Multi-Objective Multi-Commodity Flow Optimization for Wartime Planning with Cyber-Effects

Alex Hoffendahl
United States Air Force
alex.hoffendahl.1@us.af.mil

Chancellor Johnstone
Air Force Institute of Technology
chancellor.johnstone.1@us.af.mil

Alex Stephens
United States Air Force
alexander.stephens.7@us.af.mil

Richard Dill
Air Force Institute of Technology
richard.dill@us.af.mil

Lance Champagne
Air Force Institute of Technology
lance.champagne.1@us.af.mil

ABSTRACT

In this work, we enhance the analytical capabilities and overall usability of cyber-wargames by providing a quantitative approach for generating optimal cyber-effect courses of action in conjunction with other kinetic courses of action. Specifically, we introduce the Cyber-Wargame Commodity Course of Action Automated Analysis Method, which balances risk with cost. We utilize a multi-commodity flow (MCF) formulation within a multi-objective mixed-integer program (MO-MIP) to determine optimal courses of action in a wargame scenario. We also assess the robustness of our optimal course of action through sensitivity analysis.

1 INTRODUCTION

The focus of this research is to explore the implementation of cyber-effects in wargaming. To motivate this discussion, we recall a real-world example concerning Iran. Since 2009, Iran has executed a continuous stream of cyber attacks targeting the United States (US) government and private sector systems, costing western firms millions of dollars in lost business and creating a substantial financial burden to local residents. Beginning in 2020, conflicts between the US and Iran have consistently taken place in cyberspace. Although the breadth remains unclear, cyberspace has become a primary battleground, providing an alternative to kinetic military action [12]. The prevalence of cyber capabilities has increased the technical complexity of modern warfare; today's warfare is more technologically advanced than ever and those using cyber capabilities gain an operational advantage [11].

In previous research, [8] introduced the Wargame Commodity Course of Action Automated Analysis Method (WCCAAM) as a systematic procedure to aid in the course of action (COA) development, analysis and comparison phases of the military decision-making process (MDMP). Assuming enemy behavior is known, along with high-reliability on information sources, WCCAAM generates an optimal COA, minimizing engagement risk subject to successfully achieving various objectives, e.g., nullifying enemy targets. We introduce an extended version of WCCAAM, named Cyber-WCCAAM (C-WCCAAM), which delivers an optimal friendly COA considering two objectives:

(1) minimize engagement risk
(2) minimize cyber-effect cost

To consider decisions related to the employment of cyber-effects within a wargame, we utilize a mixed-integer program (MIP). C-WCCAAM encodes cyber-effects as binary decision variables; a one represents the use of a particular cyber-effect and a zero represents anything otherwise. Thus, C-WCCAAM enables decisions related to the employment of friendly forces and cyber-decisions, simultaneously. We note that while our application utilizes a multi-objective formulation with two objectives, i.e., a bi-objective formulation, there is no reason one could not include additional objectives. The inclusion of additional objectives would be left to the decision-maker.

We compare results generated with WCCAAM to those generated with C-WCCAAM on a fictitious, yet plausible, scenario, adding friendly cyber-effects into the decision space. With C-WCCAAM, we provide a trade-off between engagement risk and cost for a cyber-effect. Ultimately, we extend WCCAAM to incorporate multiple cyber-effects, formulating a new modeling approach that advances the state-of-the-art in cyber wargaming and COA development.

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. Section 5 concludes the paper.

2 BACKGROUND

This section provides the necessary background and foundational concepts for C-WCCAAM, to include a brief discussion of cyber-wargaming and WCCAAM.

2.1 Wargaming in the Cyber Realm

Historically, the US military has relied on wargaming to achieve both short-term and long-term objectives, examples of which include naval warfare during World War II [25], the US response to the Iraqi invasion of Kuwait during the Gulf War [4] and counterinsurgency tactics during the Vietnam War [24]. Wargaming has a long history as a tool for decision-makers to improve their critical thinking and inventiveness [20]. Wargaming is also a crucial step in the military decision-making process [10], which enables the construction and selection of effective COAs to achieve strategic, operational and tactical goals [8].

Today's warfare is marked by technological advances in information, communication, and artificial intelligence [5]. Thus, there is a growing demand for wargames that effectively incorporate

modern elements, i.e., specific effects, that can directly impact one's operational advantage. One such set of effects includes *cyber-effects*. While cyber-effects might be "invisible," they are as vital to victory in armed conflict as kinetic effects [17]. A cyber-effect denotes an attempt to breach the information systems of another person or organization to gain some advantage by executing unauthorized activities to disrupt, manipulate, or destroy opposition electronic systems, networks or data [1]. These effects come in many forms, e.g., phishing scams, ransomware or denial-of-service attacks, and can cause significant financial damage, as well as damage to reputation [18].

The complexity of cyber-wargames cannot be overstated. While the behavior of the air, sea, land, and space assets is well-known in most games, cyber-effects themselves are often abstract or misunderstood [15]. As a result, many decision-makers undermine rules to implement cyber-effects in a wargame [23]. For instance, players may use a cyber-effect at any time during a cyber-wargaming session, regardless of practical implementation. As a result, the gap between the actual operations and simulated games often diminishes the results generated by cyber-wargaming.

Examples of effective implementation of cyber-effects in wargaming include [14] and [2].

2.2 Wargaming Commodity Course of Action Automated Analysis Method

To reduce the time required to develop, analyze and compare COAs, [8] developed the Wargaming Commodity Course of Action Automated Analysis Method (WCCAAM). As our foundational model, WCCAAM sets the groundwork for the extensions included in this paper. In WCCAAM, a collection of different friendly units, identified as *commodities*, are utilized to confront enemy COAs. Various commodities are dispatched from multiple locations to nullify enemy targets, as set out by tactical and strategic objectives, while minimizing engagement risk to friendly forces.

WCCAAM relies on a multi-commodity flow algorithm (MCFA) to process the directed network, made up of nodes, i.e., bases and targets, and engagement paths; this network is derived from the mission analysis phase of the MDMP. The MCFA outputs the optimal flow of each commodity along each engagement path in the network. This output translates to an optimal COA for a commander to allocate resources to accomplish different objectives while minimizing operational risk. These objectives can be tactical, operational or strategic in nature, e.g., achieve air superiority or eliminate all enemy armor assets.

Formally, the mathematical formulation utilized by WCCAAM is

$$\min_{x} \sum_{(i,j)} \sum_{t} R_{tij} x_{tij} \tag{1a}$$

$$\text{subject to:} \sum_{j} x_{tij} \leq S_{it} \qquad \forall\, i \in N \tag{1b}$$

$$\sum_{i} x_{tij} \geq D_{jt} \qquad \forall\, j \in N \tag{1c}$$

$$x_{tij} \geq 0 \qquad \forall\, t \in T, i, j \in N \tag{1d}$$

where R_{tij} is the engagement risk associated with commodity t on engagement path (i, j), x_{ijt} is a decision variable related to the number of commodity t sent along path (i, j), S_{it} is the *supply* of commodity t available at node i, and D_{jt} is the *demand* for commodity t at node j. Demand, in this case, refers to enemy threats that must be nullified or objectives that require certain friendly assets to be achieved.

3 METHODOLOGY

In this section, we introduce C-WCCAAM, which includes decisions related to the implementation of cyber-effects. We first introduce relevant notation, then extend the formulation previously introduced in Section 2 to include cyber-effect decisions.

3.1 Notation

Relevant model decision variables and parameters are shown below.

Sets:

- T: set of friendly commodities with index $t \in T$
- N: set of nodes
- K: set $\{0, 1\}$ denoting non-use (0) and use (1) of cyber-effect.
- E: set of engagement paths (edges) from node i to node j with index set $(i, j) \in E$ where $i, j \in N$

Parameters:

- R_{tij}: engagement risk of commodity t sent from node i to satisfy demand at node j
- S_{ti}: number of commodity t that can be sent from node i
- D_{tj}: demand for commodity t at node j
- P : cyber budget
- C_{tij}: cost of using cyber-effects for commodity t when sent along engagement path (i, j)
- ϵ_{tij}: engagement risk-reduction factor for commodity t along engagement path (i, j); value between 0 to 1

Decision Variables:

- x_{tij0}: number of commodity t from friendly base i sent to nullify target j without the use of cyber-effects
- x_{tij1}: number of commodity t from friendly base i sent to nullify target j with the use of cyber-effects
- y_{tij}: equal to 1 when cyber-effect activated for commodity t when engaging target j from base i, 0 otherwise

Engagement risks are used to determine effective engagement paths for moving commodities to nullify targets. The higher R_{tij} for a given commodity-engagement path pair, the higher the potential operational risk.

The risk-reduction factor, ϵ_{tij} for commodity t on engagement path (i, j), defines the percentage of engagement-risk that can be eliminated through the use of a specific cyber-effect. The risk-reduction-factor, for example, can be used to measure the disruption, e.g., reduction in accuracy, of adversarial surface-to-air missile (SAM) systems, as a result of some offensive cyber action. The greater the risk-reduction factor, the greater the disruption to these systems.

3.2 Cyber-WCCAAM Formulation

To consider cyber decisions when determining the optimal friendly COA, we introduce a binary decision variable y_{tij} to the original

WCCAAM formulation in (1). The activation of y_{tij} comes with a reduction in engagement risk, ϵ_{tij}, along engagement path (i, j) for commodity t. We note that domains of indices are defined in Section 3.1.

In essence, we augment the original WCCAAM formulation in (1) with a slightly different objective function

$$\underbrace{\sum_t \sum_{(i,j)} R_{tij} x_{tij}(1 - \epsilon_{tij} y_{tij})}_{f_1} + \underbrace{\sum_t \sum_{(i,j)} C_{tij} y_{tij}}_{f_2}, \tag{2}$$

including an engagement risk term, f_1, and a cyber-effect cost term, f_2, which we aim to minimize, turning our problem into a multi-objective one. To reduce the problem back to a single objective, we can forgo the inclusion of f_2 in the objective function and instead add an additional cyber-budget constraint

$$\sum_t \sum_{(i,j)} C_{tij} y_{tij} \leq P, \tag{3}$$

thus adding a knapsack problem [19] to WCCAAM, with the objective to minimize engagement risk without exceeding a *cyber budget*, denoted as P. We note that in the context of multi-objective optimization, the addition of constraint (3) is called the ϵ-constrained approach [16]. This approach allows for the translation of a multi-objective function to a single-objective function. The ϵ-constrained approach is often used to determine Pareto-optimal solutions; this is in contrast to, say, a weighted multi-objective function.

Unfortunately, the introduction of cyber-effect decision variables into the objective function shown in (2) transforms the linear WCCAAM formulation into a nonlinear one, which can be time-consuming and impractical to solve within a high-dimension problem [9]. Thus, we linearize the formulation by constructing cyber decisions as alternating engagement paths, one associated with cyber reinforcement, engagement path $(i, j, 1)$, and one without reinforcement, engagement path $(i, j, 0)$. The decision variables x_{tij0} and x_{tij1} are then constrained to ensure that all of commodity t are sent across engagement path $(i, j, 1)$ if y_{tij} is equal to 1; otherwise, all of commodity t utilizing path (i, j) must be sent across $(i, j, 0)$.

With the inclusion of f_1 and (3), as well as the subsequent changes to make the formulation linear, the formulation for C-WCCAMM is

$$\min_{x,y} \sum_t \sum_{(i,j)} \sum_k R_{tijk} x_{tijk} \tag{4a}$$

$$\text{subject to: } \sum_j (x_{tij0} + x_{tij1}) \leq S_{ti} \quad \forall\, t \in T, i \in N \tag{4b}$$

$$\sum_i (x_{tij0} + x_{tij1}) \geq D_{tj} \quad \forall\, t \in T, j \in N \tag{4c}$$

$$\sum_t \sum_{(i,j)} C_{tij} y_{tij} \leq P \tag{4d}$$

$$x_{tij0} \leq M(1 - y_{tij}) \quad \forall\, t \in T, (i, j) \in E \tag{4e}$$

$$x_{tij1} \leq M y_{tij} \quad \forall\, t \in T, (i, j) \in E \tag{4f}$$

$$x_{tijk} \geq 0 \quad \forall\, t \in T, (i, j) \in E, k \in K \tag{4g}$$

$$y_{tij} \in \{0, 1\} \quad \forall\, t \in T, (i, j) \in E \tag{4h}$$

where R_{tij0} is the engagement risk without the use of cyber-effects across engagement path (i, j) and $R_{tij1} = R_{tij0}(1 - \epsilon_{tij})$ is the engagement risk with the use of cyber-effects across engagement path (i, j), all for commodity t.

Additionally, we constrain the total cost of cyber-effects with some cyber budget P using constraint (4d). An alternate constraint might instead constrain the number of cyber-effects used. For a simplified decision space, we can utilize the constraint

$$y_{tij} = y_{t'ij} \;\forall\, t, t' \in T, (i, j) \in E, \tag{5}$$

which ensures that any cyber-effect activated along path (i, j) is activated for all commodities. This constraint can be added for cyber-effects shared across commodities. We explore the addition of constraint (5) in later sections. Constraints (4e) and (4f) enforce the cyber-path restrictions, with M defined as a value large enough to prevent breaking said constraints.

3.3 Assumptions

In a real-world scenario, the success of a cyber-effect is often random [7]. The probability of a successful cyber-effect may be dependent on multiple factors, e.g., enemy cyber defenses. In many cases there is also a *probability of detection*, whereby to achieve a particular cyber-effect, a cyber-attack must also go undetected by enemy forces. For our purposes, we ignore this potential unpredictability. Examples of cyber-games utilizing these probabilistic approaches include [6] and [21], among others.

[22] extends WCCAAM itself to deal with uncertainties related to enemy force size. Weaknesses of disregarding the probabilistic aspect of cyber-effects in wargames in the context of denial and deception are described in [13]. We also require precise and reliable information related to engagement risk, enemy force structure and enemy action, as well as risk-reduction factors for cyber-effects. More specifically, we require that these model inputs be *known*.

4 APPLICATION TO OPERATIONAL SCENARIO

In this section we introduce a modified operational scenario. We then compare optimal COAs generated with WCCAAM and C-WCCAAM. To further explore these optimal COAs, we also provide sensitivity analysis for the C-WCCAAM results.

4.1 Scenario

For this work, we adjust a scenario previously used in [8] and introduced in [3]. The scenario concerns two civilizations, Phoenicia and Sumer, fighting against each other in a multi-domain conflict. In this section, we use the terms *friendly* and *enemy* interchangeably with Phoenicia and Sumer, respectively. We adjust the original scenario to include additional fighter, armor, and infantry units for Phoenicia and Sumer.

While (4) is a general formulation, we simplify the scenario at hand to include supply nodes and demand nodes. Phoenician bases (Striker Air Base (AB)), Camp Kipling and Pendem International Airpot (IAP)) have a fixed supply of various commodities, while Sumerian targets require a certain number of dedicated Phoenician commodities to be nullified. This scenario aims to allocate and

Table 1: Cyber-Effect Risk-Reduction Factors

		Mountain AB	Plains AB	Capital AB
Armor	Striker AB	0.60	0.33	0.40
	Camp Kipling	0.30	0.70	0.40
	Pendem IAP	0.40	0.20	0.40
Fighters	Striker AB	0.30	0.50	0.40
	Camp Kipling	0.30	1.00	0.40
	Pendem IAP	0.00	0.50	0.40
Infantry	Striker AB	0.60	0.20	0.83
	Camp Kipling	0.50	0.40	0.50
	Pendem IAP	0.67	0.20	0.20

assign friendly commodities to eliminate all enemy targets while optimally employing cyber-effects to minimize overall engagement risk.

For initial exploration of the scenario of interest, we utilize the pseudo-data shown Table 1. Cyber-effect costs are \$2K, \$3K and \$9K for armor, fighters and infantry, respectively. We include force structure in Table 2 and Table 3 for Phoenician and Sumerian forces, respectively.

Computational experiments were implemented using Python within the base version of Google Colabratory. We utilized the default CBC solver included in PuLP version 2.7.0.

Table 2: Phoenician Forces

Blue	Striker AB	Camp Kipling	Pendem IAP
Armor	5	20	0
Fighters	4	2	0
Infantry	280	20	150

Table 3: Sumerian Forces

Red	Mountain AB	Plains AB	Capital AB
Armor	10	15	0
Fighters	2	1	3
Infantry	100	50	300

4.2 Results

With the parameters stated earlier, we generate two COAs: one constructed with WCCAAM and the other with C-WCCAAM using a cyber budget of \$50K. These COAs are shown in Table 4.

The optimal solution with C-WCCAAM decreased engagement risk from 1,125 (using WCCAAM) to 777. While this decrease can be attributed to cyber-effect decisions, it is interesting to explore where decisions in optimal commodity flows differ from WCCAAM, as opposed to decreases in engagement risk due to the risk-reduction factors associated with cyber-effects alone. We can see slight differences between the two COAs, specifically in the deployment of infantry to counteract enemies.

With WCCAAM, the optimal COA satisfies the demand required by the Plains AB Infantry forces completely through infantry supplied by Striker AB, while C-WCCAAM satisfies this demand through the use of infantry at Striker AB and Camp Kipling. WCCAAM also uses infantry at all three bases to satisfy Capital AB Infantry demand, while C-WCCAAM consolidates by using forces from Striker AB and Pendem IAP. The optimal COA for C-WCCAAM selects cyber-effects for forces moving from Striker AB to Capital AB Infantry, resulting in additional infantry sent along this engagement path compared to the optimal WCCAAM COA. Thus, fewer infantry are available to be sent to Capital AB infantry from Striker AB, requiring Camp Kipling to send infantry.

Table 4: WCCAAM and C-WCCAAM Optimal COAs

WCCAAM	C-WCCAAM
Optimal Flow for Armor:	Optimal Flow for Armor:
Striker AB → Mountain AB: 5	Striker AB → Mountain AB: 5*
Camp Kipling → Mountain AB: 5	Camp Kipling → Mountain AB: 5*
Camp Kipling → Plains AB: 15	Camp Kipling → Plains AB: 15*
Optimal Flow for Fighters:	Optimal Flow for Fighters:
Striker AB → Plains AB: 1	Striker AB → Plains AB: 1
Striker AB → Capital AB: 3	Striker AB → Capital AB: 3*
Camp Kipling → Mountain AB: 2	Camp Kipling → Mountain AB: 2*
Optimal Flow for Infantry:	Optimal Flow for Infantry:
Striker AB → Mountain AB: 100	Striker AB → Mountain AB: 100*
Striker AB → Plains AB: 50	Striker AB → Plains AB: 30*
Striker AB → Capital AB: 130	Striker AB → Capital AB: 150*
Camp Kipling → Capital AB: 20	Camp Kipling → Plains AB: 20
Pendem IAP → Capital AB: 150	Pendem IAP → Capital AB: 150*
	*denotes use of cyber-effect
	Cyber Budget: \$50K
Total Engagement Risk: 1125	Total Engagement Risk: 777

4.3 Sensitivity Analysis

In this section, we utilize sensitivity analysis to assess the robustness of the C-WCCAAM COA shown in Table 4. Specifically, we perturb cyber budget, cyber-effect costs and engagement risk. Labels for engagement paths are shown in Table 5. We note that these path labels are the same for all friendly commodities.

Table 5: Scenario Engagement Path Labels

Path	Armor			Fighters			Infantry		
	Mountain	Plains	Capital	Mountain	Plains	Capital	Mountain	Plains	Capital
Striker AB	1	2	3	4	5	6	7	8	9
Camp Kipling	10	11	12	13	14	15	16	17	18
Pendem IAP	19	20	21	22	23	24	25	26	27

We first explore trade-offs between total COA engagement risk and cyber budget by varying the cyber budget P, the results of which are shown in Figure 1. Under a cyber budget constraint formulation, C-WCCAAM achieves greater cyber-effect selection stability at a lower cost of approximately \$65K.

Figure 1 shows the relationship between the overall engagement risk and cyber budget as P increases. The cyber budget intervals of constant engagement risk indicate regions that do not change the optimal objective function value; in rare cases, the same objective function value can result from different optimal solutions.

4.3.1 Location of Cyber-Effects vs. Cyber Budget. Cyber-effect locations may shift in response to a change in cost of executing a

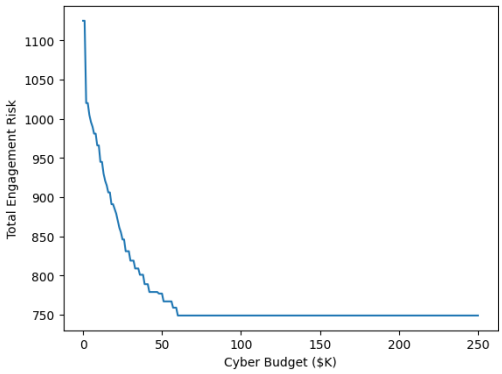

Figure 1: Total engagement risk with respect to cyber budget.

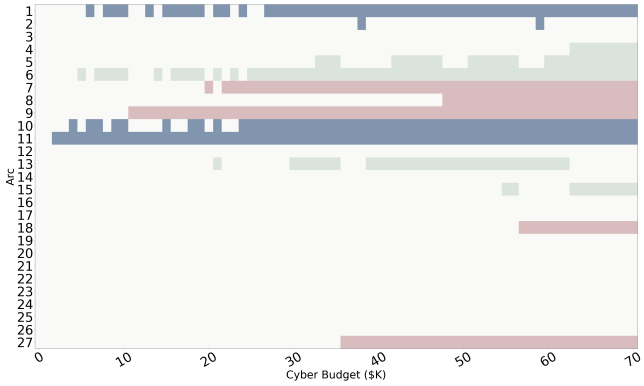

Figure 2: Location for cyber-effects with cyber budget of $1K-$70K for armor (blue), fighters (gray), and infantry (red).

cyber-attack in another location. Figure 2 shows on which paths cyber-effects are used as the cyber budget increases. We note that, based on Figure 2, changes to the cyber budget greatly affect the overall optimal solution, and, unlike the reduction of engagement risk on a single arc, does not result in predictable changes to said solution.

4.3.2 Location of Cyber-Effects vs. Cyber Risk-Reduction Factor. Figure 3 illustrates the changes in cyber-effect deployment location when there is a simultaneous adjustment in the engagement risk-reduction factor for infantry moving from Pendam IAP to engage infantry stationed at Mountain AB, Plain AB and Capital AB. With risk-reduction ranging from 0 to 16%, preference shifts towards applying cyber-effects at path 7, where infantry from Striker AB engage those at Mountain AB, and at path 27, which supports the infantry moving from Pendam IAP to confront forces at Capital AB, in conjunction with infantry from Striker AFB engaging the Capital AB infantry. Additionally, with a risk-reduction from 0% to 2%, there is an initiation of cyber-effects at path 8, deploying infantry from Striker AB to face off against those at Plains AB, rather than deploying from Pendam IAP. However, once the risk-reduction reaches 16% or higher, cyber-effects at paths 7, 8, and 27 are ceased, and reliance is placed solely on cyber-effects at paths

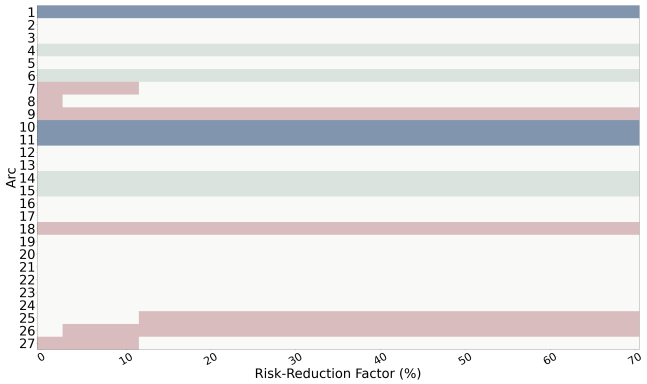

Figure 3: Location of cyber-effects vs. risk-reduction factor on paths 25, 26 and 27 simultaneously.

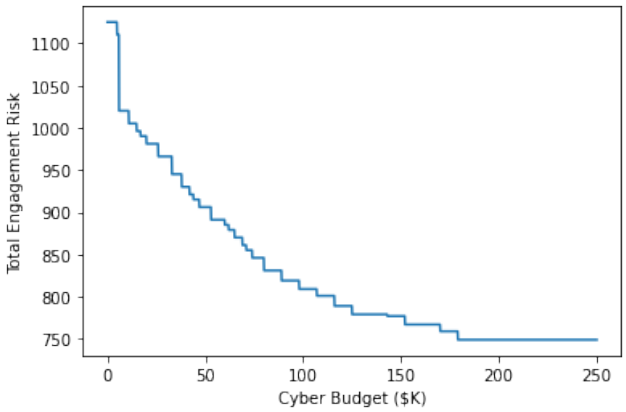

Figure 4: Total engagement risk with respect to cyber budget when utilizing constraint (5).

25 and 26, which involve deploying the majority of infantry from Pendam IAP against forces at Plain AB and Capital AB.

4.3.3 Results Using Constraint (5). In this section, we explore results when we enforce shared cyber-effects using constraint (5). We note that the use of constraint (5) allows for cyber-effects to be utilized on paths where no commodities are sent. However, the inclusion or exclusion of this constraint can vary based on my factors, e.g., decision-maker opinion, operational relevance.

Figure 4 shows the decrease in overall engagement risk as cyber budget increases; we reach a minimum engagement risk of 749 at a cyber budget of $179. Cyber-effects are not utilized until the cyber budget reaches $5K. This is due to the cost associated with enabling cyber-effects for each of the three commodities to satisfy constraint (5); we see the largest decrease in engagement risk as the cyber budget increases at $6K. A cyber-effect for Camp Kipling Armor to Plains AB Armor was utilized resulting in a 0.7 engagement risk-reduction factor along that engagement path.

Figure 5 shows how the costs of cyber-effects on blue fighters from Camp Kipling can affect where to implement other effects. When the cyber cost on path 13 is $3K or less, the cyber-effects

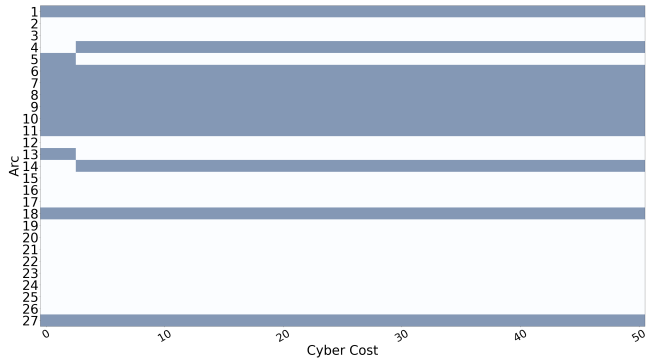

Figure 5: Location of cyber-effects vs. cyber-effect cost on path 13 when utilizing constraint (5)**.**

are launched at paths 5 and 13. When the cost exceeds $3K, the cyber-effects utilized previously at paths 5 and 13 switch to paths 4 and 14.

5 CONCLUSION

With the inclusion of cyber-effects, C-WCCAAM generates a comprehensive, quantitative approach for wargaming scenarios to facilitate effective cyber-effect decision-making. Moreover, C-WCCAAM provides a course of action for implementing cyber capabilities into military operations, ensuring that the use of cyber assets is optimized and aligned with other mission objectives.

Future work could weaken assumptions related to the certainties associated with our model parameters, e.g., engagement risk and cyber-effectiveness. Additionally, in our work, we assume enemy action is known. In future work, 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 C-WCCAAM application through open-source methods.

DISCLAIMER

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, United States Department of Defense, or United States Government.

REFERENCES

[1] 2022. What is A Cyberattack? https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
[2] Kimo Bumanglag, David Law, Adam Welle, and Peter Barrett. 2019. Constructing large scale cyber wargames. In *International conference on cyber warfare and security*. Academic Conferences International Limited, 653–X.
[3] Matthew B Caffrey. 2019. *On wargaming: How wargames have shaped history and how they may shape the future*. Vol. 43. Naval War College Press.
[4] Matthew Caffrey Jr. 2000. Toward a history-based doctrine for wargaming. *Air & Space Power Journal* 14, 3 (2000), 33.
[5] Gary Chapman. 2003. An introduction to the revolution in military affairs. In *XV Amaldi Conference on Problems in Global Security*. Citeseer, 1–21.
[6] Edward J Colbert, Alexander Kott, Lawrence III Knachel, and Daniel T Sullivan. 2017. *Modeling Cyber Physical War Gaming*. Technical Report. US Army Research Laboratory Aberdeen Proving Ground United States.
[7] John Curry and Nick Drage. 2018. Developments in state level cyber wargaming. In *Proceedings of the 11th International Conference on Security of Information and Networks*. 1–6.
[8] William T DeBerry, Richard Dill, Kenneth Hopkinson, Douglas D Hodson, and Michael Grimaila. 2021. The wargame commodity course of action automated analysis method. *The Journal of Defense Modeling and Simulation* (2021).
[9] F Delbos, T Feng, J Ch Gilbert, and D Sinoquet. 2008. Nonlinear optimization for reservoir characterization. In *ENGOPT International conference on engineering optimization, Rio de Janeiro, Brazil*.
[10] Department of the Army. 2019. *ADP 5-0 The OPERATIONS PROCESS*.
[11] David B Fox, Catherine D McCollum, Eric I Arnoth, and Darrell J Mak. 2018. *Cyber wargaming: Framework for enhancing cyber wargaming with realistic business context*. Technical Report. Mitre Corporation Homeland Security Systems Engineering and Developme Institute.
[12] Andrew Hanna. 2019. The Invisible US-Iran Cyber War. *The Iran Primer* (2019).
[13] Kristin E Heckman and Frank J Stech. 2015. Cyber counterdeception: How to detect denial & deception (D&D). In *Cyber Warfare*. Springer, 103–140.
[14] Kristin E Heckman, Michael J Walsh, Frank J Stech, Todd A O'boyle, Stephen R DiCato, and Audra F Herber. 2013. Active cyber defense with denial and deception: A cyber-wargame experiment. *computers & security* 37 (2013), 72–77.
[15] Nina Kollars. 2021. Pathologies of Obfuscation.
[16] Kaisa Miettinen. 2012. *Nonlinear multiobjective optimization*. Vol. 12. Springer Science & Business Media.
[17] Vikram Mittal and Andrew Davidson. 2020. Combining wargaming with modeling and simulation to project future military technology requirements. *IEEE Transactions on Engineering Management* 68, 4 (2020), 1195–1207.
[18] Seattle Office of Emergency Management. 2023. Cyber Attack and Disruption. https://seattle.gov/documents/departments/emergency/plansoem/shiva/shivav7.0-cyber.pdf
[19] Harvey M Salkin and Cornelis A De Kluyver. 1975. The knapsack problem: a survey. *Naval Research Logistics Quarterly* 22, 1 (1975), 127–144.
[20] Jeremy Sepinsky, Eric Heubel, and Matthew Cumpian. 2019. Gaming Cyber in an Operational-Level Wargame: Merlin Cyber Wargame Module Rules for Adjudicators. (2019).
[21] Abderrahmane Sokri. [n.d.]. Cyber Deterrence: A Wargaming Approach. ([n. d.]).
[22] Alexander Stephens, Richard Dill, Chancellor Johnstone, and Douglas D. Hodson. 2023. The Wargame Commodity Course of Action Automated Analysis Method Under Uncertainty.
[23] Bibi van den Berg and Sanneke Kuipers. 2022. Vulnerabilities and cyberspace: A new kind of crises. *Oxford Research Encyclopedia of Politics* (2022). https://doi.org/10.1093/acrefore/9780190228637.013.1604
[24] Natalia Wojtowicz. 2019. From sandboxes to laboratories: evolution of wargaming into a method for experimental studies. *International Journal of Scientific and Research Publications* 9, 12 (2019), 399.
[25] Robert Work and Paul Selva. 2015. Revitalizing wargaming is necessary to be prepared for future wars. *War on the Rocks* 8 (2015).