Preface

This book introduces several new advances in security and defense. Unlike previous work, much of this relies on modern computational abilities to model scenarios in much more detail than has previously been possible. Key to much of this work is the principle of complex behavior emerging from local interaction of a large number of simple components. By this, it is possible to design a system of many small components with very simple interactions. The emphasis when modeling this system is placed on a system approach, where the components and their relationships are identified. By executing this system, extremely complex behavior can be generated.

In this respect, this approach differs from previous work that emphasized modeling of a problem in a top-down manner or by modeling the global behavior directly without considering the local interaction that contributes to this global behavior. For example, in the military sphere, the Lanchester equations represent a time-dependent abstract value for some attacker's and defender's strengths, where each of those strengths are modified dependent on their opponent's strength and some function. Equations of this type have the advantages that they are easy to simulate and easy to evaluate. However, they suffer from many disadvantages.

First, often it is difficult to modify these equations to incorporate more complex interactions; for example, to add in concepts of morale, ammunition, resupply or terrain. Partly, this is due to the nature of the differential equation, which is exclusively limited to specifying the change of different components as a function over the different elements of the system of equations. Thus, as the model becomes more complex, describing the differential equation be-

comes exponentially more difficult. These models are also often deterministic; the parameters of a model are specified, including, maybe, the strengths of the opposing forces and their effectiveness. However, each time the simulation runs, if the same parameters are used, the same results will occur. In this sense, these equations often give an average view of the event being studied, but fail to give a more robust understanding of the variations that may occur.

The stronger approach, used by many of the works in this text, is to model a topology within which interaction may occur. This topology might be a battlefield, or a computer or social network. The key difference is that each location in that topology will model how the contents of that location may change based on its current state, "neighboring" states and possibly global effects. Often, these models use older, perhaps modified, differential equations – but as a way of solving subparts of the problem, rather than the entire problem. For example, a battlefield topology might model various units at various positions upon it, and then when these units establish contact with enemy units, a short time-step of a modified Lanchester equation may be used to determine the results of any combat.

The term "agent-based simulation" is applied to those simulations that model units or individuals within their topology, where those units implement some model of behavior to describe how they interact with their model. These models may be simple or more complicated, but the key aspect of this simulation is that the larger simulation has been broken into a number of smaller components. This means that the behavior for each part of the simulation may be somewhat individually specified, leading to the development of the simulation being simpler than it otherwise would be. This often makes it easy to modify the simulation in order to examine different scenarios. For example, the topology might be altered, some of the units might be altered, certain units might be added or removed, or some of the rules of interaction might be modified. Another difference and strength of these models is that the rules of interaction, and the behavior of the agents, are often implemented with a random component. At its simplest, an agent might randomly wander across the topology; or, certain conditional randomness might occur. For example, an agent might usually move north 80% of the time, and west 20% of the time, but if the agent can see a mountain, then 50% of the time, the agent will move towards that higher ground. The complexity of these agents is largely limited only by the amount of time available to encode the individual and the requirements of the simulation.

The result of this approach is that from the description of the topology and its rules of interaction, rules specifying the actions of agents, and the initial loca-

tion and characteristics of the agents, a large, richly complex simulation will be formed. Subsequently, once this simulation has been created, it typically will be executed multiple times, even with identical parameters, in order to understand the characteristics of the simulation and, in turn, the situation it is modeling.

The first chapter, "All Hazards Analysis: A Complexity Perspective," serves as an extended description of future and current security concerns toward which complex systems are relevant. It also introduces the ways that complex systems may serve to model, understand or serve as training tools within this field. It draws together similarities between the modeling of bushfires, epidemics and biological, chemical, nuclear and terror attacks. By outlining the approaches that have been taken in the previously well-studied fields of bushfires and epidemics, it traces the increasing sophistication of models in those fields, from the early Rothermel models to those that incorporate forms of cellular automata and those that add more complex agents into virtual environments. The chapter points out, and then leaves as a development to be completed, the ways in which the techniques that have been developed for modeling bushfires and epidemics can be improved and also how the same techniques can be modified to address modeling of biological, chemical, nuclear and terrorism scenarios.

The second chapter, "Small & Simple: Application-Specific Multi-Agent Systems," demonstrates a number of instances that conform to the premise outlined by its preceding chapter. This chapter presents more specific arguments for how agent-based systems can be used within a military context. It first reviews a number of agent-based projects that have previously been developed to simulate various forms and types of combat. After then reviewing a number of principles that may be used for the development (or distillation) of an agent-based system, three agent-based systems are presented to give a more concrete understanding of the character and capabilities of these types of systems. The first of these is CROCADILE (Conceptual Research Oriented Combat Agent Distillation Implemented in the Littoral Environment), a complex simulation within which agents may engage in differing types and levels of combat dependent on a wide range of choices from which a particular scenario may be specified. The second, TDSS (Tactical Decision Support System), demonstrates the flexibility of agent-based systems by itself being a tool that sits above CROCADILE. This tool was designed for the study of differing possible courses of action that could then be implemented and examined within CROCADILE. The last, SLIM (System for Life and Intelligence Modeling), is a small, generic model that was customized to form a terrorist/

anti-terrorist simulation. These examples demonstrate a number of advantages of agent-based systems, such as flexibility in terms of both the ease in which differing simulations could be generated and the ways in which the simulations could be used, and also the ability to analyze the critical factors affecting a simulation, where by rerunning a scenario multiple times an understanding of both what "average behavior" entailed and also the relative importance or effect of differing components within a simulation.

The third chapter, "How Hard Is It to Red Team?", presents another agent-based system, called WISDOM (Warfare Intelligent System for Dynamic Optimization of Missions). The chapter starts with introducing the concept of Red Teaming, where a game is established to understand adversary behaviors by simulating them. The authors then look at a detailed analysis for the fitness landscape for a number of scenarios. The fitness landscape analysis identifies the characteristics of the search space for a problem to establish how hard it is to find a good strategy in this search space. The analysis also reveals the relationship between the strategy followed by a combat force and the range of possible strategies that may exist to counteract the former strategy. The chapter focuses on a number of scenarios representing a wide range of strategies used in real life and reveals that aggressive strategies, such as those of a terrorist group, can be counteracted very easily while a defensive strategy is hard to compete with, but not impossible to beat.

The fourth chapter, "Network Robustness for Critical Infrastructure Networks," continues the theme of studying complex real-life problems with computer models. This chapter uses the CAVALIER tool to simulate, visualize and analyze networks. In particular, it demonstrates how that tool can be used to simulate a number of attacks on various types of networks. It is also used to analyze the effect of those attacks, so as to understand the relative venerability of different types of networks. That study is then extended by extracting statistical information on the frequency of terror attacks from ICT's International Terrorism Database, and by then using that knowledge with the results of the CAVALIER simulation, a number of guidelines are developed about the required connectivity of networks in order to give some desired resistance to attacks. In summary, this shows the general capabilities of complex simulations in terms of being able to simulate a complicated scenario and by then studying multiple runs of those scenarios, to develop a higher-level understanding about the characteristics of that scenario. It also demonstrates how known real-world data can then be incorporated into that model in order to develop more concrete results that may be of practical use.

The fifth chapter, "Distributed Intrusion Detection Systems: A Computational Intelligence Approach," once again examines the issue of network security, but this time considers it at a much finer level. In the preceding chapter, nodes of the networks were considered to be a simple entity that could be randomly disrupted if the simulator chose to attack that node. In this chapter, data from the 1998 DARPA intrusion detection evaluation program is used. That data represents a number of connection records, and the problem is to find some algorithm that efficiently calculates which of those connection records represent some form of attack. This chapter then presents a series of studies where various data mining approaches are used to find an efficient description of which records are under some form of attack. This work is an instance of a larger set of work, concerned with extracting patterns from certain data sets. While this chapter is aimed at the specific intrusion detection problem it presents, the approaches used are general ones that can be used on the outputs of many simulations to extract rules describing the behavior that occurs within that particular simulation.

The sixth chapter, "The Game of Defense and Security," extends upon all the previous chapters that used systems specifically developed for research problems to instead consider the properties and use of commercial games. The modern commercial computer game industry is extremely large, with many programmers, and substantial amounts of money being used to develop computer games. As computers have become more powerful, those games have become more and more realistic, and have become of more interest to defense forces around the world. In certain ways, commercial computer games can be thought of, and used, in similar ways as research-produced, complex agent-based scenarios. This chapter investigates some of the implications of this. To begin with, this chapter generally summarizes the different classes of games, and outlines some of the functions that these games have been used for by various militaries. After pointing out some of the more interesting developments in this field, including incidents where militaries have contracted commercial game companies to alter their games to better suit their needs, the chapter continues by pointing out some of the disadvantages, advantages and opportunities presented by either original or customized computer games.

The seventh chapter, "Realized Applications of Positioning Technologies in Counter Terrorism," forms a pair with its succeeding chapter, "The Advancement of Positioning Technologies in Defense Intelligence." This chapter summarizes previous developments in the field of Positioning Technologies, from systems such as GPS, which a user accesses in order to determine their location, to systems such as those used to locate mobile phones that can indicate

to some central point the location of particular objects or individuals. It also covers developments made possible by these technologies, such as navigation units. Subsequently, the chapter considers new applications that have been made possible by these technologies, in both the military and civilian spheres, such as "smart weapons" and fleet tracking systems. The chapter concludes in a similar manner as the theme of the previous chapter; namely, by examining the use of commercial tracking systems in the military or counter-terrorism roles. These systems include several designed for determining the position of individuals, and also national identification schemes potentially incorporating biometric information.

The eighth chapter expands on the previous one by examining how positioning technologies potentially may be used in the future, while also examining in more detail their potential links to defense intelligence. One of the key possibilities that this chapter examines is the wider use of systems that can locate individuals under differing assumptions of both the level of capability of these systems and the scale of their coverage. In particular, this chapter discusses the possibilities of tracing the locations of persons of concern with the aim of interfering with events that they may be planning. Also discussed are the responsive possibilities of these types of technologies; in particular, the ability to give warnings or assistance to individuals known to be close to some particular event. This chapter also analyzes the information systems required to implement the types of possibilities outlined in this chapter, whereby some of the characteristics that are required of information systems to enable the optimal use of positioning technologies are established.

The final chapter, "Simulating Complexity-Based Ethics for Crucial Decision Making in Counter Terrorism," examines how complex systems may be implemented in order to model, understand and act upon differing ethics or belief systems between opposing groups. This chapter describes and critiques Belief Systems Models (BSM). These models are means to describe the various belief systems that belong to various agents, where these models can indicate both shared and conflicted beliefs. Related to this is the issue of how decisions are made in the context of the beliefs of the agents making those decisions. The POWER (Purpose, Options, Which option, Execution, Resources) general planning framework is also covered. This framework attempts to cover the variously competing factors, such as differing pressures or values that influence what decisions are made. The chapter continues with one possible synthesis of these studies, the AcesCT (Agent-based Crucial Ethical Simulations for Counter Terrorism) modeling tool. This tool will enable users to see the effects of manipulating various aspects that relate to the belief systems

embedded in the BSMs of the agents in the simulation. Thus, using related ideas to those introduced in previous chapters, it will be possible to study, in a dynamic manner, the critical aspects of those BSMs, and to thus help develop plans to neutralize or ameliorate the influence of those forces that drive ideologically driven violence.

In summary, this text aims to familiarize readers with the basic nature of complex systems modeling and to then give insight to how that modeling has and can be used within the field of counter-terrorism or military operations. Through the diverse areas where this modeling has been described, it is hoped that readers may gain a greater understanding of the flexibility and capabilities of these systems.