Proceedings of the Annual General Donald R. Keith Memorial Conference
West Point, New York, USA
April 28, 2022
A Regional Conference of the Society for Industrial and Systems Engineering

Modeling and Refining the Life Cycle of a Defensive Cyber Operation in USCYBERCOM

Mackenzie Doyle, Brendan Thiele, Brandon Walters, Joshua Williams, and Julia Coxen

Department of Systems of Engineering
United States Military Academy
West Point, NY 10996

Corresponding Author's Email address: brandon.walters@westpoint.edu

Author Note: This research was done with the help and support of United States Cyber Command's readiness division. It would not have been possible without their help and insight.

Acknowledgments: We would like to thank the team at USCYBERCOM J34, especially LTC Michael Tilton and Tom Full for their cooperation and commitment to our research. To the staff and faculty at West Point DSE (Department of Systems Engineering), especially MAJ Kyle Ditonto, Zhanna Malekos Smith, and Miguel Welch, for aiding us with their technical expertise. Finally, our Advisor COL Julia Coxen. Ma'am, the impact your mentorship has had on our group cannot be understated. Thank you.

Abstract: The cyber domain is the newest and most dynamic arena of warfare in the 21st century. As such, United States Cyber Command's mission is to direct, synchronize, and coordinate cyberspace planning operations to defend national interests. Training soldiers, sailors, air men, and marines to fight and win in this domain is a key task for the command, and one which decision makers have struggled to synchronize across the joint force. Following the Systems Decision Process, this research focuses on the modeling, optimization, and implementation of policy to improve the training pipeline and career lifecycle of defensive cyber operators specific to the US Army. Utilizing stakeholder analysis, value modeling, and discrete event simulation, the research points toward policy recommendations that will improve these areas, internal to Army defensive cyber operations.

Keywords: Army, Cyber, USCYBERCOM, discrete event simulation, readiness modeling, stakeholder analysis, training pipeline, process optimization, defensive cyber operations, army cyber, cyber protection, blue cyberspace.

1. Introduction

1.1 Background

Cyber has become one of the most prominent domains in modern warfare due to the rapid evolution of the Information Technology (IT) network. Consequentially, nations have shifted focus to building their defensive and offensive cyber capabilities. This has resulted in the United States (US) forming the United States Cyber Command (USCYBERCOM), a joint combatant command that branched off from the National Security Agency (NSA). Consisting of personnel from the Army, Navy, Air Force, and Marine Corps, components in the USCYBERCOM merge to assist in completing its mission. Determining how to forge these components has been an arduous challenge and there are many inconsistencies and mishaps that have happened as a result. Nevertheless, the US has been proactive in finding solutions to the challenges that USCYBERCOM faces.

1.2 Structure of a Cyber Protection Team (CPT)

The Cyber Protection Team (CPT) is the main operational element within the Defensive Cyberspace Operations (DCO) realm, with the function of ensuring effective movement and maneuver within cyberspace protected by the US (blue) cyberspace to target malicious cyberspace activities (USCYBERCOM 2020). CPTs are divided into the mission areas of National, DoDIN, CCMD, and Service Command. Doctrinally, a CPT consists of 39 personnel, with three mission elements and one support element. However, stakeholder analysis revealed that it is common for a CPT to have two mission elements rather than three due to training and personnel constraints (USCYBERCOM 2020). Further stakeholder analysis would shift the scope of this problem primarily to the mission element echelon, which is the primary maneuver element that fulfills core

CPT functions. The two main work roles in the mission element are the Host Analyst and Network Analyst with between two and four personnel from each role in the CPT. There are two crew leads which can be either of the two work roles. The mission element lead, a leadership role typically fulfilled by a junior officer, oversees leveraging expertise to broaden the CPT's capabilities.

2. Methodology

2.1 Systems Decision Process

The systems decision process (SDP) is a four-step decision-making process created by the Department of Systems Engineering, the United States Military Academy (USMA). The SDP is iterative, with four main phases: Problem Definition, Solution Design, Decision Making, and Solution Implementation. The nexus of the SDP is the decision-maker and stakeholder value. Each phase is distinct and has key tasks throughout. Systems thinking has provided the framework to evaluate this complex and interconnected problem.

2.2 Problem Statement

Initially the problem statement for this project included modeling the entire lifecycle of a cyber soldier in all branches of the military, for both offensive and defensive teams, to identify and rectify inefficiencies. After extensive research, we concluded the lifecycle model would be vastly different for each service. There are multiple distinct phases that all cyber operators endure including initial schooling, advanced training, and joining a team. Although these phases are the same for all the services, the length and content of each stage are slightly different. These differences made modeling the lifecycle for each service inefficient provided the time constraints. Therefore, we narrowed the scope of the problem, so the model only consists of one type of cyber team and one branch of the military. The final problem statement includes modeling the life cycle of an Army Defensive Cyber Operator to identify inefficiencies in the training pipeline. The research aims to find solutions to challenges plaguing the cyber branch, such as slow throughput, retention, and readiness.

2.3 Stakeholder Analysis

The stakeholder analysis we conducted helped to scope the problem from modeling all four of the branches of the military to the more important aspects of the lifecycle. Specifically, we moved into the Solution Design phase of the SDP focused on modeling the training and career lifecycle of an Army defensive cyber operator. This section summarizes the expert interviews we conducted.

2.3.1 USCYBERCOM J34 – Readiness

The J34 office at USCYBERCOM, whose mission is to ensure the readiness of the military's cyber branch, were excellent partners in this research. Prior to discussing with them, we concluded that modeling both offensive and defensive components of all branches was not feasible given the time constraints. Therefore, we presented a Zwicky's morphological box to develop new possible courses of action. We wanted their input on how to proceed, so we still created a model that was useful for them. During the meeting, we decided our model would include only the Army's defensive teams moving forward. As an Army organization, we had a better understanding of the lifecycle of an Army soldier so focusing on this branch allowed us to make a more accurate model. Also, we have greater access to resources regarding the Army cyber branch due to our proximity to the Army Cyber Institute. We also made a trip to visit the USCYBERCOM headquarters towards the end of November, where we presented our current research and met our client in person. During the meeting, we were provided a chart that drove the structure of the life cycle model. It also gave us numbers needed to verify and validate the model. Using all the information our clients provided, we were able to build a more accurate model.

2.3.2 USCYBERCOM J7 – Exercises and Training

Since a substantial portion of the lifecycle of a cyber operator consists of the training they endure, our clients gave us the contact information for USCYBERCOM J7. Their organization regulates the training performed at the joint level under USCYBERCOM. During the meeting, we obtained a chart that detailed the name and length of the training each Cyber Mission Force work role endures. They also explained that there are three work roles in CMF (Combat Mission Forces) teams- offensive, defensive, and support. To not complicate the model, we only used the strictly defensive work roles. Following this logic, we included the all-source analyst, host analyst, network analyst, and network technician in the lifecycle model.

2.3.3 US Army Cyber School

Prior to meeting with an expert from the Army Cyber Schoolhouse, we had created a basic model with MOS, BOLC, and WOBC training, work role education pipelines, 61 Army CPTs, and the four ways an operator could exit the system. After explaining our general problem statement and presenting the model, the expert provided us with constructive feedback. First, he explained that officers do not endure work role training at the 2000 level. Instead, they go straight from BOLC to their first unit. This was a misconception we had due to the research we completed that was eventually fixed in the updated model. Secondly, the expert from the schoolhouse explained that although the Army has 61 total cyber teams, only 20 of these are considered defensive active-duty teams. Therefore, we could eliminate 40 of the teams from our model. He also explained that although each team is divided into two mission elements and a support element, the two mission elements are the ones pertinent to defensive cyber operations for the Army. This information helped us build a more accurate and useful model.

2.3.4 US Army Cyber Protection Brigade (CPB)

In one of our final stakeholder meetings, the researchers spoke with the officers and noncommissioned officers (NCOs) from the cyber protection brigade (CPB). The purpose of this meeting was to gain clarity on the in-processing procedure for new operators and the type of training they endure once on their teams. The one meaningful change to the model that came from this meeting was the addition of RAPTOR, an in-processing detachment located at the cyber protection brigade. The unit's new cyber operators report to this unit and spend about 45-60 days there before joining their team. With this information, we clarified the problem statement and built the final model.

2.4 Building the Model

To model the life cycle of defensive cyber operators most effectively in the Army, we used software called ProModel, which creates discrete event simulations over any given period for multiple iterations. This software allowed us to model the training pipeline to have enlisted service members, commissioned officers, and warrant officers moving through the system for years at a time. By continually running the model, we could identify where the inefficiencies such as long wait times occur in the lifecycle. We took multiple iterations in the final model before achieving the result.

2.4.1 Initial Model (Model 4.1)

The first model we built was created after multiple discussions with our clients in J7 at USCYBERCOM. This model included locations for BOLC, basic training, two thousand level training, joining a team, and the four locations for exiting the system. The main framework for this model came from a chart we obtained during a meeting at Ft. Meade near the end of November. Although we quickly concluded that this model was too simplistic given the intricacies, it was still a solid baseline to use moving forward. An image of our original model can be seen below.

2.4.2 Model Version 2 (Model 4.2)

The next iteration of the model we developed was slightly different due to input received from our clients at USCYBERCOM and the J3 at USCYBERCOM. Initially, we had not considered modeling warrants in the system. However, our client mentioned their importance to the branch, so we created a location for the Warrant Officer Basic Course. We also included queues at the beginning of each location at the suggestion of our client. Due to the nature of the cyber training operators must endure, there are a limited number of seats available for classes. Therefore, there is typically a wait between training courses. After discussing training more in-depth with the J7, we were able to break down the various defensive work roles into their individual training pipelines. Host and Network Analysts must complete Intermediate Cyber Core and Discovery Cyber Core classes before joining their teams. All Source Analysts must complete the Cyber Threat Intelligence Analyst course before joining their teams. The Network Technicians, however, do not have to endure any 2000 level training. We had all the entities entering the system joining the queue to endure the training for one of the four work roles. From here, we modified the single "Join Team" location from the initial model into 60 separate locations to represent the number of defensive cyber teams in the Army.

2.4.3 Final Model (Model 4.3)

Although not pictured here in this article, the final version of this model was developed after extensive stakeholder input from the Army Cyber School and the Cyber Protection Brigade. The expert at the Army Cyber Schoolhouse made it clear during our meeting that we only need to model the 19 active-duty defensive cyber teams. He also suggested dividing each team into their two mission elements to assess their readiness more accurately. To accurately represent the teams, we chose to label the teams using the same classifications as the Army. Our model contains 1 DoD (Department of Defense) information network team, 6 Service teams, 8 Combatant Command teams, and 5 National Cyber Protection Teams. Although we were able to represent this suggestion accurately, we chose to separate the teams into their officer positions versus enlisted and warrant positions rather than separating the teams into their individual mission elements. This allowed for more accuracy with the routing logic and capacities at each location. Also, after the discussion with the Cyber Protection Brigade, we changed the name of the queue for joining a team to "RAPTOR" and increased the wait time for the entity to 60 days (about two months). The final version of the model can be seen below.

2.4.4 Verification and Validation

Verification and validation are processes used to ensure that a model is functioning properly. Verification is the process of making sure that the created model is working properly and does not have any unwanted glitches that will throw off the numbers returned at the end of the process. Validation is the process of determining the degree to which the model corresponds to the real system. Validation was done in our model by watching the animation, testing for face validity, and overall comparing the model to our understanding of the real-life system as we understand it.

3. Policy Implementation, Results, and Analysis

3.1 Policy #1- Increase Capacity of Training Classes (Model 4.6)

One of the most deleterious issues in the cyber branch is getting personnel through 2000 level training and onto teams. Currently, cyber operators spend more months waiting to join a class than they do completing the training. For example, host and network analysts have two classes they must complete prior to joining a team. Both classes have queues, meaning there are wait times prior to entry. Instead of spending eight weeks in the Intermediate Cyber Core Class followed by eight weeks of the Discovery and Cyber Core class, cyber soldiers can spend months before each class waiting for a spot to open. Increasing the capacity of operators in each class would expediate the process of personnel getting on teams.

To implement this policy, we increased the capacity of the schoolhouses in the "Intermediate Cyber Core," "Discovery Cyber Core," and "Cyber Threat Intelligence Analyst Course" to 200 from 100. Furthermore, we allowed only 10 enlisted and warrant operators to accumulate before the start of each course instead of 30. We decreased the number accumulating at the locations to simulate operators completing training at a faster rate. This is the expected outcome if more operators could be trained at once. Since more operators would be completing training each iteration, we expect the overall readiness of the teams to increase. We ran the simulation 10 times for 20,000 days to gather data. Results of the simulated utilization across all the different policies can be found in Figure 1.

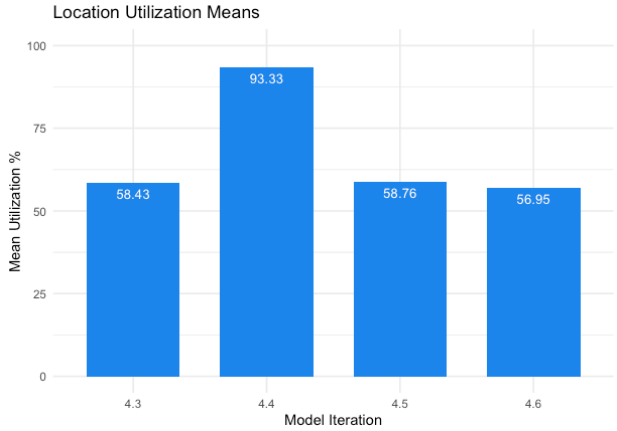

Figure 1. Team Location Utilization (Readiness

The assumptions we made proved to be true when we implemented the changes in the base model. The average time spent in training decreased significantly from 425.44 days in the base model to 172.47 days. However, the percentage of teams ready decreased as well, which is not optimal. This decrease was not significant as it only decreased by 2.5%, so this brought us to the conclusion that the capacity of the 2000 level training classes does not influence the percentage of teams ready.

3.2 Policy #2- Increase Tour Length (Model 4.4)

Another course of action to increase the number of cyber operators on teams is by increasing the amount of time cyber operators are required to spend on a team. Cyber operators currently follow a three-year PCS (Permanent Change of Station) routine consistent with the rest of the Army. However, our research suggests if we require personnel to remain in teams for longer, this will enable a higher percentage of team readiness due to the decreased turnover rate. This would also enable new personnel to complete all the required training, so they arrive at their team with all the skills required to successfully fulfil their work role.

To implement this policy in our model, we increased the wait time at each of the team locations. We extended the wait time in the cyber team locations from 3 years to 5 years and evaluated the results. We expected this to increase team readiness, similar to the other alternatives. Increasing the tour length significantly changed the percentage of teams ready from the base model. This number increased by about 36%. Since our main priority was to have the number of teams ready at a higher value, this policy will help do this significantly.

To gauge the sensitivity of the tour length duration, we created different models that altered the duration that entities spent on the teams. We varied the durations from 3.5 years to 6 years and evaluated the results after running each model for 20,000 days for 10 iterations. The results can be seen below in Figure 2. Overall, a 5-year tour length is most ideal for ensuring readiness. There is a small increase in a 6-year tour length, but likely not enough to justify an entire extra year of service within the team.

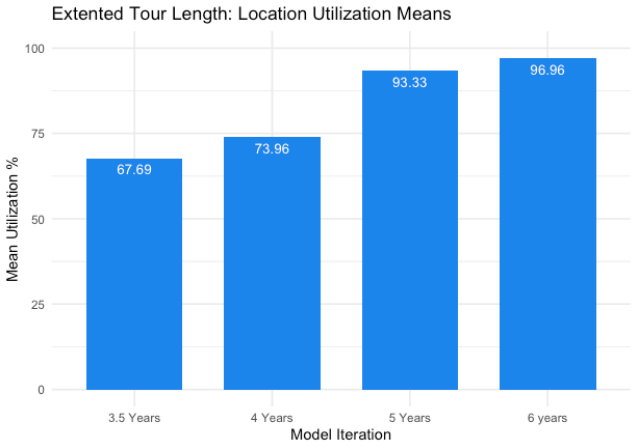

Figure 2. Team Location Utilization (Readiness) for Extended Tour Length Alternatives

3.3 Policy #3 – Fast Pass (Model 4.5)

One way to enable cyber operators to get on teams faster is by implementing a fast pass, which would allow skilled cyber operators to take a test that demonstrates they already possess the necessary capabilities to fulfill their work roles instead of enduring the required 5 to 16 weeks of training. This would enable more cyber operators to fulfill work roles on teams.

To implement this policy in our model, we changed the processing of the cyber soldiers and warrant officers. Instead of all the soldiers participating in the training for their respective work role, we configured the model to so that 10 percent of soldiers passed the test required to skip their training, allowing these entities to be processed directly to the “RAPTOR 2” location from the MOS training location. By doing this, we expected the percentage of enlisted soldiers in operation to increase while the time each entity spends training would decrease. Furthermore, the percentage of teams considered “ready” should have also increased. We ran the simulation 10 times for 20000 days to gather data.

After running this model, the percentage of teams ready increased compared to the base model, which confirmed our predictions. However, this readiness number only increased by 1.61%. This estimated change is not significant enough to

allocate resources to integrating this policy into the life cycle. In theory this is an attractive alternative, but in the long run we see that the utilization on the team is only marginally improved.

4. Conclusion

4.1 Conclusion

This area of research has proved complex and dynamic. Through immense stakeholder analysis, we were able to produce a baseline model to identify inefficiencies, provide insight, and ensure a proof of concept for further research in the field. Modeling this system allowed us to determine places in the training lifecycle where policies could be implemented that improve certain factors, all of which aim to improve the overall readiness posture of active-duty defensive cyber mission elements. Through this analysis, we also found that the percentage of teams that were ready was the most valuable measure that we could use to compare different policies. Our proposed policies included increasing the capacity at 2000 level training, a "fast pass", and increasing tour length. After analyzing these alternatives' and inputting their data into our quantitative value model, we discovered a clear recommendation. Supported by our results, we conclude that the policy #2, or increasing the tour life of a cyber operator, will support a more efficient training lifecycle for defensive cyber operators of all rank and therefore is our final alternative recommendation.

4.2 Future Work

The possibilities for expansion of this research is prolific. One area for future work is to continue to expand on the model and to include the offensive and supporting work roles for cyber protection teams in the Army. The framework is already there, but it would be necessary to expand the type and number of training courses as well as the number of teams represented. Furthermore, this research could be extrapolated to the other branches of the military. Time was our limiting factor, but the groundwork we have done can be used as a starting point for future research.

5. References

Craft, P. BG. (11, February 2022). US Army Cyber School. Stakeholder Analysis. West Point, NY.
Harrell, C. (2000). *Simulation Using ProModel* (3rd ed.). New York, NY: McGraw-Hill Education.
Parnell, G. S. (2011). *Decision making in systems engineering and management*. Wiley.
Sedivy, D. LTC (15, February 2022). Cyber Protection Brigade. Stakeholder Analysis. West Point, NY.
Tilton, M. LTC. (29, November 2021). USCYBERCOM J34. Stakeholder Analysis. Ft. Meade, MD.
United States Cyber Command. (2020). *Cyber Warfare Publication 3-33.4: Cyber Protection Team (CPT) Organization, Functions, and Employment*