynamic Bayesian Security Game Framework for Strategic Defense Mechanism Design". In *Decision and Game Theory for Security*, edited by Poovendran R., Saad W., 319–328. New York: Springer.

Hayel, Y. and Q. Zhu. 2015. "Resilient and Secure Network Design for Cyber Attack-Induced Cascading Link Failures in Critical Infrastructures". In *Information Sciences and Systems (CISS), 2015 49th Annual Conference on*, March 18th – 20th , Baltimore, MA, USA, 1–3.

Hora´k, K., Q. Zhu, and B. Bosˇansky`. 2017. "Manipulating Adversary's Belief: A Dynamic Game Approach to Deception by Design for Proactive Network Security". In *International Conference on Decision and Game Theory for Security*, October 23rd – 25th, Vienna, Austria, 273–294.

Huang, L., J. Chen, and Q. Zhu. 2017. "A Large-Scale Markov Game Approach to Dynamic Protection of Interdependent Infrastructure Networks". In *International Conference on Decision and Game Theory for Security*, October 23rd – 25th, Vienna, Austria, 357–376.

Huang, L. and Q. Zhu. 2018a. "Adaptive Strategic Cyber Defense for Advanced Persistent Threats in Critical Infrastructure Networks". In *ACM SIGMETRICS Performance Evaluation Review*, 46(2):52-56.

Huang, L. and Q. Zhu. 2018b. "Analysis and Computation of Adaptive Defense Strategies Against Advanced Persistent Threats for Cyber-physical Systems". In *International Conference on Decision and Game Theory for Security,* October 29th – 31st, Seattle, WA, USA, 205–226.

Jajodia, S., A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang. 2011. *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. 1st ed. New York: Springer, Inc.

Maleki, H., S. Valizadeh, W. Koch, A. Bestavros, and M. van Dijk. 2016. "Markov Modeling of Moving Target Defense Games". In *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, October 24th – 24th, Vienna, Austria, 81–92.

Miao, F., Q. Zhu, M. Pajic, and G. J. Pappas. 2018. "A Hybrid Stochastic Game for Secure Control of Cyber-Physical Systems". *Automatica* 93:55–63.

Pawlick, J., E. Colbert, and Q. Zhu. 2017. "A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy". *arXiv preprint arXiv:*1712.05441.

Pawlick, J., E. Colbert, and Q. Zhu. 2018. "Modeling and Analysis of Leaky Deception using Signaling Games with Evidence". *arXiv preprint arXiv:*1804.06831.

Pawlick, J., S. Farhang, and Q. Zhu. 2015. "Flip the Cloud: Cyber-Physical Signaling Games in the Presence of Advanced Persistent Threats". In *International Conference on Decision and Game Theory for Security,* November 4th – 5th, London, United Kingdom, 289–308.

Pawlick, J., and Q. Zhu. 2015. "Deception By Design: Evidence-Based Signaling Games For Network Defense".*arXiv preprint arXiv:1503.05458*.

Pawlick, J. and Q. Zhu. 2016. "A Stackelberg Game Perspective on the Conflict Between Machine Learning and Data Obfuscation". In *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, December 4th – 7th, Abu Dhabi, UAE, 1–6.

Pawlick, J. and Q. Zhu. 2017a. "A Mean-Field Stackelberg Game Approach for Obfuscation Adoption in Empirical Risk Minimization". *arXiv preprint arXiv:*1706.02693.

Pawlick, J. and Q. Zhu. 2017b. "Proactive Defense Against Physical Denial of Service Attacks Using Poisson Signaling Games". In *International Conference on Decision and Game Theory for Security*, October 23rd – 25th, Vienna, Austria, 336–356.

Pawlick, J. and Q. Zhu. 2017c. "Strategic Trust in Cloud-Enabled Cyber-Physical Systems with an Application to Glucose Control". *IEEE Transactions on Information Forensics and Security* 12(12):2906–2919.

Rass, S., A. Alshawish, M. A. Abid, S. Schauer, Q. Zhu, and H. De Meer. 2017. "Physical Intrusion Games–Optimizing Surveillance by Simulation and Game Theory". *IEEE Access* 5:8394–8407.

Wang, W., and Q. Zhu. 2017. "On the Detection of Adversarial Attacks against Deep Neural Networks". In *Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense*, October 30 – November 3, Dallas, Texas, 27–30.

Xu, Z., and Q. Zhu. 2015. "A Cyber-Physical Game Framework for Secure and Resilient Multi-Agent Autonomous Systems". In *2015 IEEE 54th Annual Conference on Decision and Control (CDC)*, December 15th – 18th, Osaka, Japan, 5156–5161.

Xu, Z., and Q. Zhu. 2016. "Cross-Layer Secure Cyber-Physical Control System Design for Networked 3D Printers". In *American Control Conference (ACC),* July 6th – 8th, Boston, MA, USA,1191–1196.

Xu, Z., and Q. Zhu. 2017a. "A Game-Theoretic Approach to Secure Control of Communication-Based Train Control Systems Under Jamming Attacks". In *Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles*, April 18th – 21st, Pittsburgh, PA, USA, 27–34.

Xu, Z., and Q. Zhu. 2017b. "Secure and Practical Output Feedback Control for Cloud-Enabled Cyber-Physical Systems". In *Communications and Network Security (CNS), 2017 IEEE Conference on*, October 9th – 11th, Las Vegas, NV, USA, 416–420.

Yuan, Y., Q. Zhu, F. Sun, Q. Wang, and T. Basar. 2013. "Resilient Control of Cyber-Physical Systems Against Denial-Of-Service Attacks". In *6th International Symposium on Resilient Control Systems (ISRCS)*, August 13th – 15th, San Francisco, USA, 54–59.

Zhang, R., and Q. Zhu. 2015. "Secure and Resilient Distributed Machine Learning under Adversarial Environments". In *2015 18th International Conference on Information Fusion (Fusion)*, July 6th – 9th, Washington, DC, USA, 644–651.

Zhang, R., and Q. Zhu. 2016. "Student Research Highlight: Secure and Resilient Distributed Machine Learning under Adversarial Environments". *IEEE Aerospace and Electronic Systems Magazine* 31(3):34–36.

Zhang, R., and Q. Zhu. 2017a. "A Game-Theoretic Analysis of Label Flipping Attacks on Distributed Support Vector Machines". In *2017 51st Annual Conference on Information Sciences and Systems (CISS)*, March 22nd – 24th, Baltimore, MD, USA, 1–6.

Zhang, R., and Q. Zhu. 2017b. "A Game-Theoretic Defense Against Data Poisoning Attacks in Distributed Support Vector Machines". In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, December 12th – 15th, Melbourne, Australia, 4582–4587.

Zhang, R. and Q. Zhu. 2018. "A Game-Theoretic Approach to Design Secure and Resilient Distributed Support Vector Machines". *IEEE Transactions on Neural Networks and Learning Systems* 29(11):5512-5527.

Zhang, R., Q. Zhu, and Y. Hayel. 2017. "A Bi-Level Game Approach to Attack-Aware Cyber Insurance Of Computer Networks". *IEEE Journal on Selected Areas in Communications* 35(3):779–794.

Zhang, T., and Q. Zhu. 2017c. "Strategic Defense Against Deceptive Civilian GPS Spoofing of Unmanned Aerial Vehicles". In *International Conference on Decision and Game Theory for Security*, October 23rd – 25th, Vienna, Austria, 213–233.

Zhu, Q. and T. Basar. 2009. "Dynamic Policy-Based IDS Configuration". In *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*, May 28th – 30th, Yinchuan, China, 8600–8605.

Zhu, Q. and T. Basar. 2013d. "Game-Theoretic Approach to Feedback-Driven Multi-Stage Moving Target Defense". In *International Conference on Decision and Game Theory for Security*, October 23rd – 25th, Vienna, Austria, 246–263.

Zhu, Q. and T. Basar. 2015. "Game-Theoretic Methods for Robustness, Security, And Resilience of Cyber Physical Control Systems: Games-In-Games Principle for Optimal Cross-Layer Resilient Control Systems". *Control Systems, IEEE* 35(1):46–65.

Zhu, Q., L. Bushnell, and T. Basar. 2012b. "Game-Theoretic Analysis of Node Capture and Cloning Attack with Multiple Attackers in Wireless Sensor Networks". In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, December 10th – 13th, Maui, Hawaii, USA, 3404–3411.

Zhu, Q., A. Clark, R. Poovendran, and T. Basar. 2012c. "Deceptive Routing Games". In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, December 10th – 13th, Maui, Hawaii, USA, 2704–2711.

Zhu, Q., A. Clark, R. Poovendran, and T. Basar. 2013e. "Deployment and Exploitation of Deceptive Honeybots in Social Networks". In *2013 IEEE 52nd Annual Conference on Decision and Control (CDC)*, December 10th – 13th, Florence, Italy, 212–219.

Zhu, Q., H. Li, Z. Han, and T. Basar. 2010a. "A Stochastic Game Model for Jamming in Multi-Channel Cognitive Radio Systems.". In *IEEE International Conference on Communications,* May 23rd – 27th, Cape Town, South Africa, 1–6.

Zhu, Q., and S. Rass. 2018. "On Multi-Phase and Multi-Stage Game-Theoretic Modeling of Advanced Persistent Threats". *IEEE Access* 6:13958–13971.

Zhu, Q., H. Tembine, and T. Basar. 2010g. "Heterogeneous Learning in Zero-Sum Stochastic Games with Incomplete Information". In *2010 49th IEEE Conference on Decision and Control (CDC)*, December 15th – 17th, Atlanta, GA, USA, 219–224.

Zhu, Q., H. Tembine, and T. Basar. 2010h. "Network Security Configurations: A Nonzero-Sum Stochastic Game Approach". In *American Control Conference (ACC)*, June 30th – July 2nd, Baltimore, MA, USA, 1059–1064.

Zhu, Q., H. Tembine, and T. Basar. 2013f. "Hybrid Learning in Stochastic Games and its Applications in Network Security". *Reinforcement Learning and Approximate Dynamic Programming for Feedback Control*, edited by Frank L. Lewis and Derong Liu, 305–329. New York: Wiley – Institute of Electrical and Electronics Engineers, Inc. Press.

Zhu, Q., Z. Yuan, J. B. Song, Z. Han, and T. Basar. 2010i. "Dynamic Interference Minimization Routing Game for On-Demand Cognitive Pilot Channel". In *Global Telecommunications Conference (GLOBECOM 2010)*, December 6th – 10th , Miami, Florida, USA, 1–6.

Zhu, Q., Z. Yuan, J. B. Song, Z. Han, and T. Basar. 2012. "Interference Aware Routing Game for Cognitive Radio Multi-Hop Networks". *IEEE Journal on Selected Areas in Communications* 30(10):2006–2015.

Zhuang, J., V. M. Bier, and O. Alagoz. 2010. "Modeling Secrecy and Deception in A Multiple-Period Attacker–Defender Signaling Game". *European Journal of Operational Research* 203(2):409–418.

AUTHOR BIOGRAPHIES

SACHIN SHETTY is an Associate Professor at the Virginia Modeling, Analysis and Simulation Center at Old Dominion University. He holds a Masters degree in Computer Science and a PhD in Modeling and Simulation. His research interests are at the intersection of machine learning and cybersecurity. He is a senior member of IEEE. His email is sshetty@odu.edu.

INDRAJIT RAY is a Professor in the Department of Computer Science at the Colorado State University. He received his M.E. in Computer Science and Engineering and Ph.D. in Information Technology. His research interests are in areas of data and application security, network security, security modeling, risk management, trust models, privacy and digital forensics. His email address is indrajit@cs.colostate.edu.

NURCIN CELIK is an Associate Professor and the Director of Simulation and Optimization Research Laboratory in the Department of Industrial Engineering at the University of Miami. She received her M.S. and Ph.D. degrees in Systems and Industrial Engineering. Her research interests include architectural design and application of dynamic data-driven adaptive simulations for distributed systems including power and cyber systems. Her email address is celik@miami.edu.

MICHAEL MESHAM is an undergraduate student and research assistant at the Simulation and Optimization Research Laboratory in the Department of Industrial Engineering at the University of Miami. His research interests lie in the areas of modeling, simulation, and optimization with a focus on cyber-physical networks. His email address is mxm2301@miami.edu.

NATHANIEL D. BASTIAN is an Operations Research Scientist and Assistant Professor of Operations Research and Data Science within the Army Cyber Institute at the U.S. Military Academy at West Point. He holds a Ph.D. in Industrial Engineering and Operations Research from the Pennsylvania State University, an M.Eng. in Industrial Engineering from Penn State, an M.S. in Econometrics and Operations Research from Maastricht University, and a B.S. in Engineering Management (Electrical Engineering) with Honors from the U.S. Military Academy. His primary research interests include multiple objective optimization and decision-making under uncertainty for resource allocation problems, as well as predictive modeling and pattern recognition using machine/deep learning for artificial intelligence at scale. His email address is nathaniel.bastian@westpoint.edu.

QUANYAN ZHU is an Assistant Professor in the Department of Electrical and Computer Engineering at the New York University. He received his M.S. and Ph.D. in Electrical and Computer Engineering. His research interests are in areas of Game Theory and Applications Resilient and Secure Socio-Cyber-Physical Systems. His email address is quanyan.zhu@nyu.edu.