THE CYBER WARGAME COMMODITY COURSE OF ACTION AUTOMATED ANALYSIS METHOD

THESIS

Alex Hoffendahl, First Lieutenant, USAF

AFIT-ENS-MS-22-M-138

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

DISTRIBUTION STATEMENT A
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this document are those of the author and do not reflect the official policy or position of the United States Air Force, the United States Department of Defense or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENS-MS-22-M-138

THE CYBER WARGAME COMMODITY COURSE OF ACTION AUTOMATED ANALYSIS METHOD

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Operational Sciences

Alex Hoffendahl, B.S.

First Lieutenant, USAF

March 24, 2022

DISTRIBUTION STATEMENT A
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT-ENS-MS-22-M-138

THE CYBER WARGAME COMMODITY COURSE OF ACTION AUTOMATED ANALYSIS METHOD

THESIS

Alex Hoffendahl, B.S.
First Lieutenant, USAF

Committee Membership:

Capt Chancellor Johnstone, Ph.D
Chair

Lance E Champagne, Ph.D
Member

Maj Richard Dill, Ph.D
Member

AFIT-ENS-MS-22-M-138

Abstract

In the modern operational landscape, strategic decisions are made and executed, under uncertain conditions, with many potential constraints and limited information. The end goal of these decisions is to minimize and mitigate the effect of adversarial threats, which may or may not act in line with previous assumptions. Wargaming is a powerful tool that allows for the practical implementation of theoretical knowledge into real-world scenarios, enhancing decision-makers' critical thinking and problem-solving skills. Furthermore, including cyber-effects in a wargame leads to a broader decision scope for an entire operation. This research aims to enhance the analytical capabilities and overall usability of the Wargame Commodity Course of Action Automated Analysis Method (WCCAAM) by incorporating cyber-effects in determining optimal blue-team actions. The original WCCAAM model receives mission objectives, available units, and enemy targets as inputs. Then, a multi-commodity flow algorithm (MCFA) is applied to identify the optimal engagement approach to combat a known enemy course of action (COA). This proposed extension of WCCAAM, aptly named the Cyber-Wargame Commodity Course of Action Automated Analysis Method (C-WCCAAM), balances engagement risk with blue-team cyber-effects to combat enemy targets. The resulting model utilizes an MCFA approach within a multi-objective mixed-integer program (MO-MIP) to determine an optimal blue-force COA. We explore a fictitious wargame scenario and compare C-WCCAAM results on this scenario to previous results achieved with WCCAAM, achieving lower risk by utilizing potential cyber-effects in our blue-force COA. We also assess the robustness of our optimal COA through sensitivity analysis.

Acknowledgements

I would like to express my sincere appreciation and gratitude to my advisor, Capt Chancellor "Chance" Johnstone, who gave me direction and support throughout this research, which made this work possible. His guidance and advice carried me through all the stages of writing. Thanks to him.

I would also like to thank my committee members, Dr. Lance Champagne and Maj Richard Dill, for their comments and suggestions during my defense.

Finally, I would like to thank my significant other for standing by my side throughout the school year and challenges.

Alex Hoffendahl

Table of Contents

List of Figures

Figure Page

List of Tables

THE CYBER WARGAME COMMODITY COURSE OF ACTION AUTOMATED ANALYSIS METHOD

I. Introduction

In the modern operational landscape, strategic decisions are made and executed, under uncertain conditions, with potential constraints and limited information. The end goal of these decisions is to minimize and mitigate the effect of adversarial threats, which may or may not be acting in line with previous assumptions. Wargaming as a decision-making tool allows for the practical implementation of theoretical knowledge into real-world scenarios and enhances decision-makers' critical thinking and problem-solving skills [1]. Additionally, wargames provide opportunities to test new ideas and capabilities, and help decision-makers to visualize alternative ways of operating would make the difference between success and failure in future conflicts. In particular, the use of wargames can assist decision-makers in resolving complex military challenges by introducing new strategic and operational concepts, stimulating debate, and aiding in the discovery of offensive courses of actions (COAs) [2].

Our focus for this research is the exploration of cyber-effects in wargaming. To motivate this discussion, we recall a real-world example concerning Iran. Beginning in 2009, Iran has continued to implemented focused cyberattacks on U.S. government and private sector systems, costing western firms millions of dollars in lost business and adding huge financial burden to local residents. By 2020, conflicts between the U.S. and Iran consistently took place in cyberspace. Although the breadth remains unclear, cyberspace has become the primary battleground, providing an alternative to kinetic military action [3]. Given that the prevalence of cyber capabilities has

increased the technical complexity of modern warfare, those that utilize cyber-effects gain the operational "high ground." With this, traditional wargame models can no longer represent the reality of any operation where cyber-effects are involved, that is, with any modern operation. We aim to extend a new paradigm in wargaming: cyber-wargaming.

Cyber operations have become a critical engagement method and are no longer separate from conventional combat. Just as the combination of cyber and kinetic operations adds to the complexity of modern warfare, existing wargaming approaches must also increase their complexity; the inclusion of cyber operations within wargames is paramount. However, a critical problem is that current wargame frameworks are not effectively develop cyber-wargaming scenarios or model cyber-effects with the required level of realism, due to designers' lack of knowledge regarding the impact of cyber on military missions [4].

In previous research, [5] introduced the Wargame Commodity Course of Action Automated Analysis Method (WCCAAM) as a systematic procedure to aid in the COA development, analysis and comparison phases of the Military Decision-Making Process (MDMP). Assuming that the potential enemy's behavior is known, along with a high-reliability on information sources, WCCAAM generates an "optimal" COA, minimizing engagement risk subject to successfully achieving tactical and strategic objectives and nullifying enemy targets. We introduce an extended version of WCCAAM, named Cyber-WCCAAM (C-WCCAAM), which delivers an optimal blue-team COA concerning two objectives:

1. the minimization of engagement risk
2. the minimization of cyber-effect cost

Similar to WCCAAM, we generate an optimal COA under constraints constructed from a set of known future enemy actions, e.g., enemy troop movements or enemy

fighter aircraft attacks. While WCCAAM generates an optimal COA through a multi-commodity network flow formulation, we deliver an optimal COA through a mixed-integer multi-commodity network flow problem. The optimal solution to our network flow formulation delivers even lower engagement risk than WCCAAM by including decisions on the most effective use of offensive and defensive cyber operations, with the ultimate goal of counteracting or destroying enemy targets. We compare results generated with WCCAAM to those generated with C-WCCAAM, on a fictitious, yet realistic, scenario, adding into the decision-space a collection of potential blue-team cyber-effects. Ultimately, we extend WCCAAM to incorporate cyber-effects, formulating a new model approach that advances the state-of-the-art in cyber-wargaming.

Section 2 of this paper provides relevant background used in the research. Section 3 provides a detailed methodology specific to constructing C-WCCAAM. Section 4 is dedicated to analysis results and discussion. Finally, Section 5 provides conclusions and discussion related to future research.

II. Background and Literature Review

This chapter includes discussion of previous research crucial to the development of C-WCCAAM. We provide background on wargaming, cyber-wargaming, as well as WCCAAM. We also include discussion of relevant mathematical programming approaches.

2.1 Wargaming

Wargaming has a long history as a tool for decision-makers to improve their critical thinking and inventiveness [6]. One advantage of conducting wargames is that they allow for the validation of ideas and tactics via simulation without the use of physical forces. Wargaming is also critical for determining the strengths and weaknesses of said tactics, or even a specific force structure. Typically, a small-scale simulation may provide an overview of how an organization should operate throughout an operation. However, a discrepancy between reality and theory is unavoidable. Reducing this gap becomes a wargame's driving issue. This has resulted in a surge in demand for more realistic wargames to tackle real-world problems [7].

Making the "right" choices entails determining what action to take, when to take said action, as well as realizing the repercussions of those actions [8]. The manner in which commanders carry out their end-state vision results in decision-making that is more similar to art than science. The "art" of war incorporates factors such as leadership impact, operational complexity, and adversary goal [9]. One such method that considers each of the factors mentioned is the Military Decision-Making Process (MDMP).The MDMP assists the commander and their staff in making reasonable decisions by transforming those "artistic" components into quantifiable, logic-based approaches [10]. Using the MDMP, commander and mission planners iteratively

develop an operational strategy for achieving strategic goals [5].

The purpose of WCCAAM is to help commanders build and analyze COAs via automation of a portion of MDMP, namely the COA development, analysis, and comparison phases . We reproduce a graphic from [5] to emphasis WCCAAM's role within the MDMP. We elaborate on WCCAAM in Section 3.

Wargames serve as a training tool by immersing decision-makers in a realistic scenario and allowing them to make choices comparable to those they would face in the real world [11]. At times, some of many cognitive biases may inadvertently impede decisions makers and prevent better judgments from being made [12]. We include a subset of these cognitive biases. In Figure 1, reproduced from [12].

Cognitive Biases

Cognitive Biases
Mental filters: Research shows that people tend to force the world into their existing frames. Weak signals that don't fit are typically distorted or ignored. Humans see what they expect to see, rather than what is there.
Overconfidence: A demonstrated tendency to be too certain also makes people tend to believe that the current view they hold is correct.
Penchant for confirming as opposed to disconfirming evidence: It is more difficult to detect disconfirming evidence than confirming evidence, so the mind is more likely to accept than to reject an idea.
Dislike for ambiguity: People dislike ambiguity, particularly in organizations in which managers are expected to have answers to questions.
Groupthink: Members of organizations take comfort from belonging to the majority and seeing the world in the same way, so there is a tendency to go along with what other say. Rather than to use an individual mind to find flaw in the group's thinking.

Figure 1: Cognitive barriers for the failure to develop foresight [12]

Within every decision-making process, biases in our thinking provide significant challenges. However, as a result of repetition and visualization, wargames help commanders establish confidence in their decision-making abilities, increase comprehension of military operations, and form effective teams, while demonstrating individual personality characteristics and cognitive processes [13].

In addition to the physical changes to the decision-making environment, there are psychological repercussions to both making and coping with choices. Biases may

distort and disturb objective contemplation of a problem when variables other than the option itself are brought into the decision-making process. Many people are often unaware of their prejudices, which makes it difficult to make rational judgments. The most common cognitive biases include mental filters, overconfidence, a preference for confirming evidence over disconfirming evidence, a disdain for ambiguity, and groupthink [12]. Likely, decision-makers will be faced with these biases along with emotional and psychological strains, and operational difficulties when confronted with a large-scale real-world disaster [11]. Nonetheless, engaging in wargames may better prepare leaders for any situation they must face, and developing new mental skills, facilitating to reduce cognitive biases might assist crisis-management leaders better prepare themselves to deal with the implications of their actions [11].

One advantage of wargames as a military training tool is they enable decision-makers to acquire insight and creativity as a habit via repetition, eliminating mental barriers that might impair decision-making quality. During Operation DESERT STORM, Marine divisions performed planned training and instruction, as well as tactical force-on-force free-play training. Additionally, each event had scenario-based elements that required time management and wargaming [14]. Additionally, the "wargaming" unit answered to tactical orders and assisted commanders and staff in making judgments in the face of a rational adversary, providing rapid feedback during decision-making [14].

As an analytical tool for comprehending diverse types of threats, battles and problems, wargaming has gained widespread acceptance in recent years. However, despite its roots in military planning, the use of wargaming is increasing in the assessment and testing of a variety of different systems [1]. As an illustrative example, we present a set of COAs and consequences for a North Atlantic Treaty Organization (NATO) scenario concerning the invasion of the Baltics by Russia. In this scenario, NATO

only has a few options:

1. a bloody counteroffensive, fraught with risk, to free the Baltic State
2. escalation, as it threatened to do during the Cold War
3. defeat, with uncertain but predictable disastrous consequences for the Alliance and the Baltic People [15].

Currently, the same hypothetical scenario is playing out with the 2022 Russian invasion of Ukraine. As of February 27, 2022 Russia's nuclear deterrence forces were on high alert in response to the escalation of resistance and retaliation from Ukrainians and sanctions imposed by US and NATO nations on Russia's financial institutions from the global economy [16][17]. These scenarios can cripple the Russian economy and defeat them in the form of a trade war, while escalation of nuclear deterrence on Russia's parts signals others to back down [18]. Along with the invasion, the actual consequences between Ukraine people and people of NATO nations are not far off from predicted consequences simulated by the "hypothetical" wargame. The nuclear escalation of Russia could bring a disastrous consequence for the Alliance and Ukraine as a Baltic state. With this, a valuable aspect of wargaming has been emphasized. The benefits of include tools to train and educate critical thinking and creativity, but more importantly, help tactical commanders prepare for future difficulties.

2.2 Cyber-Wargaming

For many nations, cyber warfare is becoming a reality; each nation has a suite of its own offensive and defensive cyber weapons. Today's warfare is more technologically advanced than ever before; those that make use of cyber capabilities gain an operational advantage. There is a growing need for new wargame models that effectively incorporate cyber-effects into operations. Using cyber wargaming to test and

develop proactive and reactive incident response strategies will help decision-makers better align with real-world scenarios involving possible cyber-attack/defense options. In theory, cyber-wargaming will lead to a better awareness of engagement risks and an opportunity to practice collaboration and swift decision-making among players.

The complexity of cyber-wargames cannot be overstated. The behavior of the air, sea, land and space is well known in most games. However, cyber-effects in wargames are abstract, invisible, and misunderstood, making designing a cyber-wargame model harder than a classic wargame [19]. One existing cyber-wargame scenario, named "Merlin," was constructed by the Center of Naval Analysis (CNA), to imitate how to achieve cyber-effects with particular uncertainty in the real-world. The wargaming team uses dice to simulate uncertainty related to whether a player successfully achieves the desired cyber-effect based on the cyber resources the player had assigned for each desired effect [20].

While wargaming is an excellent training tool, it is also vital for developing a better understanding of the strengths and weaknesses of force formations. Wargaming may help discover weaknesses in a preliminary strategy or course of action by simulating its execution. A good simulation is crucial for identifying and managing key tasks and conditions required for a successful military operation, as well as for improving the quality of plans and decreasing planning time [21]. To accomplish the benefits indicated above, simulation-based wargaming consistently includes four processes that aid designers in accurately modeling wargames based on compelling scenarios [22]. These processes include:

1. establish a common understanding of the objective of the wargaming experiments
2. define the overall scenario, including external conditions and limitations
3. choose one or more simulation systems and calibrate simulation models

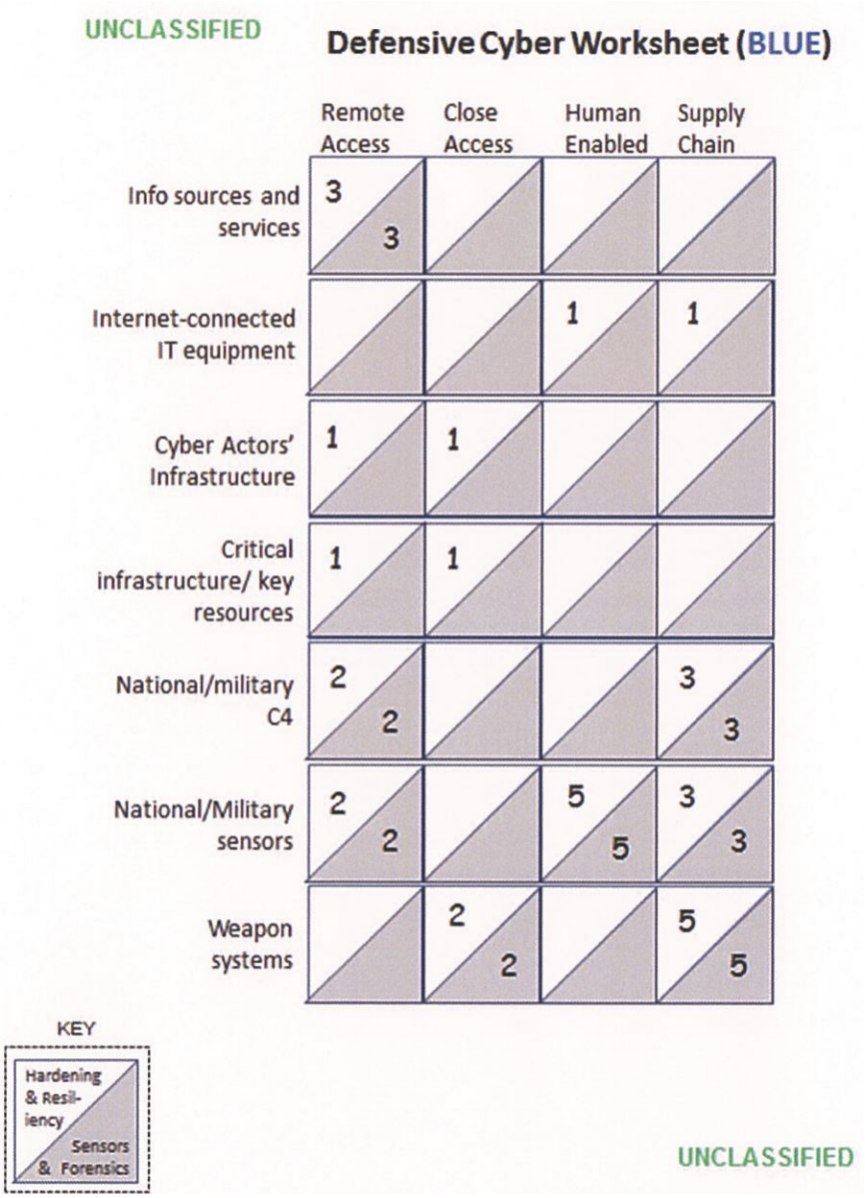

Figure 2: Example of a cyber defense matrix used in the Merlin wargame

4. define the order of battle (OOB) for the blue and red sides [22]

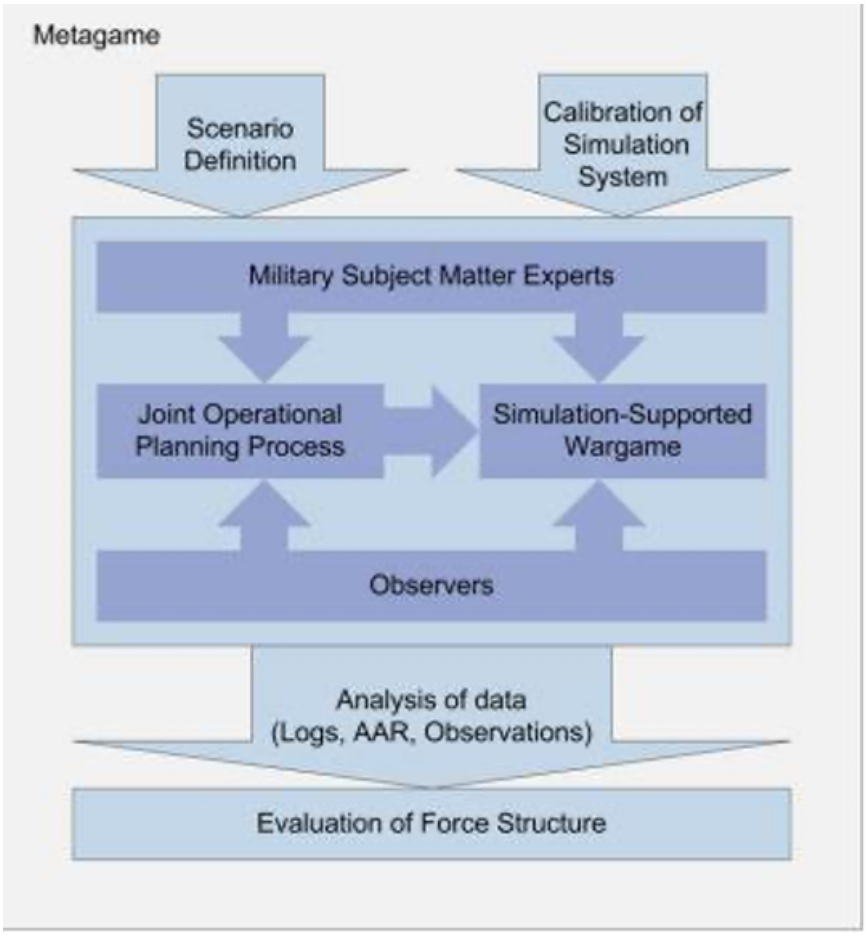

Figure 3: Procedures of designing a wargame

Figure 3 displays the steps to launching a state-level wargame. After defining the scenario, each player needs to interact with military subject-matter experts to plan a joint operational process. Then observers, as the "adjudicators" of the game, will observe both the interactions of the players with the experts and the evaluating results and force structure based on their decisions.

2.3 Mathematical Approaches: Optimization

2.3.1 Linear Programming vs Nonlinear Programming

Linear programming (LP) is a method by which we can compute an optimal and feasible solution, subjected to a linear objective function and linear constraints. The canonical form for a linear programming is:

$$\max \sum_{i=1}^{I} c_i x_i \tag{1a}$$

$$\text{subject to:} \sum_{i=1}^{I} A_{ij} x_i \leq b_j \quad \forall j \tag{1b}$$

In contrast to linear programs, nonlinear programs generate optimal solutions subject to potentially nonlinear objectives or constraints. Nonlinear programs are used in planning production schedules, transportation, in military logistics [cite]. The difference between NLP and LP is that NLP optimization problems contain nonlinear constraints or nonlinear objective functions, and example of which is

$$\max f(x, c) \tag{2a}$$

$$\text{subject to: } g(x) \leq b, \tag{2b}$$

where $f(x, c)$ and $g(x)$ might be nonlinear.

2.3.2 Mixed-Integer Programming

Mixed-Integer Programming (MIP) methods handle minimization and maximization problems with a linear objective function subject to linear constraints [23]. MIPs

contain variables that are restricted to be integer values. For example, a binary variable, taking the values of 0 or 1, may represent the acceptance or rejection of a decision. Because of this feature, MIP as a mathematical optimization method has prevailed in decision-making related to portfolio optimization and monitoring military operations [24].

MIPs also play a crucial role in supporting decision-making under uncertainty by simplifying complex systems to understand potential outcomes better. Consider an investment problem where decisions involve selecting several potential investment. We define c_j as the contribution resulting from the j^{th} investment and A_{ij} as the amount of resource i, e.g., cash or human resources, used on the j^{th} investment. Then, the maximization of total contributions from all investments without exceeding the limited availability b_j of specific linear combinations of resources can be achieved through the following integer program:

$$\max \sum_{j=1}^{J} c_j x_j \tag{3a}$$

$$\text{subject to:} \sum_{j=1}^{J} A_{ij} x_j \leq b_i \qquad \forall i \tag{3b}$$

$$x_j \in \{0, 1\} \tag{3c}$$

where $x_j = 1$ represents the decision of investment j.

Decisions on the use of specific cyber capabilities are central to C-WCCAAM. The problem of choosing units and a low-risk engagement path to destroy the enemy targets defines the core components of the wargaming design. We can formulate this problem using a mixed-integer method to calculate an optimal COA based on risk reduction and cost. We expand on this in Section.

Linear programming seeks to maximize (minimize) the value of a linear objective function given one or more constraints. The approach has a wide range of applications in operations research. In some cases, both LPs and MLPs share similar programming structures, except LPs are more flexible and robust by accepting real-number $x_j \in \mathbb{R}$ as an input, while some variables in MIPs may only accept integers $\mathbb{Z}$. The structure of an MIP consists of a linear objective function subject to one or more linear constraints. In addition, linear programming can be used for mixed-integer programming as long as the objective functions and constraints can be quantified linearly.

MPs have often been used in monitoring system network flows and optimization [23]. In many mixed-integer programming problems, the continuous variables represent an amount of "flow" in a system, while the binary variables correspond to decisions associated with each path flow. The goal of the optimization process is to find a set of binary decision variables that link to a set of continuous variables, minimizing the objective function, subject to a set of constraints [23].

III. Methodology

In this chapter, we introduce an extension of WCCAAM to include decisions related to the use of cyber effects, aptly named Cyber-WCCAAM or C-WCCAAM. We start with some background on WCCAAM, then introduce the mathematical formulation used for C-WCCAAM. We also provide a "linearization" of C-WCCAAM in order to reduce solving time and allow for implementation on open-source solvers.

3.1 Assumptions/Hypothetical Conditions

As the foundational model, WCCAAM sets the groundwork for developing C-WCCAAM. In WCCAAM, a collection of different blue force units, identified as "commodities," are utilized to confront a unique overall red force course of action (COA). The model's purpose is to minimize engagement risk "to friendly forces" by dispatching commodities from various location to nullify targets, as set as by tactical and strategic objectives. However, the challenge is that all engagement risks associated with any potential engagement path must be precisely quantified.

On the other side, cyber effects have to be successful achieved in order to minimize engagement risk. However, it is difficult to adequately quantify the risk-reduction potential associated with specific cyber effects. As mentioned in Section II, WCCAAM aids in the COA development, analysis and comparison of the MDMP. With this, any information used in the model must come from the mission analysis phase. Thus, we require precise and reliable quantification of engagement risk and risk-reduction factors for cyber-effects.

We formalize our assumptions below:

1. engagement risks provided during the mission analysis phase.

2. all desired cyber-effects are successfully achieved and their engagement risk reduction factors are known.

3. red team behavior is known.

3.2 C-WCCAAM Formulation

3.2.1 Single-Commodity

Before introducing the large-scale multi-forces aspect of C-WCCAAM, we will describe some key ingredients of a single-commodity model, such as the decision to use cyber effects and risk-reduction factors from cyber-effects, along with the cost of implementing them. For our simple model based on WCCAAM, we will use infantry as our single commodity. We will then look into the C-WCCAAM model formulation to see if it can help us figure out what we can expect in terms of multi-commodity formulations.

At first, we describe relevant decision variables and model parameters for a single-commodity model; blue infantry versus the red infantry:

Indices:

i: Blue Bases: Base 1, Base 2, Base 3 (I = 1,2,3)

j: Red Targets - Infantry (J = 1,2,3)

Decision Variables:

X_{ij}: Number of infantry from blue base i sent to nullify red infantry j

Y_{ij}: Cyber-effects for infantry when engaging red infantry j from blue base i, in binary form as 1: *yes*, 0: *no*

Constants:

R_{ij}: Engagement risk of infantry from blue base i to nullify red infantry j

S_i: Total number of infantry that can be sent from blue base i

D_j: Total number of infantry required to nullify red infantry j

P : Cyber budget

C_{ij}: The cost of using cyber-effects for infantry when engaging red infantry j from blue base i

ϵ_{ij}: Engagement risk-reduction factor when engaging red infantry j from blue base i: value between 0 to 1

WCCAAM is built on a multi-commodity network flow algorithm, where the ultimate objective is to nullify all targets with a risk-minimizing COA. However, this algorithm remains the same in a single-commodity model as handling network flow for one type of force. For simplicity, blue infantry will be referred to as "supply nodes" in the sense of "providing infantry," whilst the red infantry will be referred to as "demand nodes."

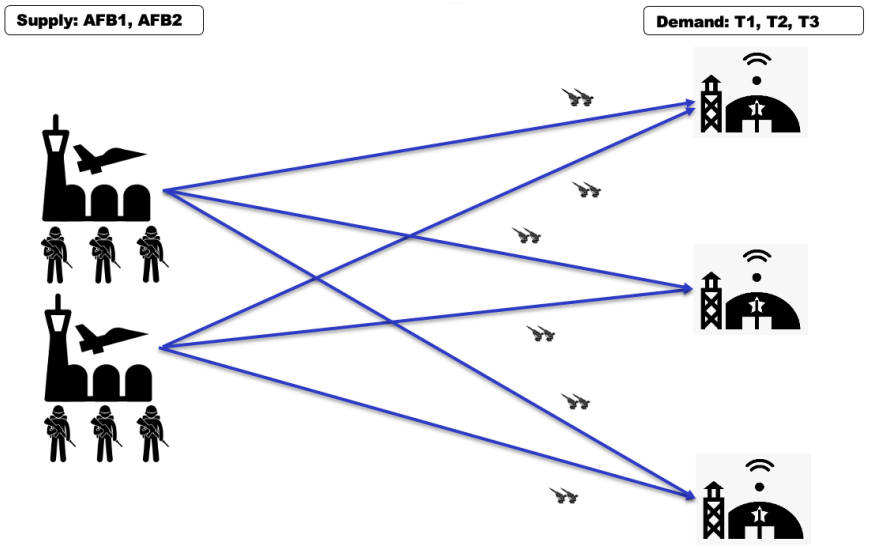

Figure 4: Single-Commodity Model: Infantry Only

The plot Figure 4 indicates the engagement path when blue infantry attacks red infantry. Specifically, our objective is to nullify all red infantry by sending infantry from bases. In the single-commodity model with infantry in three blue bases as "supply nodes" and four red infantry as "demand nodes," we will be constructing twelve engagement paths. Each path is threatened by a by red team targets. Cyber-effects infiltrate the system and make a less harmful and detrimental space for the blue forces.

Single-Commodity Flow Algorithm (SCFA) in WCCAAM:

$$\min \sum_{i=1}^{I} \sum_{j=1}^{J} R_{ij} X_{ij} \tag{4a}$$

$$\text{subject to:} \sum_{j=1}^{J} X_{ij} \leq S_i \qquad \forall(i) \tag{4b}$$

$$\sum_{i=1}^{J} X_{ij} \geq D_j \qquad \forall(j) \tag{4c}$$

$$X_{ij} \geq 0 \tag{4d}$$

$$\tag{4e}$$

In C-WCCAAM, we introduce binary decision variable Y_{ij}, which represent representing the implementation of cyber-effects for infantry on the engagement path (i, j), i.e., from base i to red infantry j. In contrast, the movements of commodities are represented by continuous variables X_{ij}. Given the introduction of binary decisions variables, we augment the original WCCAAM formulation with the following integer program:

$$\min \sum_{i=1}^{I} \sum_{j=1}^{J} R_{ij}(1 - \epsilon_{ij} Y_{ij}) \tag{5a}$$

$$\text{subject to:} \sum_{i=1}^{I} \sum_{j=1}^{J} C_{ij} Y_{ij} \leq P \tag{5b}$$

$$Y_{ij} \in \{0, 1\} \tag{5c}$$

with the objective to minimize engagement risk without exceeding a "cyber budget" P. The augmentation of the WCCAAM model with cyber-effects leads to the following formulation:

$$\min \sum_{i=1}^{I} \sum_{j=1}^{J} R_{ij}(1 - \epsilon_{ij} Y_{ij}) \tag{6a}$$

$$\text{subject to:} \sum_{j=1}^{J} X_{ij} \leq S_i \qquad \forall(i) \tag{6b}$$

$$\sum_{i=1}^{I} X_{ij} \geq D_j \qquad \forall(j) \tag{6c}$$

$$\sum_{i=1}^{I} \sum_{j=1}^{J} C_{ij} Y_{ij} \leq P \tag{6d}$$

$$\epsilon_{ij} \in [0, 1] \qquad \forall(i, j) \tag{6e}$$

$$Y_{ij} \in \{0, 1\} \qquad \forall(i, j) \tag{6f}$$

$$X_{ij} \geq 0 \qquad \forall(i, j) \tag{6g}$$

After formulating the single-commodity model of C-WCCAAM based on WCCAAM, we can expand the C-WCCAAM to a multi-commodity model and track the different commodities' movements with and without cyber-effects. In terms of model formulation, we introduce a new index t to represent the team commodities. By using a

model that manages the COA of multiple forces at the same time, we will have to set the index for the blue team to be $t = 1, 2, ..., T$ to show how many commodities the blue team is using in its mission to destroy all red targets.

3.2.2 Multi-Commodity

For multi-commodity model, we describe relevant decision variables and model parameters:

Indices:

t: Blue Commodities: Fighters, Armor, Infantry ($T = 1, 2, 3$)

i: Blue Bases: Base 1, Base 2, Base 3 ($I = 1, 2, 3$)

j: Red Targets: Fighters, Armor, Infantry ($J = 1, 2, 3, ..., 9$)

Decisions Variables:

X_{tij}: Number of commodity t from blue base i sent to nullify red target j

Y_{tij}: Cyber-effects for commodity t when engaging red target j from blue base i, in binary form as 1: yes, 0: no

Constants:

R_{tij}: Engagement risk of commodity t from blue base i to nullify red target j

S_{ti}: Total number of commodity t that can be sent from blue base i

D_{tj}: Total number of commodity t required to nullify red target j

P : Cyber budget

C_{tij}: The cost of using cyber-effects for commodity t when engaging red target j from blue base i

ϵ_{tij}: Engagement risk-reduction factor when engaging red target j from blue base i; value between 0 to 1

"Supply nodes" and "demand nodes" are the same terms used in a single-commodity model. Blue bases will be referred to as "supply nodes" in the sense of "providing forces," and the targets will be called "demand nodes." An additional condition that needs to be clarified is a commodity's influence on other commodities. The multi-commodity model assumes that the causality scale for the same commodity from opposing force is 1-to-1 in the model. This means that one blue fighter is the same as one red fighter in terms of conveying one supply unit to one demand unit.

Describe the multi-commodity model used in WCCAAM below:

$$\min \sum_{t=1}^{T} \sum_{i=1}^{I} \sum_{j=1}^{J} R_{tij} X_{tij} \tag{7a}$$

$$\text{subject to:} \sum_{j=1}^{J} X_{tij} \leq S_{ti} \qquad \forall (t,i) \tag{7b}$$

$$\sum_{i=1}^{J} X_{tij} \geq D_{tj} \qquad \forall (t,j) \tag{7c}$$

$$X_{tij} \geq 0 \qquad \forall (t,i,j) \tag{7d}$$

Similar to the single-commodity, the multi-commodity model's objective is to minimize total engagement risk. We introduce a binary decision variable Y_{tij}, represents the implementation of cyber-effects for commodity t on the engagement path (i,j), i.e., from base i to target j.

Given the introduction of binary decisions variables, we augment the original WCCAAM formulation with the following integer program:

$$\min \sum_{t=1}^{T} \sum_{i=1}^{I} \sum_{j=1}^{J} R_{tij}(1 - \epsilon_{tij} Y_{tij}) \tag{8a}$$

$$\text{subject to:} \sum_{t=1}^{T} \sum_{i=1}^{I} \sum_{j=1}^{J} C_{tij} Y_{tij} \leq P \tag{8b}$$

with the objective to minimize engagement risk without exceeding a "cyber budget" P. The augmentation of the WCCAAM model with cyber effects leads to the following formulation:

$$\min \sum_{t=1}^{T} \sum_{i=1}^{I} \sum_{j=1}^{J} R_{tij}(1 - \epsilon_{tij} Y_{tij}) \tag{9a}$$

$$\text{subject to:} \sum_{t=1}^{T} \sum_{i=1}^{I} \sum_{j=1}^{J} C_{tij} Y_{tij} \leq P \tag{9b}$$

$$\sum_{j=1}^{J} X_{tij} \leq S_{ti} \qquad \forall (t, i) \tag{9c}$$

$$\sum_{i=1}^{I} X_{tij} \geq D_{tj} \qquad \forall (t, j) \tag{9d}$$

$$Y_{tij} = Y_{t'ij} \qquad \forall (t, t', i, j) \tag{9e}$$

$$X_{tij} \geq 0 \tag{9f}$$

$$Y_{tij} \in \{0, 1\} \tag{9g}$$

Due to the lack of real-world engagement risk and risk-reduction factors, we construct pseudo data. Additionally, we must provide the "cost" of using specific cyber-effects. This cost could be the amount of money required to acquire and retain a specific cyber effect. We could also consider the cyber-effects as a cost. We can constrain these two "costs" as some "cyber budget" P, the total budget to support and retain the effect during an operation, shown with Equation 9b.

To simplify the model, we assume that if a cyber-effect is used for one commodity, it is used by all. Because of this, once a cyber-effect is utilized, all commodities must "pay" to accomplish the cyber-effect. This constraint, implemented with Equation 9e, can be dropped in if necessary.

Modeling both the unit capacity of a path flow and the associated decision to use cyber reinforcement forms a nonlinear objective function, which is time-consuming

and impractical to solve within a high dimension problem [25]. Therefore, to improve the effectiveness by using MILP solver, the resulting MINLP model is converted into a MILP by adjusting nonlinearity in the objective function coming from each discrete decision variable into two separate variables that represent a path with cyber reinforcement and a path without order reinforcement, respectfully.

There exists a special condition in making decision of cyber-effects. We "linearize" the nonlinear formulation by constructing cyber decisions as alternating "engagement path", one associated with cyber reinforcement X_{tij1} and the one without X_{tij0}:

$$\min \sum_{t=1}^{T} \sum_{i=1}^{I} \sum_{j=1}^{J} \sum_{k=1}^{K} R_{tijk} X_{tijk} \tag{10a}$$

$$\text{subject to: } X_{tij0} \leq M(1 - Y_{tij}) \qquad \forall (t, i, j) \tag{10b}$$

$$X_{tij1} \leq M(Y_{tij}) \qquad \forall (t, i, j) \tag{10c}$$

$$\sum_{j=1}^{J} X_{tij0} + X_{tij1} \leq S_{ti} \qquad \forall (t, i) \tag{10d}$$

$$\sum_{i=1}^{I} X_{tij0} + X_{tij1} \geq D_{tj} \qquad \forall (t, j) \tag{10e}$$

$$\sum_{t=1}^{T} \sum_{i=1}^{I} \sum_{j=1}^{J} C_{tij} Y_{tij} \leq P \tag{10f}$$

$$Y_{tij} = Y_{t'ij} \qquad \forall (t, t', i, j) \tag{10g}$$

$$X_{tijk} \geq 0 \qquad \forall (t, i, j, k) \tag{10h}$$

$$Y_{tijk} \in \{0, 1\} \qquad \forall (t, i, j, k) \tag{10i}$$

$$\tag{10j}$$

Engagement risk R_{tijk} is classified with two paths k to targets: one path with cyber-effects as $k = 1$, one path without cyber-effects as $k = 0$. The engagement risk on the path without cyber-effects will be the original risk R_{tij0} for k is 0, whereas the

risk of the path with cyber-effects will be reduced by a factor of ϵ_{tij}, where k is 1 and $R_{tij1} = R_{tij0}(1 - \epsilon_{tij})$.

IV. Results and Analysis

In this chapter we introduce a modified operational scenario. We then compare optimal COA's generated from WCCAAM and C-WCCAAM. To further explore these optimal COA's, we also provide sensitivity analysis for C-WCCAAM results.

4.1 Scenario

For this work, we adjust a scenario originally used in [5]. Introduced in [8], the scenario concerns two fictitious nations, Nation A and Nation B, fighting against each other in a multi-domain conflict, i.e., including air and ground forces, in attempt to imitate 1990 Gulf War between to Kuwait and Iraq [8].

4.1.1 Single-Commodity

While Chapter 2 emphasized a multi-commodity approach, we first describe a single-commodity scenario where we use C-WCCAAM to minimize engagement risk for "blue" infantry when fighting against "red" infantry.

Table 1: Single-Commodity Scenario

	C-WCCAAM
Nations	Blue Team: Nation A Red Team: Nation B
Commodities	Blue Team: Infantry Red Team: Infantry
Objectives	1. Eliminate all red infantry 2. Find the optimal COA for minimizing engagement risk with cyber-effects

To reiterate, we attempt to find the optimal blue team COA to engage and destroy all red infantry simultaneously with cyber-effect reinforcement, given the assumption of known red team courses of actions, e.g., the number of red units at different locations.

Because we are not given data on engagement risk or risk-reduction variables, we utilize pseudo data, shown in the following tables.

Table 2: Blue Infantry

Blue	Base 1	Base 2	Base 3
Infantry	200	300	500

Table 3: Red Infantry

	Red Infantry 1	Red Infantry 2	Red Infantry 3	Red Infantry 4
Quantity	100	60	130	300

Table 4: Cyber-Effect Risk-Reduction Factor (ϵ_{ij})

		Red Infantry 1 (j = 1)	Red Infantry 2 (j = 2)	Red Infantry 3 (j = 3)	Red Infantry 4 (j = 4)
Blue Infantry	Base 1 (i=1)	0.5	0.8	0.5	0.6
	Base 2 (i=2)	1	0.3	0.9	0.7
	Base 3 (i=3)	0.3	0.6	0.6	0.9

Table 5: Cost C_{ij} (in dollars \$) of using Cyber-Effects Y_{ij}

		Red Infantry 1 (j = 1)	Red Infantry 2 (j = 2)	Red Infantry 3 (j = 3)	Red Infantry 4 (j = 4)
Blue Infantry	Base 1 (i=1)	\$4k	\$3k	\$2k	\$9k
	Base 2 (i=2)	\$1k	\$10k	\$3k	\$6k
	Base 3 (i=3)	\$3k	\$1k	\$1k	\$2k

4.1.2 Multi-Commodity

Our multi-commodity scenario closely relates the scenario in [5]. We include additional fighter and armor units for both Nation A and Nation B.

Table 6: Multi-Commodity Scenario

	C-WCCAAM
Nations	Blue Team: Nation A Red Team: Nation B
Commodities	Blue Team: Fighters, Armor, Infantry Red Team: Fighters, Armor, Infantry
Objectives	1. Eliminate all targets 2. Find the optimal COA for minimizing engagement risk with cyber-effects

Same as in the single-commodity model, we are not given with data on engagement risk or cyber-effect risk-reduction. Thus, we utilize pseudo data shown below.

Table 7: Blue Commodities

Blue	Base 1	Base 2	Base 3
Fighters	4	2	0
Armor	5	20	0
Infantry	280	20	150

Table 8: Red Commodities

	Red Fighters 1	Red Fighters 2	Red Fighters 3	Red Armor 1	Red Armor 2	Red Armor 3	Red Infantry 1	Red Infantry 2	Red Infantry 3
Quantity	2	1	3	10	15	0	100	50	300

Table 9: Cyber-Effect Risk-Reduction Factor (ϵ_{tij})

		Red Fighters 1 (j = 1)	Red Fighters 2 (j = 2)	Red Fighters 3 (j = 3)	Red Armor 1 (j = 4)	Red Armor 2 (j = 5)	Red Armor 3 (j = 6)	Red Infantry 1 (j = 7)	Red Infantry 2 (j = 8)	Red Infantry 3 (j = 9)
Blue Fighters (t = 1)	Base 1 (i = 1)	0.35	0.5	0.4	0.35	0.5	0.4	0.35	0.5	0.4
	Base 2 (i = 2)	0.35	0.5	0.4	0.35	0.5	0.4	0.35	0.5	0.4
	Base 3 (i = 3)	0.35	0.5	0.4	0.35	0.5	0.4	0.35	0.5	0.4
Blue Fighters (t = 2)	Base 1 (i = 1)	0.8	0.6	0.4	0.6	0.67	0.4	0.8	0.2	0.4
	Base 2 (i = 2)	0.8	0.6	0.4	0.3	0.7	0.4	0.8	0.2	0.4
	Base 3 (i = 3)	0.8	0.6	0.4	0.4	0.2	0.4	0.8	0.2	0.4
Blue Fighters (t = 3)	Base 1 (i = 1)	0.8	0.6	0.4	0.5	0.4	0.4	0.6	0.2	0.17
	Base 2 (i = 2)	0.8	0.6	0.4	0.5	0.8	0.4	0.5	0.4	0.4
	Base 3 (i = 3)	0.8	0.6	0.4	0.33	0.4	0.4	0.67	0.2	0.2

Table 10: Cost C_{tij} (in dollars \$) of using Cyber-Effects ϵ_{tij}

		Red Fighters 1 (j = 1)	Red Fighters 2 (j = 2)	Red Fighters 3 (j = 3)	Red Armor 1 (j = 4)	Red Armor 2 (j = 5)	Red Armor 3 (j = 6)	Red Infantry 1 (j = 7)	Red Infantry 2 (j = 8)	Red Infantry 3 (j = 9)
Blue	Base 1 (i = 1)	\$3k	\$3k	\$3k	\$1k	\$2k	\$3k	\$9k	\$9k	\$9k
Fighters	Base 2 (i = 2)	\$3k	\$3k	\$3k	\$2k	\$2k	\$2k	\$9k	\$9k	\$9k
(t = 1)	Base 3 (i = 3)	\$3k	\$3k	\$3k	\$2k	\$2k	\$2k	\$9k	\$9k	\$9k
Blue	Base 1 (i = 1)	\$3k	\$3k	\$3k	\$2k	\$2k	\$2k	\$9k	\$9k	\$9k
Fighters	Base 2 (i = 2)	\$3k	\$3k	\$3k	\$2k	\$2k	\$2k	\$9k	\$9k	\$9k
(t = 2)	Base 3 (i = 3)	\$3k	\$3k	\$3k	\$2k	\$2k	\$2k	\$9k	\$9k	\$9k
Blue	Base 1 (i = 1)	\$3k	\$3k	\$3k	\$2k	\$2k	\$2k	\$9k	\$9k	\$9k
Fighters	Base 2 (i = 2)	\$3k	\$3k	\$3k	\$2k	\$2k	\$2k	\$9k	\$9k	\$9k
(t = 3)	Base 3 (i = 3)	\$3k	\$3k	\$3k	\$2k	\$2k	\$2k	\$9k	\$9k	\$9k

In any real-world scenario, the manner in which one unit engages or interacts with other commodities is complicated, since a single commodity may serve numerous uses. As a result, we simplified our model, ensuring that a trade-off between commodities from both teams was balanced and that unit-to-unit interchangeability was maintained. For example, we expect that blue fighters would engage in battle with red fighters, blue armor would engage in combat with red armor, and blue infantry would engage in combat with red infantry. We continue to follow the assumptions in 3.1

4.2 COA Results

After analysis of the modified single-commodity scenario with WCCAAM and C-WCCAAM, we generate two set of COAs, one without cyber-effects and one with cyber-effects.

4.2.1 Single-Commodity

Table 11: COAs between WCCAAM and C-WCCAAM, Scenario Table 1

WCCAAM	C-WCCAAM
Optimal Flow for Infantry:	Optimal Flow for Infantry, (Cyber On):
Base 1 ->Red Infantry 1: 30	Base 1 ->Red Infantry 2: 60
Base 2 ->Red Infantry 2: 60	Base 2 ->Red Infantry 1: 100
	Base 2 ->Red Infantry 3: 130
Base 3 ->Red Infantry 1: 70	Base 3 ->Red Infantry 4: 300
Base 3 ->Red Infantry 3: 130	
Base 3 ->Red Infantry 4: 300	
	Optimal Flow for Infantry, (Cyber Off):
	No troop movement occurs without cyber-effect
	Cyber Budget: $9k
Total Engagement Risk: 1130	Total Engagement Risk: 144

Obviously, the total engagement risk with C-WCCAAM is lower, with a total risk of 144 compared to 1120 for WCCAAM. We also observe more units sent from Base 2 to nullify other targets, i.e., Red Infantry 1 and Red Infantry 3, and fewer units sent from Base 3. Overall, we have drastically reduced the total engagement risk, by roughly 87.2%, with an additional $9k cyber-effects spending. After finding this optimal COA, the commander should assess if it is worthwhile to spend $9k to reduce engagement risk to this level during the COA approval phase.

4.2.2 Multi-Commodity

We also generate two set of COAs, one without cyber-effects, and one with cyber-effects for the multi-commodity scenario.

Table 12: COAs between WCCAAM and C-WCCAAM, Scenario Table 6

WCCAAM	C-WCCAAM
Optimal Flow for Fighters:	Optimal Flow for Fighters:
Base 1 ->Red Fighters 2: 1	Base 1 ->Red Fighters 2: 1
Base 1 ->Red Fighters 3: 3	Base 1 ->Red Fighters 3: 3
Base 2 ->Red Fighters 1: 2	Base 2 ->Red Fighters 1: 2
Optimal Flow for Armor:	Optimal Flow for Armor:
Base 1 ->Red Armor 1: 5	Base 1 ->Red Armor 1: 5
Base 2 ->Red Armor 1: 5	Base 2 ->Red Armor 1: 5
Base 2 ->Red Armor 2: 15	Base 2 ->Red Armor 2: 15
Optimal Flow for Infantry:	Optimal Flow for Infantry:
Base 1 ->Red Infantry 1: 100	Base 1 ->Red Infantry 1: 100
Base 1 ->Red Infantry 2: 50	Base 1 ->Red Infantry 2: 50
Base 1 ->Red Infantry 3: 130	Base 1 ->Red Infantry 3: 130
Base 2 ->Red Infantry 3: 20	Base 2 ->Red Infantry 3: 20
Base 3 ->Red Infantry 3: 150	Base 3 ->Red Infantry 3: 150
	Cyber Budget: $179k
Total Engagement Risk: 1125	Total Engagement Risk: 749

While WCCAAM and C-WCCAAM have distinct model formulations, their COAs for

unit movement may be identical in certain situations, e.g., when the blue side's unit count equals that of the red team, with the difference that C-WCCAAM would have a lower risk of engagement. For the optimal COA from C-WCCAAM for this scenario, the model opts for the same unit movement on the blue team as the WCCAAM COA. However, the overall risk of engagement based on C-WCCAAM with cyber-effects is 749, roughly 33% less than the risk associated with the WCCAAM model without cyber-effects, with an additional $179k in cyber-effects spending.

4.3 Sensitivity Analysis

We analyze the optimal COAs shown in Tables 11 and 12 by adjusting given parameters such as the pseudo engagement risks, cyber-effects, and the costs of using the effects. Because we do not know what the true parameters are in the real world, we run sensitivity analyses on single and multi-commodity models to see how engagement risk and cyber-effect decisions change when the formation parameters change. By examining "budget" as a resource that we can control in our model, the analysis can consider engagement risk and cyber choices concerning cyber resources such as available funds and an available number of buyer-effects. We also explore perturbations in cyber-effect costs.

4.3.1 Single-Commodity

4.3.1.1 Engagement Risk vs. "Cyber Budget": Funds

The engagement risk on an individual path for a commodity moving from blue base i to red target j will either remain the same or be decreased by available cyber-effects. However, each cyber effect requires a specific amount of funds to support and to maintain the effects during an operation. As a result, having more funds to support cyber operations should have a positive impact engagement risk.

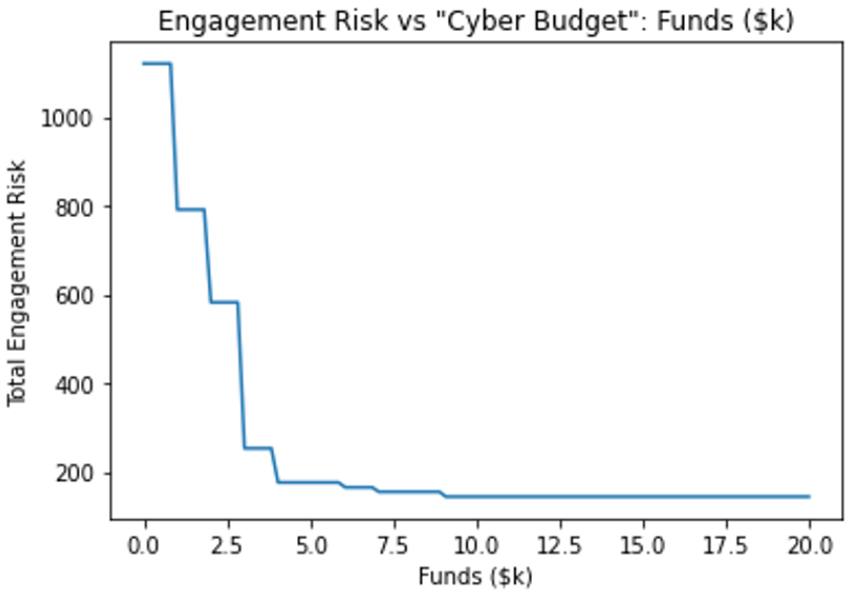

Figure 5: Engagement risk vs. Changing in Funds as Cyber Budget

Figure 5 of engagement risk versus funds ($k) demonstrates that the total engagement risk decreases as the funds for supporting cyber operations increases. Also, the first few cyber-effects purchased reduces engagement risk more significantly than the last few purchased. Another observation from the plot reveals that some points on the graph show a horizontal line, indicating that even with an increase in cyber budget the engagement risk associated with the optimal COA remains the same. Also, the engagement risk is minimized at 144, as opposed to the WCCAAM risk of 1120 when we raise funds to $9k or more. Therefore, if we increase the funds as a "cyber budget" parameter, the total engagement risk will be lower until it no longer decreases, which occurs when we have $9k or more to support cyber-effects.

4.3.1.2 Engagement Risk vs. "Cyber Budget": Available Cyber-Effects

While "cyber budget" can represent the total amount of funds that available to support cyber-effects, we can also constrain the total available cyber-effects that can be used during a mission.

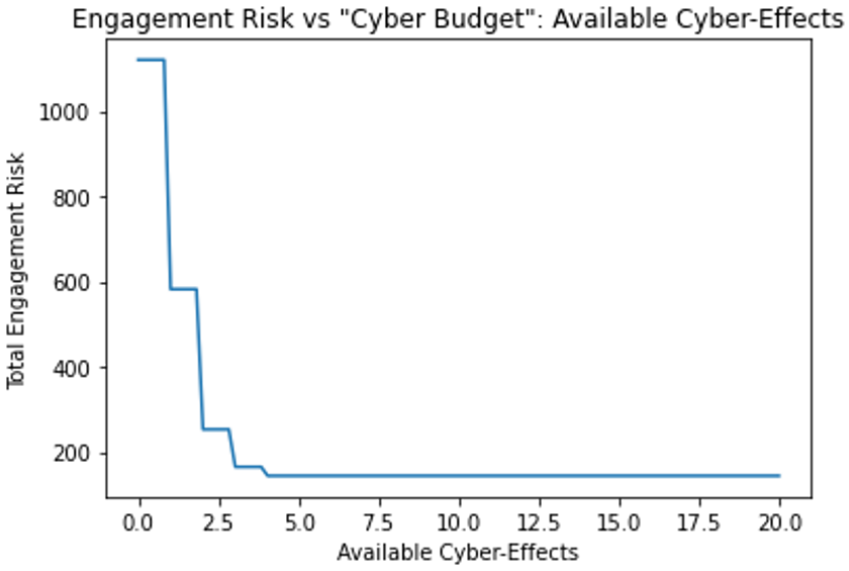

Figure 6: Engagement risk vs. Changing in Available Cyber-Effects as Cyber Budget

Figure 6 shows an inverse relationship between the total engagement risk and available cyber-effects in a mission. Because effects can reduce or maintain engagement risks along various engagement paths, increasing number of available cyber-effects as a "cyber budget" will reduce engagement risk until it reaches the minimum. Based on the plot, we need at most four cyber-effects to minimize the engagement risk for blue infantry to nullify all red infantry. Also, we can observe how much engagement risk decreases as the number of cyber-effects increases. In particular, the first cyber-effect selected by the model reduces the risk more than any other additional cyber-effects afterward.

4.3.1.3 Location of Cyber-Effects vs. "Cyber Budget": Funds

From the previous analysis, we can calculate the maximum number of cyber effects needed to minimize the engagement risk; we observe a trade-off between engagement risk and budget. However, this information does not provide insight into which engagement paths used cyber-effects to reduce the engagement risk. Thus, we inspect where to implement cyber-effects based on total funds available for supporting cyber operations. For simplification, we identify base-target connection as arcs, defined in Table 13

Table 13: Location of Cyber-Effects, Engagement Path Description of Figure 7

Arc (Location)	Red Infantry 1	Red Infantry 2	Red Infantry 3	Red Infantry 4
Infantry Blue Base 1	1	2	3	4
Infantry Blue Base 2	5	6	7	8
Infantry Blue Base 3	9	10	11	12

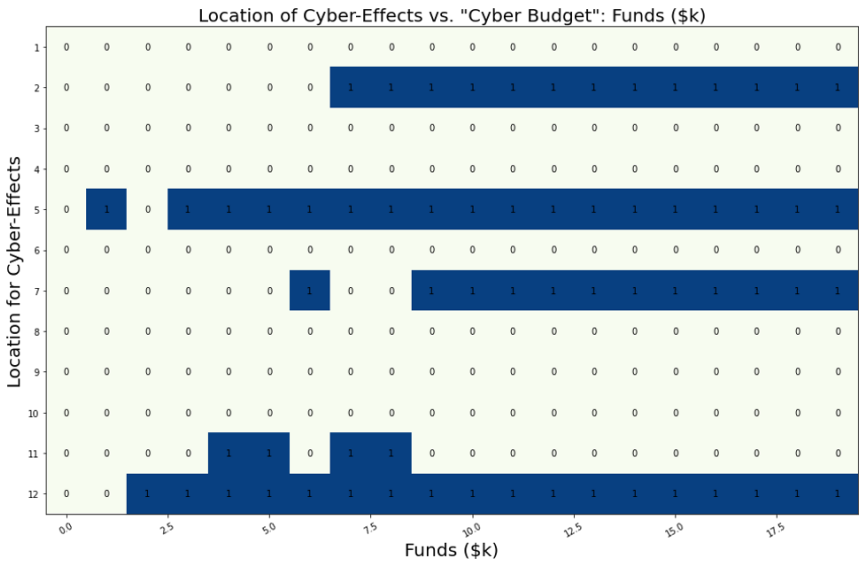

Figure 7: Location of Cyber-Effects vs. Funds as Cyber Budget

Given an increasing cyber budget, we observe that the first effect purchased is on Arc 5. As more budget becomes available, the effect on Arc 5 is traded for the effect on Arc 12. The trade-space continues to select new effects and arcs until cyber effects are used on Arcs 2, 5, 7, 11, and 12. It is interesting to note that Arc 11 employs cyber effects only in middle budget regions, until more effective mixes are available at higher budget levels. Regardless of budget, cyber effects are not chosen for Arcs 1, 3, 4, 6, 8, 9, and 10 over the entire range of available budget.

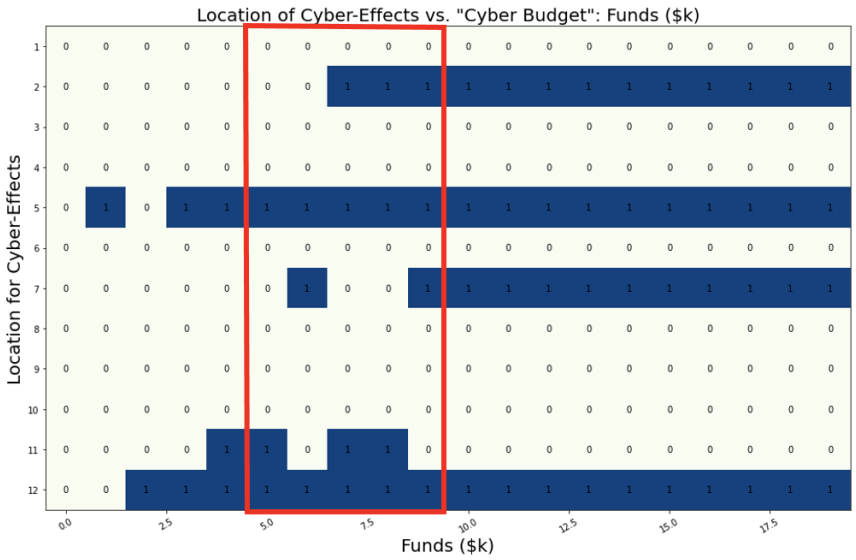

Figure 8: Location of Cyber-Effects vs. Funds as Cyber Budget

The middle budget region, highlighted in the red box in Figure 8, provides an interesting result in the budget-effects trade-space. As soon as a sufficient budget is available, the model selects cyber-effects for Arc 11. However, the effects on Arc 7 are preferred over those on Arc 11 when the budget can cover only one of these two options. As the budget increases, Arc 11 is chosen over Arc 7 when the budget allows. Additional effects can be purchased along with Arc 2. However, once there is a sufficient budget for effects on both Arcs 2 and 7, the effects on Arc 7 are again preferred over those of Arc 11. We describe these results further in Table 14.

Table 14: Description of Best Arc(s) for Cyber-Effects on Figure 8

	1st	2nd	3rd	4th
\$0k - \$1.5k	Arc 5			
\$1.5k - \$2.5k	Arc 12			
\$2.5k - \$3.5k	Arc 5	Arc 12		
\$3.5k - \$5.5k	Arc 5	Arc 12	Arc 11	
\$5.5k - \$6.5k	Arc 5	Arc 12	Arc 7	
\$6.5k - \$9.0k	Arc 5	Arc 12	Arc 2	Arc 11
\$9.0k or above	Arc 5	Arc 12	Arc 2	Arc 7

Changing the cost of cyber-effects on an individual arc can also impact the decision of where to implement cyber-effects.

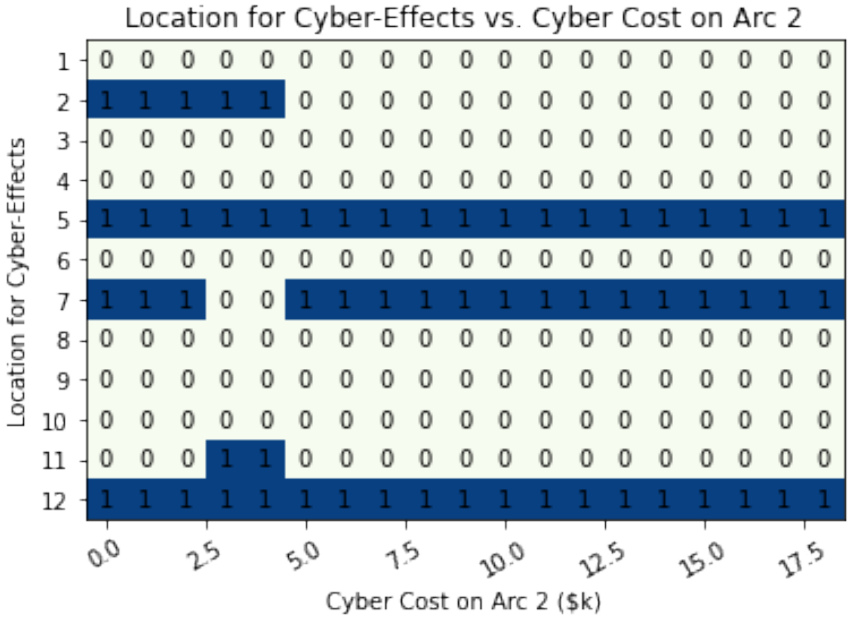

Figure 9: Best arc(s) for cyber-effects when changing cost of cyber-effects on arc 2

Figure 9 shows the choices of cyber-effects on other locations at different cost of one location. In this example, we can observe how the locations for cyber-effect

change in respect to the changing cyber cost of arc 2.

Table 15: Best arc(s) combination at each level cyber cost on arc 2 based on Figure 9

Cost of Cyber-Effects on Arc 2	Arc 2	Arc 5	Arc 7	Arc 11	Arc 12
\$0k - \$3k	x	x	x		x
\$3k - \$4.5k	x	x		x	x
\$4.5k or above		x	x		x

If the cyber cost of arc 2 increases to the range of \$2.5k to \$4.5k, we no longer select arc 7 instead substituting it with arc 11. An equivalent result occurs when the cyber budget is between \$5.5k and \$6.5k, given the cost of cyber-effect on Arc 2 is \$3k.

Table 16: Rank of arc(s) at each funds level in \$ that equivalent to results when changing cyber-cost on arc 2 Table 15

	1st	2nd	3rd	4th
\$0k - \$1.5k	Arc 5			
\$1.5k - \$2.5k	Arc 12			
\$2.5k - \$3.5k	Arc 5	Arc 12		
\$3.5k - \$5.5k	Arc 5	Arc 12	Arc 11	
\$5.5k - \$6.5k	Arc 5	Arc 12	Arc 7	
\$6.5k - \$9.0k	Arc 5	Arc 12	Arc 2	Arc 11
\$9.0k or above	Arc 5	Arc 12	Arc 2	Arc 7

4.3.1.4 Location of Cyber-Effects vs. "Cyber Budget": Available Cyber-Effects

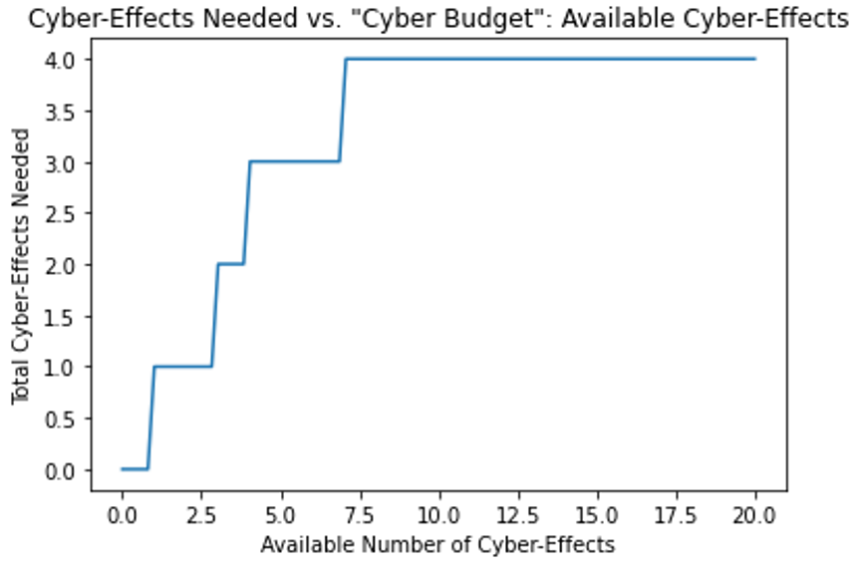

Figure 10: Cyber-Effects Needed with Respect to Available Cyber-Effects

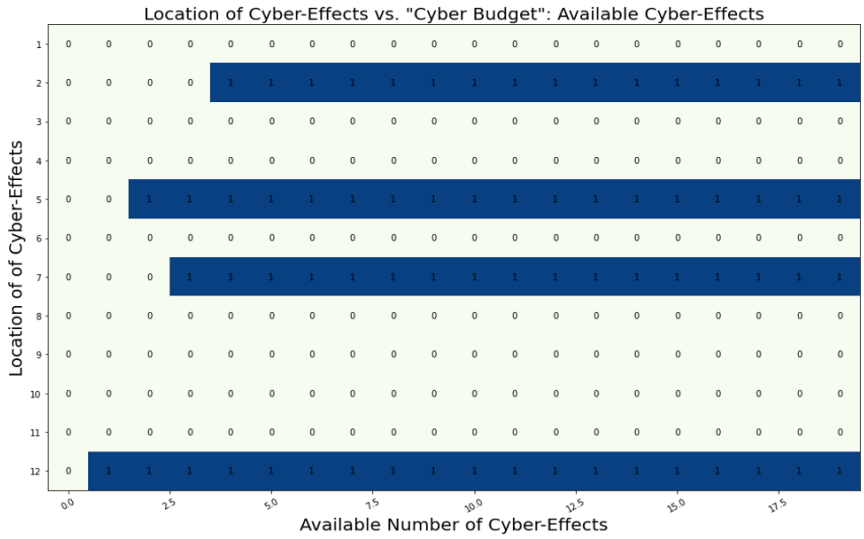

Figure 11: Location of Cyber-Effects with Respect to Available Cyber-Effects

When considering the number of effects as a "cyber budget," decisions on implementing cyber-effects can reveal other insights. For example, if we have one cyber-

effect available, the effect would be on arc 12, the engagement path for blue infantry 3 to nullify red infantry 4. The additional availability of cyber-effects reveals the next-best decision to implementing the cyber-effect. At the very beginning, arc 12 is the best decision; the next-best decisions are arc 5, arc 7 and arc 2, in that order. Because each decision on where to put a cyber-effect is not made based on the amount of funds available, the next best cyber-effect in chosen regardless of the monetary cost of said cyber-effect.

4.3.2 Multi-Commodity

4.3.2.1 Engagement Risk vs. "Cyber Budget": Funds

Similar to the single-commodity results, we explore the trade-offs between engagement risk and cyber budget, shown in Figure 12.

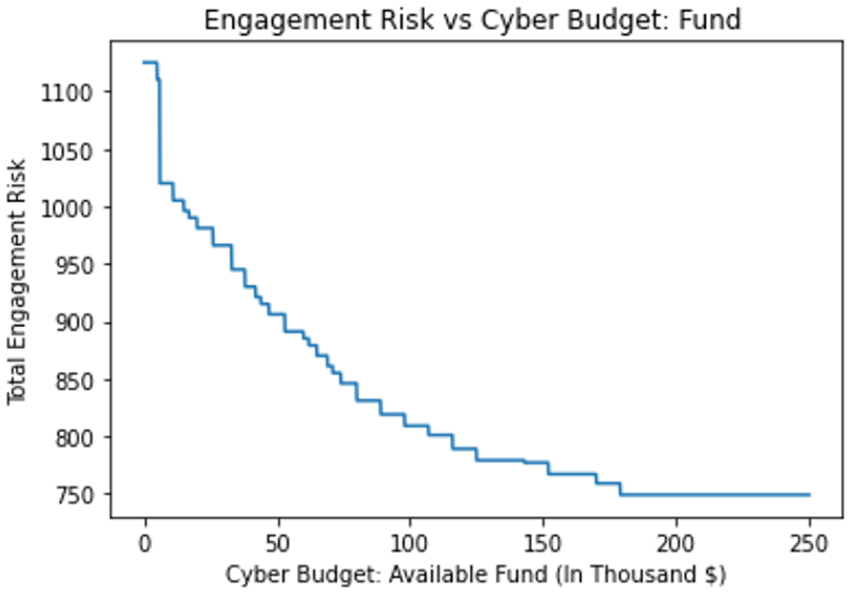

Figure 12: Total Engagement Risk with Respect to Available Funds

Figure 12 indicates the decrease of overall engagement risk until achieving the minimal risk of 749 at a cyber budget of $179k. Also, the rate of decrease in en-

gagement risk slows until reaching the minimum. Figure 13 shows the number of cyber-effects utilized as the cyber budget increases.

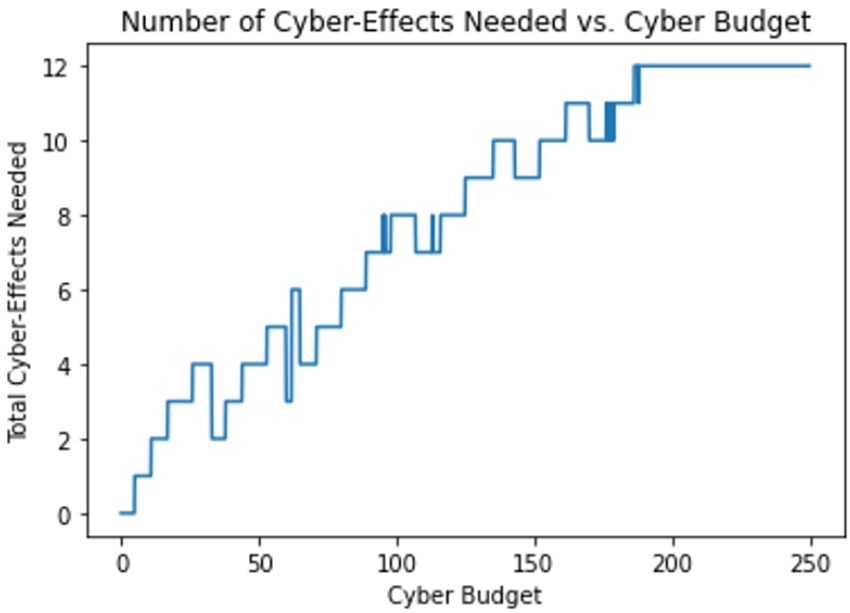

Figure 13: Total Cyber-Effects Needed with Respect to Available Funds

We see that that more cyber-effects are not always necessary to reduce engagement risk. Although the plotted trend is positively correlated between the number of cyber-effects required and the amount of cyber budget available, a few points show that when more budget is available, we might trade a cheaper set of effects for a single more expensive one, with high efficiency in terms of risk reduction on total engagement risk. For example, we see Figure 13, with respect to our multi-commodity scenario at a cyber budget of around \$30k, we go from four cyber-effects to just two in the optimal solution.

4.3.2.2 Engagement Risk vs. "Cyber Budget": Available Cyber-Effects

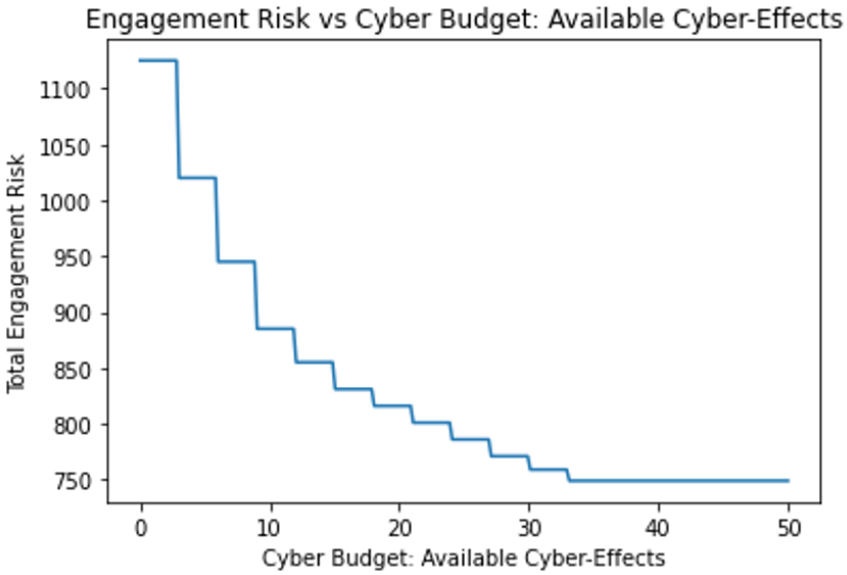

Figure 14: Total Engagement Risk with Respect to Available Cyber-Effects

With a higher cyber budget decreases the total engagement risk decreases, other we can afford more cyber-effects in an operation. In our model, the multi-commodity formulation requires that all cyber-effects on all commodities along the same engagement path are aligned.

4.3.2.3 Location of Cyber-Effects vs. "Cyber Budget": Funds

If one commodity has a cyber-effect, all the other commodities utilize that effect. Because we have three different force commodities, we have to make twelve cyber-effect decisions but must "pay" for all commodities along on engagement path even though a commodity might not use that path. This constraint simplifies the model, but it could also make it less realistic. Because all commodities along the same engagement path are aligned, the cyber-effect decisions will be the same across all

commodities. An exmaple of this is shown in Figure 15.

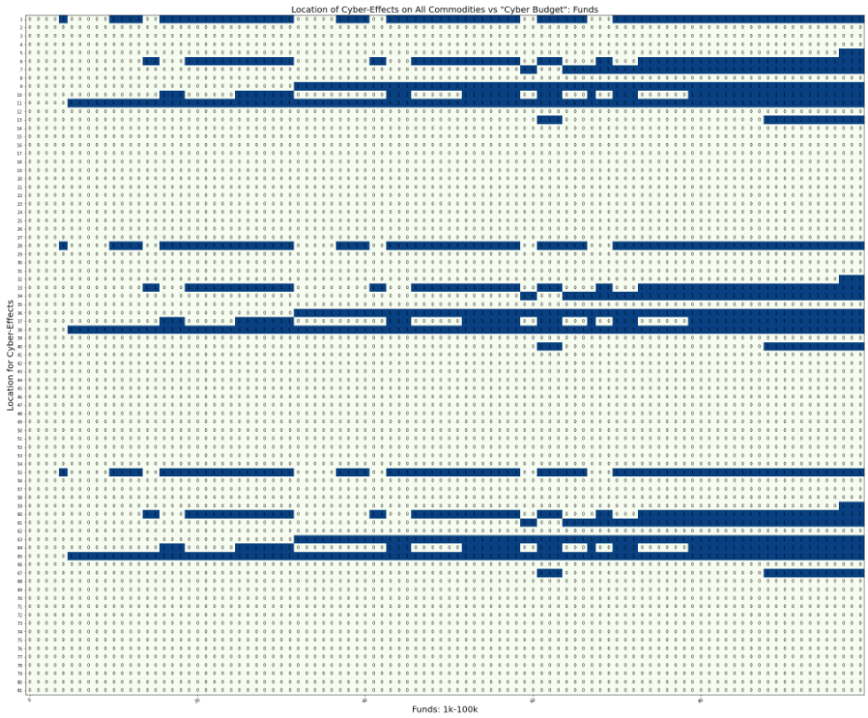

Figure 15: Best Location for Cyber-Effects with Respect to Available Funds

Instead of using all commodities, we can simplify the sensitivity analysis by selecting one commodity. Taking fighters across all blue bases, with each engagement path base to target on Table 17.

Table 17: Arc(s) Descriptions for Fighters

Arc (Location)	Red Fighters 1	Red Fighters 2	Red Fighters 3	Red Armor 1	Red Armor 2	Red Armor 3	Red Infantry 1	Red Infantry 2	Red Infantry 3
Fighters Blue Base 1	1	2	3	4	5	6	7	8	9
Fighters Blue Base 2	10	11	12	13	14	15	16	17	18
Fighters Blue Base 3	19	20	21	22	23	24	25	26	27

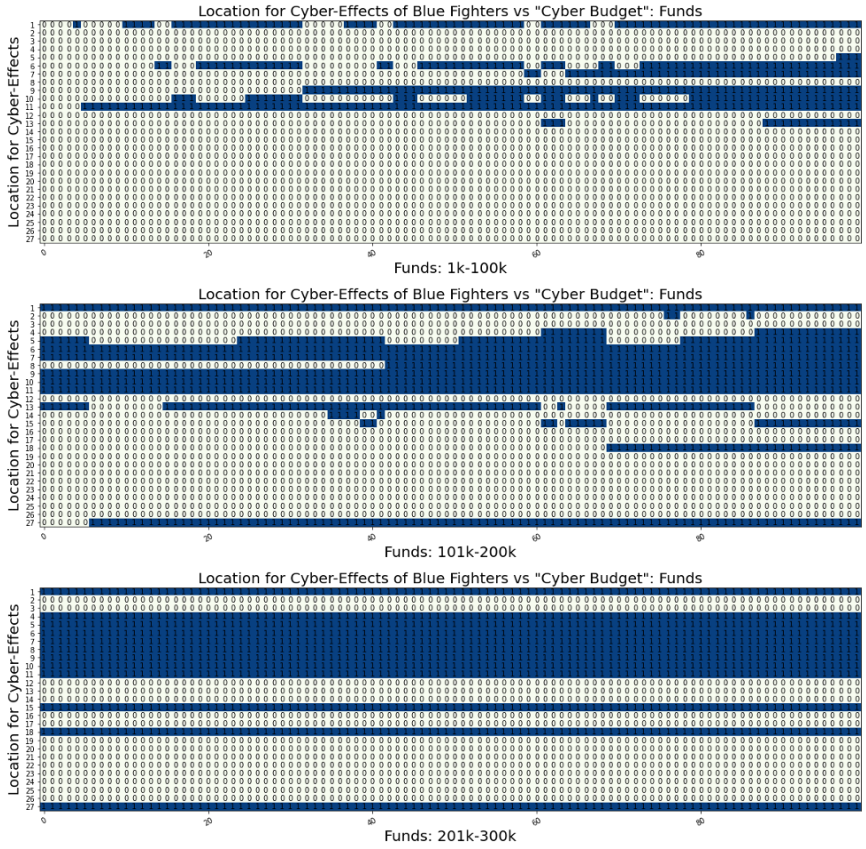

Figure 16: Location for Cyber-Effects with Respect to Available Funds

Based on Figures 16 shows the location of cyber-effects with respect to funds as a "cyber budget." We observe that the commodities from blue bases 1 and 2 would engage more often with the red targets with cyber-effects than the commodities from blue base 3. Especially when funds range from \$1 to \$100, all cyber-effects are concentrated on commodities from base 1 and base 2 to all red targets. There are few effects implemented for commodities in base 3 to nullify red team targets. Although we implemented the cyber-effect for fighters from blue base 3 when funds were \$174, it does not indicate that we should send fighters from blue base 3 to battle against other red fighters since all commodities have to "pay" for the cyber-effects decision, even if they do not use it for a mission. In this scenario, the cost of using cyber effects may be higher than it should be since we have to "turn them on" for enemy

commodity.

4.3.2.4 Location of Cyber-Effects vs. "Cyber Budget": Available Cyber-Effects

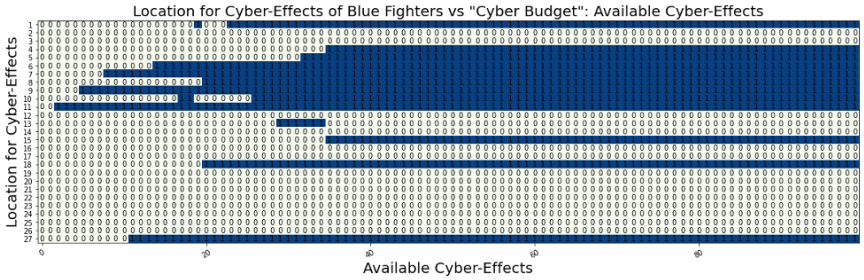

Figure 17: Location for Cyber-Effects with Respect to Available Cyber-Effects

Instead of constraining the cyber monetary budget, we can also observe the location of cyber-effects changing when there is a change in the available number of cyber-effects implemented in a mission. When increasing the number of cyber-effects, we tend to implement cyber-effects from Arc 5 to Arc 11. We prefer to use cyber-effects on fighters from Blue Base 2 to Red Fighters 1 and Red Fighters 2. Also, we implemented a cyber-effect on Arc 1 where fighters from blue base 1 fight against the red fighters 1. As previously stated, when one commodity has the cyber-effect, the constraint of all other commodities employs the effect; this plot demonstrates that we have purchased additional cyber-effects on any other arc(s) where blue fighters do not obtain conflicting action with any other red targets besides the red fighters. For example, we have utilized cyber-effect on Arc 27 for blue fighters from base 3 where they do not have engagement with red infantry 3. As a result, we have to "pay" for this extra effect. Blue infantry from base 3 that has this cyber-effect and wants to fight against red infantry and fighters as one of the commodities at base 3 must pay for the effect. Also, we have achieved an equilibrium level on the location of where

to launch the effects when the available number of cyber-effects is approximately 36.

The plot blow shows how the costs of cyber-effects on blue fighters from Base 2 can affect the decision on location of where to implement the effects.

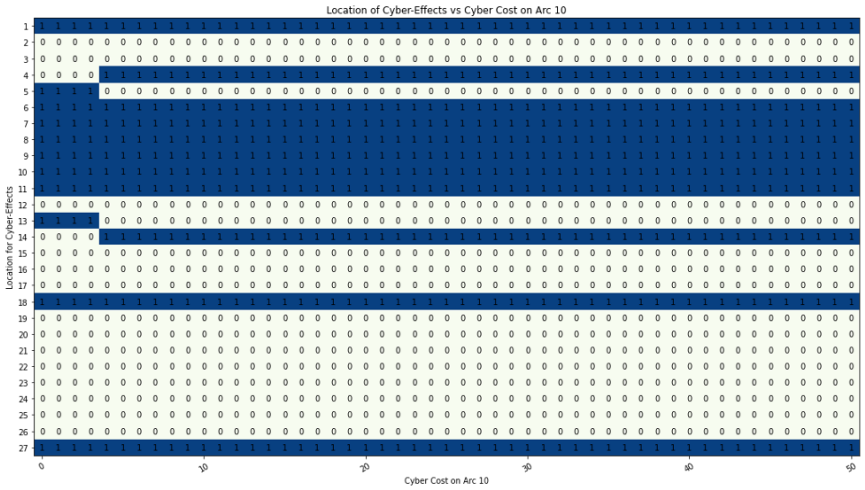

Figure 18: Location for Cyber-Effects with Respect to the Cost on Arc 10

Figure 18 shows how the costs of cyber-effects on an individual arc can affect the decision on location of where to implement the effects. It can be difficult to inspect which arc(s) will be implemented with effects since any other commodities from the same location may "force" the fighters to use the cyber-effect as reinforcement, even though the cost of using cyber-effect can become a hefty financial burden to whom in charge of mission for fighters. Also, if we have only equivalent number of blue fighters to red fighters and without any monetary cyber budget constraint, we may have to enforce to all fighters to use cyber-effects regardless of the cyber cost to reduce the engagement risk while fighting against the red fighters.

V. Conclusions and Future Works

Based on the analysis of C-WCCAAM, we can conclude that implementing cyber-effects can effectively reduce engagement risk. The Cyber-wargaming model can accurately capture the features and characteristics of a real-world scenario, especially when assumptions on engagement risk and reduction factors are provided. Although the critical data such as engagement risk for each commodity and the risk-reduction factors are not provided in the first place, C-WCCAAM shows significant results in optimizing the COA, with respect to the engagement risk, by changing the locations of cyber-effects and the cyber-effect resources P.

Future work might explore more assumptions related to the certainties associated with our model parameters, e.g., engagement risk and cyber-effectiveness. For example, consider a situation where we do not know exactly the reduction in engagement risk a cyber-effect might achieve. Rather, we might instead have a range of possible values. Additionally, in our work, we assume enemy action is known. In reality, this assumption may be harmful, so we might instead consider a small set of enemy COAs, each with a specific probability of occurring. Additionally, we can use optimization techniques to react to possible enemy actions by using C-WCCAAM in a real-world wargame, making a WCCAAM/C-WCCAAM application interface GUI through open-source methods.

Bibliography

1. Kate Kuehn. Assessment strategies for educational wargames. *Journal of Advanced Military Studies*, 12(2):139–153, 2021.

2. Robert O Work and Paul Selva. Revitalizing wargaming is necessary to be prepared for future wars. *War on the Rocks*, Dec 2015.

3. Andrew Hanna. *The Invisible U.S. - Iran Cyber War*, Oct 2019.

4. Rex Brynen. Review: Gaming disease response by ed mcgrady and john curry, May 2021.

5. William T DeBerry, Richard Dill, Kenneth Hopkinson, Douglas D Hodson, and Michael Grimaila. The wargame commodity course of action automated analysis method. *The Journal of Defense Modeling and Simulation*, page 15485129211028318, 2021.

6. Naval war college; wargaming.

7. Elizabeth M. Bartels. Getting the most out of your wargame, Jan 2016.

8. Matthew B Caffrey. *On wargaming: How wargames have shaped history and how they may shape the future*, volume 43. Naval War College Press, 2019.

9. Sun Tzu and John Minford. The art of war. *New England Review (1990-)*, 23(3):5–28, 2002.

10. Richard L. Wampler, James H. Centric, and Margaret S. Salter. The military decision-making process (mdmp): A prototype training product. 1998.

11. Peter P Perla and ED McGrady. Why wargaming works. *Naval War College Review*, 64(3):111–130, 2011.

12. Jan Oliver Schwarz. Business wargaming: developing foresight within a strategic simulation. In *Foresight for Dynamic Organisations in Unstable Environments*, pages 15–30. Routledge, 2013.

13. *How to master wargaming: commander and staff guide to improving course of action analysis*. CALL, Center for Army Lessons Learned, 2020.

14. David Furness. Winning tomorrow's battles today. *Marine Corps Gazette (Web Edition)*, 2019.

15. David A Shlapak and Michael W Johnson. Reinforcing deterrence on nato's eastern flank: Wargaming the defense of the baltics. Technical report, RAND Arroyo Center Santa Monica United States, 2016.

16. David Vergun. Russian strategic forces reportedly on high alert as fighting in ukraine intensifies. *U.S. Department of Defense*, Feb 2022.

17. Missy Ryan. With russian nuclear forces on alert, ukraine crisis enters more dangerous phase. *The Washington Post*, Feb 2022.

18. Caitlin Talmadge. What putin's nuclear threats mean for the u.s. *The Wall Street Journal*, Mar 2022.

19. Nina Kollars. Pathologies of obfuscation. Nov 2021.

20. Jeremy F Sepinsky, Eric Heubel, and Matthew Cumpian. Gaming cyber in an operational-level wargame: Merlin cyber wargame module rules for adjudicators. *Center for Naval Analyses, Virgina*, Jan 2019.

21. Solveig Bruvoll, Jo E Hannay, Guro K Svendsen, Martin L Asprusten, KM Fauske, VB Kvernelv, Rikke A Løvlid, and Jens Inge Hyndøy. Simulation-supported wargaming for analysis of plans. In *Proc. NATO Modelling and Simula-*

tion Group Symp. on M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence (STO-MP-MSG-133), 2015.

22. Per-Idar Evensen, Svein Erlend Martinussen, Marius Halsør, and Dan Helge Bentsen. Wargaming evolved: Methodology and best practices for simulation-supported wargaming. 2019.

23. Pujari Harish Kumar and R. Mageshvaran. Methods and solvers used for solving mixed integer linear programming and mixed nonlinear programming problems: A review. *International Journal of Scientific & Technology Research*, 9:1872–1882, 2020.

24. Shanglun Wang. Mixed-integer programming: A guide to computational decision-making, Jan 2018.

25. F Delbos, T Feng, J Ch Gilbert, and D Sinoquet. Nonlinear optimization for reservoir characterization. In *ENGOPT International conference on engineering optimization, Rio de Janeiro, Brazil*, pages 1–5, 2008.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704–0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
24–03–2022	Master's Thesis	Sept 2020 — Mar 2022

4. TITLE AND SUBTITLE

The Cyber Wargame Commodity Course of Action Automated Analysis Method

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Hoffendahl, Alex M, 1st Lt, USAF

5d. PROJECT NUMBER

22C226

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENS-MS-22-M-138

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/Plan & Programs Directorate
Sponsor Representative: Kenneth Selz
2610 7th St, Fairborn, OH 45324
Email: kenneth.selz@us.af.mil
COMM 312-986-4635

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/XP

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

This work is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

The purpose of this research is to enhance the analytical capabilities and overall usability of the Wargame Commodity Course of Action Automated Analysis Method (WCCAAM) by incorporating cyber effects in determining optimal blue-team actions. In contrast to WCCAAM, the extended approach, aptly named the Cyber-Wargame Commodity Course of Action Automated Analysis Method (C-WCCAAM), balances engagement risk with a selection of blue-team cyber effects, in order to combat enemy targets. The resulting model utilizes an multi-commodity flow algorithm (MCFA) approach within a multi-objective mixed-integer linear program (MO-MILP) to determine an optimal blue-force course of action (COA). We explore a fictitious wargame scenario and compare C-WCCAAM on this scenario to previous results achieved with WCCAAM, achieving lower risk by utilizing potential cyber effects in our blue-force COA. We also assess the robustness of our optimal COA through sensitivity analysis.

15. SUBJECT TERMS

cyber wargaming, linear optimization, military decision making process (MDMP), multi-commodity network flow, sensitivity analysis, decision-making, cyber-effects, course of action (COA)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Capt Chancellor Johnstone, AFIT/ENC
U	U	U	UU	62	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636 x4619 chancellor.johnstone@afit.edu