Did the Cyber Team Win?

Geoffrey Dobson and Kathleen Carley
Carnegie Mellon University, Pittsburgh, PA, USA

gdobson@cs.cmu.edu
kathleen.carley@cs.cmu.edu

Abstract: Cyber team performance in military conflict scenarios is very difficult to quantify due to its ambiguous nature. This research effort aims to improve our understanding of how cyber teams affect the terrain they are charged with protecting, and which other forces depend on. An agent-based modeling and simulation software called the Cyber Forces-Interactions-Terrain (Cyber-FIT) framework is used to simulate realistic cyber team missions in contested cyberspace and then quantify their performance from observable data sources. The software ingests configuration files to setup agent characteristics and then, after simulation runs, outputs data files that are used for statistical analysis. Two virtual experiments are conducted in this work. The first tests different team setups in terms of skill level against varying adversary complexity levels to demonstrate the importance of human resourcing in the cyber forces. The second analyses deployment delay time to an active conflict which depicts the efficacy of agent-based modeling of cyber assets for wargaming applications. All face validated simulations are based on a combination of industry frameworks, survey data, and empirical data to give a sufficiently realistic representation of cyber conflict. As military forces become ever more dependent on cyberspace to realize effects and project power, the understanding of cyberspace as a terrain of war becomes more critical. This research takes on the difficult task of defining and computationally modeling the abstract phenomenon that is cyberspace. This gives battle commander and military leadership a better answer to: did the cyber team win?

Keywords: Agent-based, Modeling, Simulation, Cyber

1. Introduction

Cyber teams have seen tremendous growth over the past decade with quarter four 2021 being the highest venture funding ever in the cyber security market at $7.8B (Metinko, 2022) and strong cybersecurity hiring through 2023 (Sabin, 2023). The United States government is also making large investments in cyber security. A recently approved infrastructure bill (Department of Homeland Security, 2022) includes $1B for state and local governments to improve the cyber security of their infrastructure. Cyber security continues its upward trend of importance and priority amongst all sectors and industries, even though it remains very difficult to measure. Leaders still struggle to articulate how secure their systems are. This work aims to help alleviate the abstruse nature of cyber security management efforts. Cyberspace is hard to quantify, measure and communicate about which results in a gap of understanding between leadership and practitioners. Simulation can help this effort by defining computational models in virtual environments that allow specific measurements to take place in fictional scenarios. Like “table-top” exercises, practitioners can work through difficult simulated situations before emergencies take place in the real world. Team performance measurement depends on defining the outcomes desired and working backwards through the behaviours that lead to these outcomes.

Measuring team performance is very difficult in most business settings. For military training scenarios, the SPOTLITE method focused on specific observables that should be accomplished throughout a training event so that team dynamics could be captured and evaluated (MacMillan, et al., 2013). Some research suggests that there are significant differences between self-assessment and observer ratings, and self-assessments don’t always correlate with team performance (Andersson, et al., 2017). This makes it difficult to rely on post-hoc surveys as a form of team performance measurement. A recent literature review of 81 papers studying team performance measurement showed that most of those papers relied on self-assessment for the performance metrics (Pavez, et al., 2022). Self-assessments are certainly valuable, but organizations should look towards objective data that can be captured independent of team member’s own biases. Research assessing the impact of studying military teams called for incorporating environmental factors and simulating those variables (Goodwin, et al., 2018) to understand what individuals need from emerging autonomous solutions to improve their performance. Rich computational models of teams performing in the cyber and information environments are critical for digital twins of simulated military missions.

1.1 Agent-Based Modeling for Cyber Security

Agent-based modeling and simulation is an excellent research tool for problems like this because it forces the researcher to define the actors and actions at play and then apply those to realistic management decision making analysis (Harrison, et al., 2007). Military specific applications lend themselves well to this technique due to scenario-based simulations such as how quickly malware spreads amongst cyber assets within mobile units

employing different defence strategies (Thompson & Morris-King, 2018). Another work employed agent-based modeling to test defence analyst collaboration decisions showing heterogeneous team makeup outperforms homogeneity when responding to security alerts (Prashanth, et al., 2013). Organizational strategies for training and creating policies to fend off cyber attackers can be modelled in agent-based systems (Shin, et al., 2022).

Recently, agent-based modeling and simulation research has been applied to understanding the "battlefield of the future" due to rapid gains in technology being used in conflict. Some work has been applied to understanding how drones can be utilized to enhance surveillance and intelligence units (Christensen & Salmon, 2022). In a cyberspace environment, autonomous agents, both offensive and defensive, are envisioned that will take actions based on cyber operator knowledge bases (Kott & Theron, 2020). The information environment has always been an aspect of military concern and with the ubiquotous use of social media, it can be analyzed like never before. Computatinally modeling the information environemnt by simulating maneuver strategies can present courses of action for mliitary organizaitons (Blane, et al., 2021). These research projects are moving the state of art towards a fideility level commensurate with the needs for military leadership seeking situation awareness leading up to and during conflicts.

1.2 Cyber-FIT Simulation Framework

The Cyber-FIT simulation framework was originally conceived to model the basic activities that are occurring between adversarial parties engaged in a cyber conflict. This generally means that two sides are vying for control of cyberspace terrain. The first version of Cyber-FIT explored this concept by defining force sides, terrain types and then simulating potential outcomes that would be important to military planning (Dobson & Carley, 2017). The next two versions added empirical adversarial behaviour (Dobson, et al., 2018) and a theoretical cognitive model to explore cyber situation awareness (Dobson & Carley, 2018). The overarching development concept for Cyber-FIT was, and continues to be, start basic and add complexity in a spiral development methodology. Cyber-FIT defines two main agent types: forces and terrain. The forces are the humans involved in conflict and the terrain are the networked computer systems representing cyberspace assets utilized by forces. The agents interact with each other as shown in the following figure.

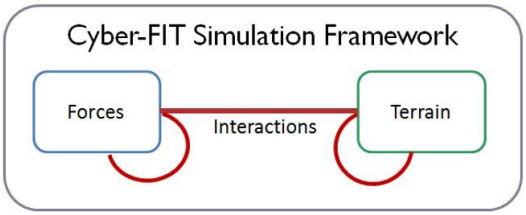

Figure 1: Cyber-FIT framework

All agents can interact with all other agent types, and interactions are modelled as directed links. The environment rulesets and behaviours evolved over time to address varying research questions posed by military leaders and researchers. These questions largely crossover to non-military environments because most corporations are dealing with protecting cyberspace assets from threats in a similar manner to military interests. Cyber-FIT versions progressed through increased complexity resulting in the most recent version that was built for the simulations and virtual experiments covered in this paper. Cyber-FIT version four (Dobson & Carley, 2021) was developed primarily to define cyber team performance measures. This was done by talking to subject matter experts and considering the following question: How would you know if the cyber team was making a difference? This version tracks output data informing 16 cyber team performance measures in a realistically scaled conflict simulation (hundreds of simulated endpoints being used by simulated military forces).

2. Simulation and Virtual Experiment Methodology

In this work Cyber-FIT is used to simulate a force-on-force conflict between one cyber protection team and one adversarial force group. The contested cyberspace consists of 500 computer terrain agents being used by 5 kinetic mission friendly force units. This simulation setup will be used for both of the following virtual experiments described.

2.1 Virtual Experiment one on Knowledge, Skills, and Experience Setup

The interaction of knowledge, skills, and experience certainly plays a role in how teams perform. When envisioning a perfect cyber team, managers might envision starting from scratch by hiring ideal candidates based

on education and experience which are shown on resumes. This assumes that the actual knowledge, skill and experience of the candidate can be gleaned from the words on the paper resume. This strategy may be ideal but probably unrealistic in both military and industry situations. In the military, commanders are selected for a position and assigned to that location with an already existing cyber team. When the commander arrives, they do not then begin hiring the ideal candidates, the team in place is already assigned to them. Similarly, in the private sector, cyber managers (who may have more flexibility with hiring) come into an already existing organization and then must compete with other firms vying for the same cyber talent. Also, even if cyber leaders do have the ability to add cyber talent, this takes time. Which means that improving the cyber team outcomes might be more likely accomplished through internal team development. So, how should cyber leaders develop the team?

Cyber leaders are usually interested in developing their teams through training. This is especially true with military cyber teams who are almost always "on mission" or "training". Training will usually come in the form of individualized classroom style educational services and products where the primary outcome goal is knowledge acquisition. There is a skill identified that some personnel are lacking, and the training resolves that gap in knowledge. Some of these trainings provide certifications that are recognized by industry by meeting a standard. Returning to the concept of individual knowledge, skills, and experience, trainings are either meant to increase the knowledge level or the skill level of the individual or both. For example, the Security+ certification is providing knowledge only. Whereas a weeklong web development software language training with a capstone project is adding to both knowledge and skill. A cyber leader sending a group of individuals to a cyber war exercise, or competition is an example of adding to the skill level only. This is what the cyber leader and management must do: decide which trainings are most appropriate given the current environment of the team.

This is the spirit that this virtual experiment exists within. Given that a cyber leader is managing a typical cyber team, which training options should be sought after? It's easily recognizable that some personnel, in any job setting, have better skill than others. Knowledge, while important, probably plays a lesser role, whereas skill seems to be the "x" factor. Skill is also far harder to define, measure, and improve. In any event, if a mechanism for identifying and improving skill is available to leadership, how would that difference manifest within a cyber conflict? To test out this concept Cyber-FIT is used to run a virtual experiment varying team skill and adversary tier and applying a value to that "x" factor.

Skill should be a key determinant in how likely a cyber team member is to restore compromised terrain. Most cyber subject matter experts believe that experience also plays a factor because over time, being exposed to different tools and techniques, and practicing those, will inform current performance. Therefore, skill will act as a multiplicative effect on the amount of experience a cyber team member has in terms of how likely that agent is to restore compromised terrain. While tuning this version of the model, exploratory analysis showed that simply multiplying the square of skill and experience did not make a significant realistic difference in performance. To account for this, a multiplier is added, with each skill and experience combination value being weighted higher in a Fibonacci sequence. The Fibonacci sequence is frequently used in software development relative scoring systems for estimating effort and complexity in project management, so it could be a good candidate for estimating cyber operational capability as well. The defender agent restoral rate (rr) for this experiment will be based on the following equation detailed in the table below where s = skill, e = experience, and m = multiplier and adhering to the following equation.

$$rr = ((s^2 * e) * m) / 5{,}000$$

Table 1: Restoral rate formula based on skill and experience

e	s	$(s^2 * e)$	m	rr
1	2	4	2	8/5,000
2	2	8	3	24/5,000
3	2	12	5	60/5,000
1	3	9	8	72/5,000
2	3	18	13	234/5,000
3	3	27	21	567/5,000

The purpose of this experiment is several: First it will show how skill acquisition can be an extremely important strategy for cyber teams in terms of impacting performance. Second, it will show that Cyber-FIT can simulate

typical battle damage from a cyberspace conflict. Third, it shows how the lowest level details and design decisions (restoral rate variable in defender agent class) must be carefully considered for sufficiently complex modeling. For this experiment an average team will engage in cyber conflict with all six tier levels of an adversary. The cyber team will be size nine, where one agent is the team lead, four are on the network squad and four are on the host squad. The cyber team demographics will be one of five settings for the virtual experiment. The skill level of all agents will be set to 2 on a scale of 1,2, or 3 meaning beginner, intermediate, and expert. Then each variation will replace two intermediate skill personnel with two expert skill personnel. The details of this experiment are detailed in the table below.

Table 2: Virtual experiment one design

Independent Variables		
IV	Variations	Range
Average team skill	5	2, 2.25, 2.5, 2.75, 3
Adversary tier	6	[1-6]
Control Variables		
Average team knowledge	1	2.5
Average team experience	1	2
Vulnerability growth rate	1	.001
Defender restoral rate	1	Table 2
Exploit success rate	1	1.0
Dependent Variables		
DV	Type	
Compromise Time	Integer	
This experiment design is 5X6X10 runs = 300 replications		

2.2 Virtual Experiment one Results and Discussion

This virtual experiment, based on the underlying model assumptions and configuration, shows that adding highly skilled team members will have a large effect on cyber team performance. It also shows that an average military cyber team, with average skill, will fare well against adversaries of tier one through four, but not well against adversary tiers five and six. The following figure shows all simulation results in a scatter plot format.

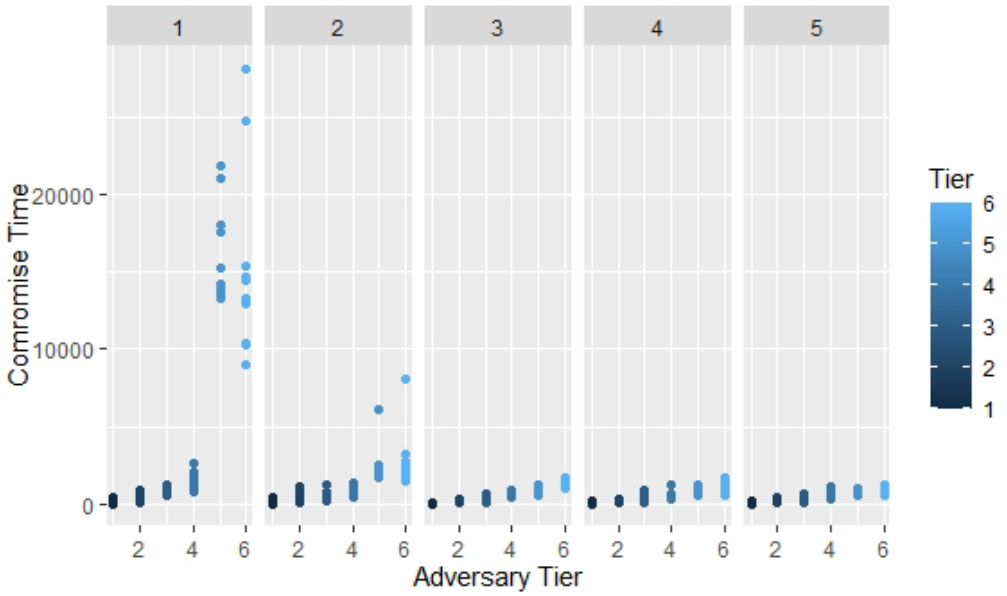

Figure 2: Virtual experiment 1 results scatter plot

As shown, with an average skilled team, the negative effects (cyber damage) seen on the cyber terrain increases sharply as tier level is increased. The results show that a simulated adversaries of tier five and six will be able to break into, compromise, and control large parts of the cyber terrain against an average skilled team. The cyber team will spend a significant amount of time in reactive mode, trying to find and restore compromised systems.

By replacing four (half) of the average skilled agents with expert skilled agents, the setting three cyber team performs significantly better. This team controls the cyber terrain and quickly remediates any compromised systems they come across that have been successfully attacked by adversaries, even tiers five and six. This means the adversary never tips the scale to the point where the team is in constant reactive mode during the remainder of the conflict. The mean compromise time from team setting one to team setting three decreases 93.8%. Just adding a couple "sharp shooters" can have enormous effects. Adding more expert team members continues to have a significant effect on performance, but clearly moving from average team skill 2.0 to 2.5 will have a much bigger impact than moving from 2.5 to 3.0. This is where simulation can inform planners. Does the commander accept the risk of significant cyber damage? If the commander does not accept the risk, where will the additional skill come from? The resulting simulated data from virtual experiment one was run through a regression model with both tier and skill setting as independent variables against the log of compromise time. The regression model is shown in the figure below.

```
Residuals:
    Min      1Q  Median      3Q     Max
-4.9748 -0.4248  0.0784  0.6311  1.9074

Coefficients:
            Estimate Std. Error t value Pr(>|t|)
(Intercept)  4.58084    0.19564  23.415  < 2e-16 ***
t            0.77812    0.03678  21.155  < 2e-16 ***
s           -0.38419    0.04442  -8.649  3.3e-16 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 1.088 on 297 degrees of freedom
Multiple R-squared:  0.6375,    Adjusted R-squared:  0.6351
F-statistic: 261.2 on 2 and 297 DF,  p-value: < 2.2e-16
```

Figure 3: Regression model of virtual experiment 1

As shown, both skill setting and tier are significant predictors of the compromise time. Tier level has a higher estimate meaning it has a greater effect on compromise time. This virtual experiment computationally models what we are trying to accomplish in the real world: Adding enough skill to a team to arrive at the performance desired. For the average team in both military and industry settings, they'll be happy to have an expert or two that can vastly improve the team. Of the thousands of teams operating in the real world, a very small number might be made up of all expert skill level members. Perhaps that most elite hacker teams, special cyber operators, and security operations centres handling high value information are made of all or mostly all expert skill. The rest are doing their best to make a marginal increase in skill level through training and practice opportunities. This virtual experiment can help them approximate their gains by doing assessments of their current strength, and what could be improved upon through training or acquisition.

2.3 Virtual Experiment two on Deployment Time Delay Setup

The exact timing of force deployment in a military conflict is an age-old question. Sun Tzu is attributed with the following statement: "Rapidity is the essence of war: take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots" (Sun, 2009). The cyber adversary will most certainly be looking for "unexpected routes" and "unguarded spots". Cyber team deployment is, in essence, sending guards to the cyber terrain prioritized due to mission requirements. The mission requirements are extremely dynamic and change near constantly because of changing cyberspace terrain, updated intelligence reporting, availability of forces, changing interests, and geopolitical events to name a few. The research question central to this virtual experiment is: How does the timing of the deployment of cyber troops affect the availability of cyberspace terrain? Thinking through questions like this are why militaries run wargames. According to the U.S. Army Field Manual 6-0, "wargaming is a disciplined process, with rules and steps that attempt to visualize the flow of the operation, given the force's strengths and dispositions, threats, capabilities, and possible COAs, impact and

requirements of civilians in the area of operations (AO), and other aspects of the situation" (Department of the Army, 2014).

Cyber-FIT can be used to simulate the outcomes of importance to inform war-gaming efforts. For this virtual experiment, an aspect of a wargame like the real-world event just presented will be undertaken. In a wargame, typical "COAs" (courses of action) involve where to move forces in the terrains in play. This could be all terrains (air, land, sea, space, and cyberspace) or a subset. Imagine that the commanders, at a turn in the game, must decide whether to deploy cyber forces based on intelligence reporting to an area of terrain. The intelligence report provided in the wargame may indicate that sophisticated cyber adversaries are in position to attack cyber assets. The decision (course of action) is deploy or delay. Deploy may be the correct move. Perhaps the adversary is already actively engaged, and the forces need to deploy immediately to hunt-forward and take remediating actions. Delay also may be the correct move if the intelligence reports were not accurate, and the enemy is of lower sophistication and therefore easier to deal with. The delay might allow for those cyber forces to be available in a future turn where they are more useful for other campaign priorities. Thus, wargaming allows the participants to practice moves and then think through the strategic implications.

The motivation of a simulation, experiment, or war-game with deployment delay is a common military issue. The U.S. Army is aware of how fast cyber defenders must recognize and remediate attacks to be effective. The Army has a saying, "the golden hour", referring to how long medical troops must start care for wounded soldiers. In a recent interview (Freedberg, 2019), Lieutenant General Stephen Fogarty, chief of Army Cyber Command contrasted that with cyber troop response requirements: "It's probably the golden five minutes, or that golden 20 to 30 minutes, to recognize what the adversary is putting out there and respond."

For this experiment, a cyber team will deploy to a conflict consisting of five kinetic missions connected to a tactical base infrastructure. The adversary will begin attacking at time t = 0. The cyber team will either: deploy immediately (t = 0), delay one day (t = 1,440), or delay two days (t = 2,880). Also, this experiment will include all adversary tiers, one through six. The outcome measure to consider is compromised systems, which is the number of cyber terrains in a compromised state, at any given time. In real-world operations, the primary job of the cyber team is to keep that number to zero, always enabling all system availability to friendly forces. The table below details the virtual experiment design.

Table 3: Virtual experiment two design

Independent Variables		
IV	Variations	Range
Deployment delay time	3	0,1,2
Adversary tier	6	[1 – 6]
Control Variables		
Average team KSE	1	[2.5, 2, 2]
Vulnerability growth rate	1	.001
Exploit success rate	1	1.0
Dependent Variables		
DV	Type	
Compromise Time	Integer	
This experiment design is 3X6X10 runs = 180 replications		

2.4 Virtual Experiment two Results and Discussion

This virtual experiment, based on the underlying model assumptions and configuration, shows that delaying the deployment of cyber forces will have an increasingly greater impact, as the sophistication of the adversary is increased. This simulation shows that for adversary tiers one through four, the cyber team would be able to overcome the adversary quickly and return to baseline cyber terrain performance where very few compromises are being accomplished. All tiers one through four will be at baseline by day three (t = 4,3200) of the simulated conflict even if the cyber team delays its deployment by two days. Similarly, for tiers one through four, the cyber team will return the cyber terrain to baseline deployment by day two if the team delays deployment by one day. This means that whether the team delays for one day or two days, it will still take the team one day to return to baseline. This is different than the response simulated for tiers five and six. For tiers five and six, a one-day delay

will take more than two days to recover from. For tiers five and six, a two-day delay could be very difficult to recover from as shown in the figure below.

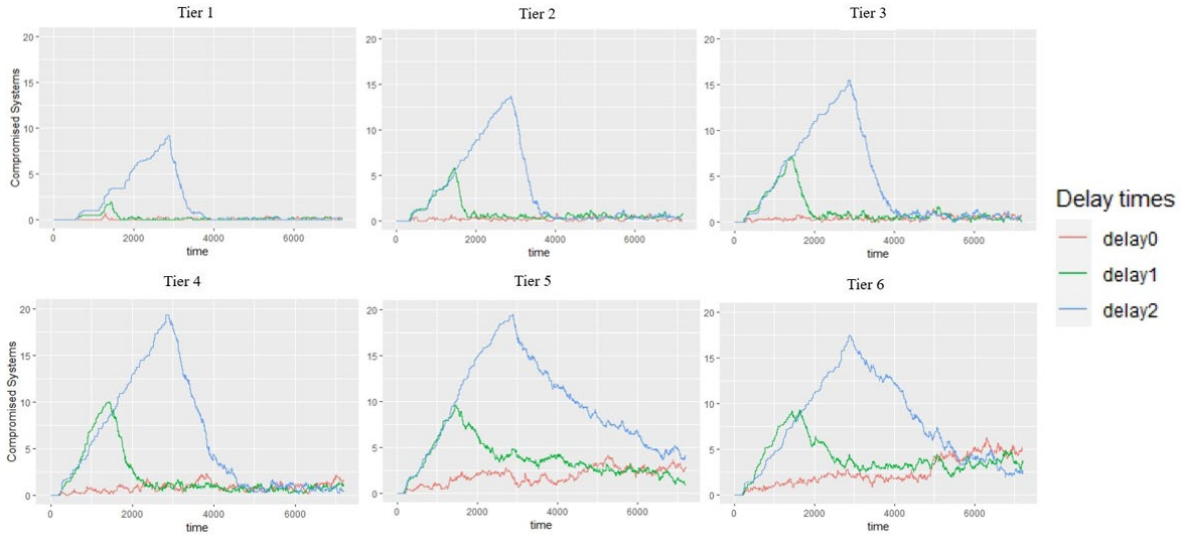

Figure 4: Results of virtual experiment two over all adversary tiers

The utility of a simulation tool for wargaming is apparent here. The details of the game will determine how granular the simulation tool must be, for simulated outcomes. If the wargame is taking turns in a one-day time horizon, then this type of simulation would work perfectly. For example, if the participant chose to delay for two days, and the adversary ended up being tier three, and the cyber terrain was needed on day four, then then the cyber team would have been very likely to restore the terrain by the time it was needed. However, under the same circumstances, if the adversary turned out to be tier five, then the systems would be much more likely to not be available on day four (t = 5,760). The wargame might take a statistical sampling of simulation turns and then provide a key terrain cyber availability value based on the average available. The wargame might also simulate all systems in question each turn. In the former, there would have to be data processing capabilities built into the wargame software. In the latter, higher variance simulation software would have a greater affect in terms of randomization presented to the participants. In any event, this virtual experiment is a proof of concept for how Cyber-FIT, and more generally, agent-based systems could be used for higher fidelity cyber informed wargames.

3. Conclusions

This research presented simulations and virtual experiments made possible by the agent-based modeling and simulation framework Cyber-FIT. The model has been used over the past several years in different ways valuable to research sponsors and partners in this space. For example, it has facilitated the exploration of methods to simulate data streams pertinent to joint all-domain battle management. In another effort it was used to emulate downed nodes that would impact the information environment for exercise design. It can also be used to create and test hypotheses, what-if analysis, and synthetic data generation for analytics. Agent-based systems can contribute to military research efforts across a multitude of domains and functions.

3.1 Limitations in Current Version

Cyber-FIT Version 4.0 is an object-oriented Java based software model implementing the Repast Simphony libraries. The version has several current limitations pertinent to this paper and the virtual experiments described. First, the defender agents do have position types, knowledge, skills, and experience that differentiate behaviour but do not have any human factors. They never get tired, make mistakes, become distracted, etc. Second, the vulnerabilities that occur within the terrain agents, and are exploited by attacker agents are numbered 0 – 99 (0 representing a complex adversary creating a zero-day vulnerability) and represent complexity level. This is a proxy to model attacker tier level and defender agent knowledge, skill, and experience affecting how efficiently they can remove vulnerabilities and restore compromised systems. In other words, vulnerability number 77 can be exploited by attack number 77. Real world cyber conflict is far more complex. Cyber-attacks do not precisely align with known vulnerabilities. Attackers seek out vulnerabilities and test methods and payloads to exploit them. In the current version, attacker agents only move in one direction

through the Lockheed Martin Cyber Kill Chain, with only one technique per phase of the kill chain. This adequately approximates the states of interest that ultimately simulate effects that might be occurring once a terrain agent is compromised (disruption, exfiltration, lateral movement, etc). But those effects are not modelled in this version.

3.2 Implications

Despite these limitations, this paper demonstrates that agent-based modeling is an effective research methodology for exploring the phenomenon of cyber team performance, and more generally, military operations research. In most any context, if performance needs to be computationally modelled, then agent-based modeling can help due to its bottoms up nature of defining behavioural rulesets. This work shows that we can successfully model the interplay of knowledge, skills, and experience and how those factors lead to successful mission performance when performing cyber security tasks. This suggests that in actual cyber teams, care should be taken to proactively prescribe what the team is setting out to do, in quantifiable terms, and then ensuring that the team is made up of operators likely to accomplish the goal based on factors controlled by management. Further, in general these teams will perform better if their knowledge, skills and experience are aligned with quantifiable and achievable results. This can be done through both targeted training programs immersive cyber exercises.

As military leadership pays more attention to the non-kinetic effects and capabilities available to them, systems like Cyber-FIT are perfectly positioned to support and advance research and development initiatives. Military training exercises that cross domains (e.g. air and sea) are used to ensure joint and combined commanders can integrate forces, communicate collective goals, and work through scenarios presented. This becomes much more difficult when trying to combine cyber security with social cybersecurity, an emerging discipline that aims to "identify, counter, and measure (or assess), the impact of influence campaigns," (Carley, 2020). This means that joint exercise environments need realistic and complex information environments integrated into the cyberspace environment, which is a very difficult and expensive task.

Acknowledgements

This work was supported in part by the Office of Naval Research (ONR) Minerva-Multi-Level Models of Covert Online Information Campaigns, N00014-21-1-2765, and the Air Force Research Lab FA8650212624 for Cyber-Fit. Additional support was provided by the Center for Computational Analysis of Social and Organizational Systems (CASOS), and the Center for Informed Democracy and Socialcybersecurity (IDeaS). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the ONR, the AFRL, or the U.S. government.

References

Andersson, D., Rankin, A. & Diptee, D., 2017. Approaches to team performance assessment: a comparison of self-assessment reports and behavioral observer scales. Cognition, Technology & Work, Volume 19, pp. 517-528.

Blane, J. T., Moffitt, J. D. & Carley, K. M., 2021. Simulating social-cyber maneuvers to deter disinformation campaigns. Cham, Springer International Publishing, pp. 153-163.

Carley, K. M., 2020. Social cybersecurity: an emerging science. Computational and Mathematical Organization Theory, 26(4), pp. 365-381.

Christensen, C. & Salmon, J., 2022. An agent-based modeling approach for simulating the impact of small unmanned aircraft systems on future battlefields. The Journal of Defense Modeling and Simulation, 19(3), pp. 481-500.

Department of Homeland Security, 2022. Biden-Harris Administration Announces $1 Billion in Funding for First-Ever State and Local Cybersecurity Grant Program, [online] https://www.dhs.gov/news/2022/09/16/biden-harris-administration-announces-1-billion-funding-first-ever-state-and-local.

Dobson, G. B. & Carley, K. M., 2017. Cyber-FIT: an agent-based modelling approach to simulating cyber warfare. Washington D.C., Springer International Publishing, pp. 139-148.

Dobson, G. B. & Carley, K. M., 2018. A computational model of cyber situational awareness. Washington, DC, USA, Springer International Publishing, pp. 395-400.

Dobson, G. B. & Carley, K. M., 2021. Cyber-fit agent-based simulation framework version 4, Pittsburgh, PA: Center for the Computational Analysis of Social and Organizational Systems.

Dobson, G. B., Rege, A. B. & Carley, K. M., 2018. Informing active cyber defence with realistic adversarial behaviour. Journal of Information Warfare, 17(2), pp. 16-31.

Goodwin, G. F., Blacksmith, N. & Coats, M. R., 2018. The science of teams in the military: Contributions from over 60 years of research. American Psychologist, 73(4).

Harrison, J. R., Lin, Z., Carroll, R. G. & Carley, K. M., 2007. Simulation modeling in organizational and management research. Academy of management review, 32(4), pp. 1229-1245.

MacMillan, J., Entin, E. B., Morley, R. & Bennett Jr, W., 2013. Measuring team performance in complex and dynamic military environments: The SPOTLITE method. Military Psychology, 25(3), pp. 266-279.

Metinko, C., 2022. Cybersecurity Venture Funding Surpasses $20B In 2021, Fourth Quarter Smashes Record, [online] https://news.crunchbase.com/venture/cybersecurity-venture-funding-2021-record/.

Pavez, I., Gómez, H., Liu, C. & González, V. A., 2022. Measuring project team performance: A review and conceptualization. International Journal of Project Management, 40(8), pp. 951-971.

Prashanth, R., Janssen, M. A. & Cooke, N. J., 2013. Agent-based model of a cyber security defense analyst team. Los Angeles, CA, SAGE Publications, pp. 314-318.

Sabin, S., 2023. Cybersecurity hiring remains strong amid tech layoffs, [online], [online] https://www.axios.com/2023/01/24/cybersecurity-hiring-tech-layoffs.

Shin, J., Dobson, G. B., Kathleen, C. M. & Carley, L. R., 2022. OSIRIS: organization simulation in response to intrusion strategies. s.l., Cham: Springer International Publishing, pp. 134-143.

Thompson, . B. & Morris-King, J., 2018. An agent-based modeling framework for cybersecurity in mobile tactical networks. The Journal of Defense Modeling and Simulation, 15(2), pp. 205-218.