Cyber-FIT: An Agent-Based Modelling Approach to Simulating Cyber Warfare

Geoffrey B. Dobson, Kathleen M. Carley

Carnegie Mellon University, Pittsburgh, PA, USA
{gdobson, kathleen.carley}@cs.cmu.edu

Abstract. This paper introduces the Cyber - Forces Interactions Terrain (FIT) Simulation Framework. This framework provides an apparatus with which to carry out virtual experiments involving cyber warfare engagements. Our agent-based modelling approach is a first attempt at providing the necessary components with which military planners can reason about cyber force projections on varying terrains and against various adversarial forces. We simulate and then predict the results of cyber warfare at the level historically desired by military planners: vulnerabilities, asset degradation, and mission capability rate.

Keywords: cyber warfare, agent-based modelling, simulation, military

1   Introduction

The U.S. Department of Defense (DoD) published its Cyber Strategy [3] in 2015, laying out strategic goals and objectives to defend the cyberspace assets that the nation and its allies depend on. The report calls out the need to "establish an enterprise-wide cyber modeling and simulation capability", and to "assess the capacity of the projected Cyber Mission Force to achieve its mission objectives when confronted with multiple contingencies". In this paper, we introduce the Cyber-FIT (Forces, Interactions, Terrain) Framework, which is designed to model and simulate cyber mission forces defending assigned terrain that is confronting multiple contingencies.

Modeling cyber warfare has proven to be very difficult. There are a multitude of variables, many of which are either dependent on the specific situation encountered, or difficult to measure. At the highest level, we can construct a modeling and simulation world, which can allow us to reason about cyber interactions amongst agents. The agents being: "forces" and "terrain", depicted in Figure 1. By assigning characteristics to the forces, interactions, and terrain, we can observe projected outcomes of cyber engagements.

Fig. 1. Cyber-FIT Simulation Framework Visualization

2 Background

Ormrod, Turnbull, and O'Sullivan [7] defined a data representation of cyber attack to model multiple domains common amongst military units. This work improves our understanding of the consequences of cyber warfare. Hamilton [8] described "executable architectures" that can be used to simulate distributed denial of service attacks against a simulated working network architecture. There are a number of simulation tools that work in this manner, but lack the ability to model the interaction of those architectures, attacks, and cyber forces simultaneously. Fischer, Masi, Shortle, and Chen [6] presented an Optimal Splitting Technique for Rare Events to simulate the effects on network traffic from a worm based cyber attack. This is an example of modeling terrain damage from specific well known attack behavior. Cayirci and Ghergherehchi [5] created a model that defined human behavior responses to cyber attacks that can be used to design training scenarios. Santhi, Yan, and Eidenbenz [4] created CyberSim and simulated a one million node network's response to malware propagation. The attack exploited a specific known vulnerability present in many real systems. For cyber warfare simulation to be realistic, empirically observed computer vulnerabilities must be present in the model. Similarly, military planners must use realistic cyber warfare simulation in order to achieve victory in the newest domain of war.

All of these approaches focus on some aspect of cyber warfare, but none in this field, that we are aware of, exist at a higher level, where we can integrate the behaviors of the systems as a whole. Our approach aims to define the low level interactions, in order to reason about the interplay between humans, technology, and the environment they exist in. We define two classes of agents, terrains and forces, and the interactions that define their behavior. Our primary objective, Cyber-FIT 1.0, is to attempt to answer specific questions about how cyber force packages might perform in realistic missions, thereby defining an expandable framework.

3 The Cyber-FIT Simulation Framework

3.1 Model Definition

The CYBER-FIT framework is an attempt to provide a holistic approach to conducting experiments about the interaction of cyber terrain and forces. It is an agent-based modeling tool built using NetLogo. NetLogo provides a useful interface with which the operator can set parameters, execute the simulation, and then view dependent variables over time. Figure 2 displays the NetLogo interface that controls the model.
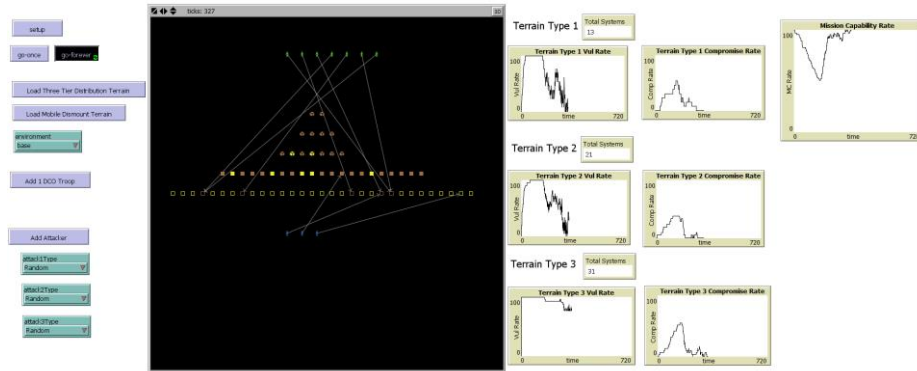
Fig. 2. Cyber-FIT 1.0 NetLogo User Interface

3.2 Terrain

Terrain is defined as the computer systems that military units depend on to execute their assigned mission. We use three terrain types, as defined in Table 1.

Table 1. Terrain Types

Terrain Type	Summary Description	Percentage of Sampled Vulnerabilities
1	Networking systems such as routers and switches	14%
2	Server systems such as web servers, domain controllers, file servers, and intrusion prevention systems	28%
3	User systems such as personal computers, devices, and tablets	58%

The different terrain types will become vulnerable at different rates. The vulnerability rates were computed by taking the known number of vulnerabilities on each of the terrain types from a sample of systems from MITRE's common vulnerability and exposures database, an industry standard for defining, assigning and tracking vulnerabilities [1,2]. The vulnerability rates are associated with a probability based on the relative number of known vulnerabilities, also shown in Table 1.

The different terrain type vulnerability rates will also be affected by the environment that they are deployed in. The current model defines three environment types that represent common military areas of responsibility. The environments are "base", "tactical", and "industrial". Table 2 provides a description of the three environments currently modeled that will affect terrain characteristics.

Table 2. Terrain Environments

Environment	Summary Description
Base	The Base environment refers to a long term fixed military installation
Tactical	The Tactical environment refers to a temporary military installation stood up for the purpose of an overseas conflict
Industrial	The Industrial environment refers to a non-military facility that controls an energy production operation the military depends on

The different environments will affect how quickly systems become vulnerable, by terrain type. Based on interviews with vulnerability experts, the terrain types were scored relative to each other, to determine within which environment vulnerabilities appear at higher or lower rates. Table 3 defines the relative vulnerability rate across the three environments and details the probability that the system in that given environment will become vulnerable at any time. This information is incorporated into the code that determines if a given terrain is vulnerable at any given time. That is, in a cell labeled "High", the probability of a system moving from non-vulnerable to vulnerable is equal to the relative share of common vulnerabilities and exposures (CVEs) as defined by MITRE [1,2]. In a cell labeled "Medium", the probability is reduced 50%. In a cell labeled "Low", the probability is reduced 50% again.

Table 3. Relative Vulnerability Rates by Terrain Type across Environments

Terrain Type	Base	Tactical	Industrial
Type 1 (Networking)	Low	Medium	High
Type 2 (Servers)	Low	High	Medium
Type 3 (Users)	High	Medium	Low

3.3 Forces

Forces are defined as the military members that are deployed to the military scenario. The current version of Cyber-FIT only supports defensive and offensive cyber forces, but future versions will support all force types. The defensive forces are deployed with the purpose of protecting the assigned cyber terrain. The model currently allows the operator to add any number of defensive forces, up to sixteen. The defensive forces will remove vulnerabilities that exist on the terrain at any given hour (each time tick in NetLogo). The defensive forces select vulnerable systems randomly, according to a schedule. At all hours, the forces defend Terrain Type 3, every third hour they defend Terrain Type 2, and every sixth hour they defend Terrain Type 1. This models the real-world constraint that servers and networking equipment can only be defended at certain times, e.g., when they are being patched. The offensive forces will attack the systems based on what type of attack is being launched. The model currently supports three attack types that offensive forces can launch, as defined in Table 4.

Table 4. Offensive Force Attacks

Attack	Target Terrain
Random	All Types
Routing Protocol Attack	Type 1 (Networking Systems)
Denial of Service	Type 2 (Server Systems)
Phishing	Type 3 (User Systems)

3.4 Interactions

Interactions are defined as any instance when a force is actively accessing cyber terrain. In the real world this could be performing operations and maintenance, coding malware, applying patches, etc. In the current version of Cyber-FIT, two types of interactions are modeled: offensive actions and defensive actions, which are limited to offensive and defensive forces, respectively. The defensive forces will perform operations and maintenance activities, and apply patches at every hour to a randomly selected vulnerable system. That system will become non-vulnerable following this interaction. The offensive forces will attack randomly selected systems of the type associated with the attack selected, at every hour.

In order for a system to become compromised, it must be vulnerable at the time that it was attacked (an offensive interaction by offensive force). If vulnerable, then the system has a 5% chance of becoming compromised. Currently all systems are modeled to have a 5% compromise rate, given that the offensive force has access and the system is vulnerable.

3.5 Model Outputs

The model currently outputs seven dependent variables: vulnerability rate per terrain type, compromise rate per terrain type, and overall mission capability rate. Table 5 describes each dependent variable.

Table 5. Dependent Variable Descriptions

DV	Description
Mission Capability Rate	Average Percentage of systems (all types) available
Vulnerability Rate	Average Percentage of systems vulnerable (by type)
Compromise Rate	Average Percentage of systems compromised (by type)

4 Virtual Experiments

We conducted three virtual experiments using the current model, seeking to answer questions a planner might have. For each experiment we provide the virtual experiment motivation, the results of the experiment, and discussion.

4.1 How many forces should we deploy to minimize the effect of a routing protocol attack (RPA) in an industrial environment?

In this experiment, we are considering a specific attack (RPA), in a specific environment (base). We'll vary the number of forces from one through fifteen and examine the decrease on Type 1 system (networking) compromise rate. We're specifically searching for the number of forces, where, when adding one more troop, the projected compromise rate is within one standard deviation of the current projected force package effectiveness. We expect that as the number of forces increases, decrease in compromise rate will level off. Results are shown in Figures 3 and Table 6.

As shown in Figure 3, we can expect a substantial increase in effectiveness moving from one troop to five. After five troops, the projected performance improvement tapers off. We still see improvements on the projected compromise rate of Terrain Type 1, our primary concern in this simulated mission, but it will be decreasing as we continue to add forces. To find the point when adding troops will make no difference at all, we search for the point where the increase in effectiveness is within one standard deviation of the current projected average Type 1 compromise rate. This is laid out in Table 7. This point is found, at forces = 11. At that point, the projected compromise rate is 4.64 with a standard deviation of 0.77. The projected compromise rate, when adding one more troop to the mission, is 4.06, within one standard deviation of the previous projection.
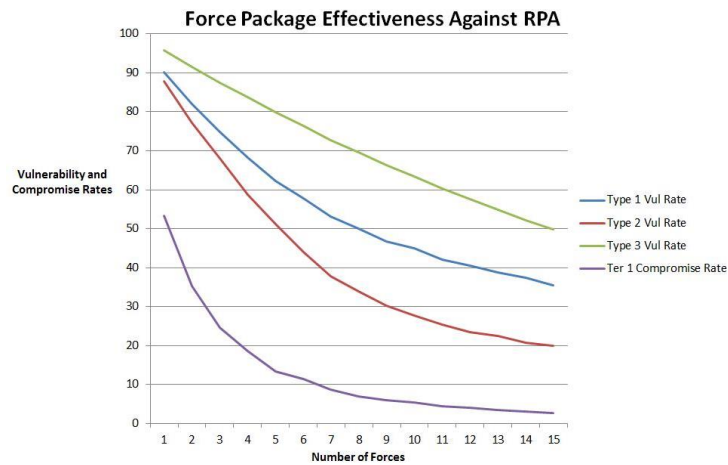

Fig. 3. Projected Force Package Effectiveness against RPA

Table 6. Projected Compromise Rate and Standard Deviation of Type 1 Systems

Forces	Compromise Rate	Standard Deviation	Forces	Compromise Rate	Standard Deviation
1	53.51	2.68	9	6.06	0.52
2	35.33	3.20	10	5.36	0.72
3	24.68	2.44	11	4.37	0.77

4	18.60	1.79	12	4.06	0.82
5	13.74	1.88	13	3.39	0.37
6	11.34	0.96	14	3.13	0.54
7	8.70	0.99	15	2.73	0.37
8	6.96	0.74			

This shows the importance of weighing the cost of adding more resources with the effectiveness of those resources. In this scenario, what do these numbers represent? We have a simulated mission on terrain that includes 21 Type 1 systems. So, if the average compromise rate, at forces = 5, is 13.74, then we can expect, on average, 2.89 systems are always compromised when facing a routing protocol attack. At forces = 6, we can expect, on average, 2.38 systems are always compromised when facing a routing protocol attack. So, somewhere between two and three systems will go down. Perhaps this is acceptable risk? Also, once the attack is recognized, will five forces be enough to make an emergency change, repair the compromised terrain, and block the attack? This might be the case, which means that the planner should actually choose to deploy five forces, rather than eleven, due to acceptable level of risk, external constraints, and knowledge of mission resources.

4.2 What will be the expected effect on cyber terrain if the adversary switches from a fifteen day routing protocol attack, to a denial of service attack in a base environment with six troops deployed?

In this experiment, we are considering the difference in how the forces and terrain will perform against two different types of attacks. Military deception has been around for as long as human warfare. This occurs quite frequently in the cyber domain. Offensive forces will start one attack, in order to focus resources on specific terrain, only to then switch the attack on different terrain. This is the attack vector we are modeling in this experiment. The adversarial force will begin with an RPA, and then switch to DOS attack halfway through the deployment time frame. Figure 4 shows the change in compromise rate of Type 1 and Type 2 systems, of one run of the virtual experiment. Table 7 shows the average compromise rate of the Type 1 and Type 2 systems, after all virtual experiment runs.
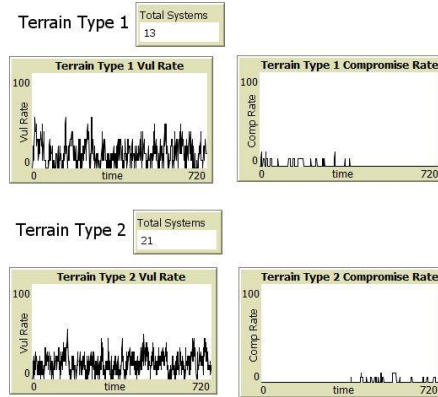
Fig. 4. Visualization of Simulation Results

Table 7. Average Compromise Rate of Type 1 and Type 2 Systems

Summary of Simulations	
Number of Forces	6
Environment	Base
Terrain Architecture	Three Tier Distribution
Compromise Rate of Type 1 Systems	1.24
Compromise Rate of Type 2 Systems	0.89

The importance of visualization is displayed in Figure 4. The Cyber-FIT interface displays real-time feedback to the user showing exactly what is occurring on the terrain at every time interval. This aids planners and researchers by allowing them to carry out test runs and ensure what they have conceived, conceptually, matches what the model is providing. In Figure 4, we can see that in the given circumstances, the terrain will hold up quite well against both attacks. The terrain and number of forces deployed, in the base environment will handle a DOS attack better than an RPA. This means that planners and enterprise architects can address this difference. If the difference isn't acceptable, leadership could send additional resources to the Type 1 systems in the way of additional forces or a better maintenance schedule, to decrease the expected compromise rate.

4.3 What number of forces maximizes expected cyber terrain mission capability rate against random attacks in a tactical environment?

In this experiment, we are considering a tactical deployment and attempting to determine which number of forces maximizes the mission capability rate when the adversary is launching random attacks against the cyber terrain. When military planners are considering what resources to send to battle, they will attempt to package forces and equipment that will perform at a high level. Since resources are limited, a challenging part of their job is deciding which number of forces will maximize the likelihood that

each unit will accomplish its mission. For this experiment, we are modeling a situation where the planners are considering a deployment of cyber terrain which will likely be attacked in multiple ways. So, we selected random cyber attacks for the adversary. Then, we simulated cyber battles against the terrain, each time increasing the number of forces. Figure 5 shows the results of the simulations.
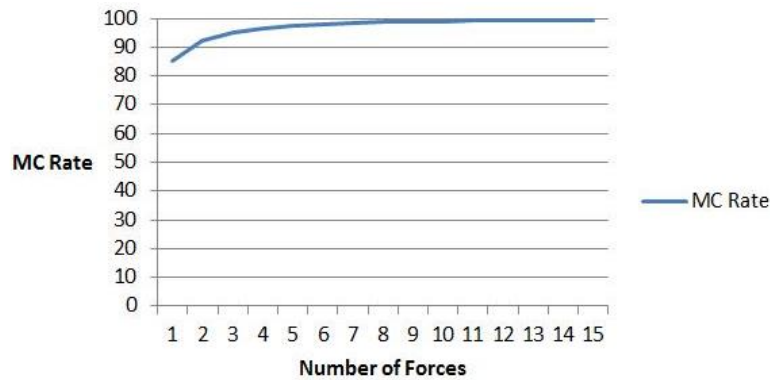

Fig. 5. Projected Mission Capability Rate as Forces Increase

Figure 5 shows that the projected mission capability rate will increase sharply as forces are added. A force package of six troops should provide a mission capability rate above 98.0%. A force package of ten troops should eclipse a 99.0% mission capability rate. The highest number of troops deployed for this set of experiments was 15, resulting in an average mission capability rate of 99.55%. This information would prove valuable for determining the number of troops to deploy to this type of mission.

5 Discussion

The Cyber-FIT simulation framework, in current form, presents a successful proof of concept. The three elements of the model (forces, interactions, and terrain) are all conceptual at this time. Forces differ in vulnerability patching routines, and attack targets. Further development of forces could include: skill level, specialty, and experience. Terrains differ in types of systems present, vulnerability state, and environmental deployment. Further development of terrain could include: increasing types of systems, realistic lists of vulnerabilities, cost, and access control.

There are nearly limitless potential extensions to this work. For example, in future work we plan to explore various improved definitions of mission capability rate. To define that, we'll model various units that depend on different parts of the terrain for mission success. Mission capability rate will be defined as the ability to provide working systems, when demanded, to various units. Another example would be adding different types of adversary complexities. Hacktivist organizations, organized crime rings, and nation states would all have different adversarial capabilities and

limitations. Then the simulation could predict performance of the forces and terrain against different classes of adversaries

6 Conclusion

We introduced the Cyber-FIT simulation framework, an agent-based cyber warfare simulation framework. We showed that the framework can enable virtual experiments that answer questions about military cyber force projections. Three virtual experiments were conducted, each testing specific questions currently being considered by military planners all over the world. In the first experiment, we found that adding any number over 11 troops does not improve terrain performance. In the second virtual experiment, we found that the terrain would handle a denial of service attack better than a routing protocol attack. In the third virtual experiment we found that a force package of ten troops would provide a cyber terrain mission capability rate above 99%.

The Cyber-FIT simulation framework will be further developed by adding empirical data. This will provide more realistic virtual experiments. Future work will focus on presenting simulations to Department of Defense experts interested in specific questions that cannot be addressed in real world scenarios due to limitations of time and resources. Our long term goal is to continually add modules that can take disparate model results as input to our model.

References

1. MITRE Common Vulnerabilities and Exposures. http://cve.mitre.org/
2. MITRE CVE Details. http://www.cvedetails.com/
3. Department of Defense (2015) The DoD Cyber Strategy. DoD, Washington D.C.
4. Santhi, N., Yan, G., Eidenbenz, S (2010) CyberSim: Geographic, temporal, and organizational dynamics of malware propagation. In: Proceedings of the 2010 Winter Simulation Conference, pp. 2876 - 2887
5. Cayirci, E., Chergherehchi, R (2011) Modeling cyber attacks and their effects on decision process. In: Proceedings of the 2011 Winter Simulation Conference, pp. 2632 - 2641
6. Fischer, M. J., Masi, D. M. B., Shortle, J. F., Chen, C. H (2010) Simulating non-stationary congestion systems using splitting with applications to cyber security. In: Proceedings of the 2010 Winter Simulation Conference, pp. 2865 - 2875
7. Omrud, D., Turnbull, B., O'Sullivan, K. O (2015) System of systems cyber effects simulation ontology. In: Proceedings of the 2015 Winter Simulation Conference, pp. 2475 – 2486
8. Hamilton, Jr. J. A (2006) DoDAF-Based Information Assurance Architectures. CrossTalk, vol 19. pp. 4-7