A Game Theory for Resource-Constrained Tactical Cyber Operations

Jonathan Goohs
U.S. Navy
Maryland, USA
jagoohs@radium.ncsc.mil

Josiah Dykstra
Trail of Bits
New York, USA
josiah.dykstra@trailofbits.com

Anthony Melaragno
United States Naval Academy
Annapolis, USA
melaragn@usna.edu

William Casey
United States Naval Academy
Annapolis, USA
wcasey@usna.edu

***Abstract*—Given the ever-increasing landscape of cyberspace, the battlespace grows at a disproportionate rate to the given tactical resources armed with proper expertise given a finite time span. Tactical cyber operations are acts to defend friendly cyber-terrain with respect to denying the ability for the adversary to conduct operations or degrading their capability to do such acts. We examine how decision makers can optimize such operations under resource constraints to best answer strategic imperatives. This study uses game theory to evaluate scenarios for completing tactical cyber operations given different resource constraints—namely time, expertise, and capabilities—to reach the outcome of a given operation. The problem displayed weighs allocation of finite resources against a vulnerability status of the opposing computer network, and articulates whether an extra percentage of time can expand the operational outcome. We recommend key decisions makers who are in a position to maneuver tactical cyber operations use game theory to inform a data-driven decision calculus that is optimal to meet their strategic imperatives. Future research discussions may include how to help decision makers maneuver intelligence and offensive operations in cyberspace.**

***Index Terms*—Game Theory, Cyber Operations, Resource Constraints**

I. Introduction

The extensive range and increasing depth of vulnerabilities throughout cyberspace indicate that limited resources emerge as a key factor driving the importance of cost-effective tactical cyber operations. Given the complexity of cyberspace, there exists a need for a guide for resource allocation to inform key decision makers in strategic positions to maximize tactical, operational, and strategic outcomes [1]. When applying resources with respect to tactical cyber operations, many factors must be considered: integrity of supply chain for infrastructure, personnel to configure/monitor/maintain infrastructure, time for planning, configuring, and enabling cyber operations with the skilled personnel to lead teams, and arguably most the vital, the time and cost of a cyber operator. Within the scope of this paper, we define tactical cyber operations as missions executed to defend a country's network infrastructure, or other cyberspace a country's cyberspace forces have been ordered to defend, from active threats [2]. The goal is to deny an adversary from continuing to infiltrate friendly networks or disrupt/degrade their ability/capability to do so. We do acknowledge, however, that there exist both independent and conditions-based offensive and intelligence cyber operations that exist external to the scope of the paper that feed a strategic outcome for key decision makers. In this work, we focus explicitly on time as the constrained resource and set aside the limited resource of *expertise* for future work. Given the worldwide scope of cyber operations, time constraints extend beyond the traditional 40-hour work week, expanding on the requirement to have personnel staged to support and enable the cyber operator at a near-continuous operational tempo.

This expansion of denominator to apply resources only increases the complexity of problem set as it relates to efficiently scoping how to employ cyber operations to drive maximum operational outcomes, that does not deteriorate the cyber operator with respect to their technical performance and willingness to continue to support the organization in the long term. Plainly stated, tactical cyber operations are stressful to the people doing them [3]. We believe that the theory applications in this paper will achieve a model for operational cyber forces to employ resources in the most cost-effective manner to achieve tactical outcomes, which serve operational and strategic goals. One point which will not be fully analyzed here, but has significant relevance to the problem set, is that there must be some resources applied to preparing a higher leverage capability for one time delivery and maximum impact on the tactical scale, on a not to exceed basis with the expiration of applicability on the target.

Clear identification the a team's goal(s) is incredibly important when optimizing tactical cyber operations. A red team may optimize for the discovery (and patching) of vulnerabilities without regard for stealth. An intelligence team may optimize for stealth and information gathering even at to sacrifice burnout. Optimizing for the wrong performance measurements can be catastrophic [4].

In this paper, we consider scenarios on the cyberspace battlefield wherein we optimize the use of forces in time in an efficient matter in the pursuit of successful cyber operations. We are inspired by anecdotal questions that a decision maker may ask in practice: When do I stop or surge operations? What could we accomplish with more time or resources?

We show how decision makers can apply game theory to tactical decisions when resources are limited, including providing related work, modeling scope, application of model, and analysis of use cases.

II. Related Work

Operational Decision-Making for Cyber Operations [5] explains the complexity of decision-making paradigms within conducting reconnaissance and then later the destructive cyberattack, but does not address the application of resource alignment for competing forces as we walk towards an impetus of terrain control. Addressing resource alignment, we offer key insights for decision-making against the spectrum of risk decisions in deploying cyber capabilities. A 2017 paper on a theoretical model for cyber-warfare games details that players in a game for cyber operations can either detect an attack, receive disclosure from other players, or discover the vulnerability by themselves and apply a patch [6]. This work did not consider the potential availability, cost, and value of additional time given the bounds of a fixed-length CTF game without elasticity; their goal (like military operations) was to win the game. We believe the game posited provides a rather accurate scope for how organizations less concerned with monetary cost address zero-days, and can inform decision makers on how to approach a target network based on where a defender is most likely to spend their majority of resources. Other research detailed chaff-aided obfuscation in resource-constrained environments discusses how time an adversary spends attempting to eavesdrop on their target's network may be outweighed by the effort of the network defender to build a bolstered defense through obfuscation [7]. This paper covers the relationship between expending resources but does not address how a decision maker should reposition their resources to overcome the adversary's allocation decision.

"Colonel Blotto" is a game in which two commanding officers have finite resources to apply over multiple battlefields simultaneously, wherein the battlefields they are fighting on have equal value. In this game, one major issue arises: the battlefield of cyberspace is ever expanding [8]. In the game, Colonel Blotto is assumed to be the better resourced officer, coming out on top given the equal battlespace to fight in. However, as the battlefield expands, the Colonel Blotto game teaches us that at a certain battlefield size, there develops numerous optimal strategies to win. In cyber operations, you may be planning towards an outcome and applying optimal strategies to deter the threat at hand or incite your intended effects on a target, whilst your target is doing the same to you in an equally optimal fashion in a divesting vector you have yet to discover and/or apply resources towards. When limited by resources, which applies to every cyber operation, effective planning against the adversary to drive strategic goals for the cyber operation's outcomes is imperative. Specifically, finding data to understand how the adversary or opposing force is most likely to strike your organization is the most effective way to allocate resources into a certain portion of the cyber battlefield. Even when you have focused on a certain type of tactics, techniques, and procedures (TTP) by a given adversary, the defensive cyber operation applied may not be able to address the given problem set due to speed of the TTP, outdated intelligence to inform the cyber operation, or precise understanding of the operational environment the cyber operation is being performed in. There are resource optimization problems in many fields, from project management to sporting competitions to training large language models. However, tactical cyber operations stand out due to their adversarial nature, technical depth, pronounced uncertainty, and the need for real-time adaptability and stealth. This combination of factors creates a uniquely challenging and dynamic problem space compared with competitive sports and other time-constrained tasks.

Due to the complexity and classification of cyber operations, it is oftentimes difficult for strategic leaders to understand how impactful the tactical effects of an operation can effect the strategic landscape [9]. In this paper detailing the adversarial knapsack [10] , the lack of realistic cyber operations data is exemplified, where data is created by using undergraduate students to emulate decision making in cyberspace through a capture the flag (CTF) style game. One important facet that this paper takes into account from [9] is that U.S. DoD Cyber Strategy from 2023 details a method of persistent engagement to defend forward in cyberspace. This strategic resource allocation perpetuates our game theory structure under some constraints, in comparison to a strategy that may hold back resources for operations for conditioned-based striking. One major gap this paper exhibits is having up-to-date means of understanding how proper resource allocation for tactical cyber operations will provide decision makers with the ability to escalate given a conflict scenario arises [11]. Additionally, a gap that exists in this paper's analysis is the ability to predict the timing and tempo for employment of capabilities (which take most times extreme investment of resources). This employment of capabilities across the matrix of resource allocation is a complicating factor, depending on the organization's strategic imperatives and decision calculus for operations, something this paper does not cover given the variance. Another related work highlights additional impetus of this research subject, while presenting a problematic limitation of live data from tactical cyber operations due to classification [9]. This gap in data of cyber operations into the public sphere only creates a larger inability for academia to make relevant hypothesis and conduct experiments with a low barrier for entry. We aim in this paper to do what the majority of cyberspace decision making research do not, use game theory and tactical experience to guide a math-based decision calculus towards informing key decision makers striving their organization towards strategic end-state through tactical operations in cyberspace.

III. Meso-Scale Formalism

A. Micro, Meso, and Macro Operation Optimization

The model should incorporate more dynamic elements to reflect the true complexity of cyber operations. In tactical and strategic planning there are three levels of granularity in decision making: micro-, meso-, and macro-level operations [12]. Micro-level tactical cyber operations are those achieved by an individual or small team towards a single objective. For

instance, the operation may be one to identify whether a target network contains any weak passwords. Individual operators and their teams make most decisions and seek to locally maximize their own resources. As we will see in the following Section, MITRE ATT&CK and D3FEND frameworks can be used by an operator to make their own resource decisions. This can also be considered a single weighted knapsack problem or its derivatives including adversarial knapsack and dueling knapsack. Micro-level tactical decisions are constrained by time, skill, and capabilities. For example, there is limited time before the operators become fatigued and performance decays. Depending on the operational goals, there may also be temporal constraints on whether the operators see the attack or attacker in progress, whether there are fleeting opportunities (such as a target device being online and accessible), and when bugs are created or patched.

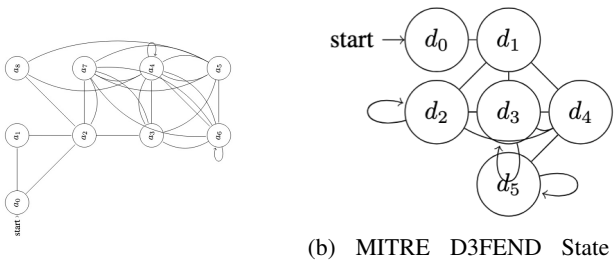
Meso-level operations are the aggregation of capability that can be conducted by teams of teams for a collective objective such as the protection of election integrity. Leaders at this level must consider the use of resources for multiple micro-level operations. They may, for instance, have the ability and need to consider operational surges and to weigh the costs and value of doing so. Figures 1(a) and 1(b) represent meso-level operations.

The macro-level considers the total capacity of an organization and could contain hundreds or thousands of operators contributing to multiple strategic objectives. Colonel Blotto exemplifies the game theory for decision makers at this level.

Cyber operations range in complexity and have complex dependency structures with critically differential values depending on which achievements are attained and in which order. To model these important dependencies and intermediate stages we consider a variety of formal methods aimed at developing the required decision making at the Meso-Scale for operations. Our primary tool will be discrete state and temporal transitional logic informed by attack and defense taxonomies.

B. State Transition and Temporal Logic

According to [13], the ability to attack and defend a system was characterized by a single Markov chain attack graph and defense graph. We use the MITRE ATT&CK framework [14] to provide a comparison mechanism. There are distinct points of time where increasing attack, defense and development resources could contribute to a decision makers calculus to employ resources. Each state transition during the attack process as illustrated in Table I can lead to an increased likelihood of detection. Transitioning from one state to the next has direct correlation to volume and allocated resources as shown in Table I. Conversely MITRE has also developed a D3FEND framework [15]. The D3FEND frame shown in Table I illustrates plausible states that can be used to detect and counter a attack. Countering an incursion into a system becomes resource intensive at states d1-d5 as shown in Table II.



(a) MITRE ATT&CK Automata which can be considered a meso-level operation.

(b) MITRE D3FEND State Transition Automata which can be thought as a meso-level operation.

Fig. 1: Attack and defense activities as transitions automata, enable various analysis, including Bayesian probability.

Correlating Table I and Table II we note that the states within Table II and subsequent Figure 1(b) can be embodied in Table II d1-d4. The entirety of the offensive strategy is to bypass defensive states d1-d4. Cyber operations is a combination of automated and manual operations. We identify the development of exploits in state a1 as a more manually intensive process.

TABLE I: Offensive State Attack State Transition

State	State Name	Team Volume	Time Const	Next State
a0	Reconnaissance	Low	No	a1, a2
a1	Resource Development	High	Yes	a2
a2	Initial Access	Low / Medium	Yes	a3, a7
a3	Execution	Low / Medium	Yes	a4
a4	Persistence	Low	No	a3-a6, a8
a5	Privilege Escalation	Low / Medium	Yes	a3, a4, a6-a8
a6	Defense Evasion	Low / Medium	Yes	a3-a6, a7
a7	Credential Access	Low / Medium	No	a2-a6
a8	Discovery	Low	No	a0, a8

IV. Essential Game

Traditionally, decision theory concerning the prioritization and scheduling of limited resources has a long and rich history. Operations research, linear programming, quadratic programming are but a few fields which have addressed these problems. In military conflict scenarios, Colonel Blotto is an example game theory which address the decisions of how resources can best be allocated to k individual battle fields. The scenario in cyber is related although has its own particularities owing to the aspects of non-physicality and action remotely.

TABLE II: D3FEND State Attack State Transition

State	State Name	Team Volume	Time Constrained	Next State
d0	Harden	Low	Yes	d1
d1	Detect	Low / Medium	No	d2,d3,d4
d2	Isolate	High	Yes	d2,d3,d4
d3	Deceive	High	Yes	d2,d3,d4
d4	Evict	High	Yes	d5
d5	Restore	Medium/High	Yes	d5

Not withstanding these issues that entail differing laws of scale for resource allocation, cyber operational planners, regardless have essential resource limitations, where mission attainment is best viewed as constrained optimization over those limited resources. A complete game theory for both offensive and defensive cyber operations is provided in [10]. Here we review the core notion of reducing operational decisions (prioritization and planning) to an instance of *The Weighted Knapsack Problem*.

A. Knapsack reduction

Let N be the count of a fixed set of subjects that can alter the game state of two sides, a defender could act to secure subject j while an attacker could act to compromise subject j. We will assume that the attacker and defender have a common understanding or assessment of hazard scores as: $H = \{h_1, h_2, \ldots, h_N\}$, however and unlike the entirely physical *Colonel Blotto Game* within the realm of cyber-systems, uncertainty to the actual state of each subject is possible. Uncertainties or stealth attack are modeled with *Flip-It game*, and those model extensions, not needed here, are found in [10].

Strategies describe agent choices of actions (as a schedule in time index k). Let

$$\phi^x_{ik} = \begin{cases} 1 \text{ if subject } i \text{ is acted on by } x \text{ at time } k \\ 0 \text{ otherwise .} \end{cases}$$

The cost and value for acting on item i is defined as: c^x_j is the cost for x to operate on subject j, and v^x_j is the value to x operating on subject j. Over a time period P, agent x attempts to maximize:

$$\Phi^x = \sum_{k \in P} \sum_{j=1}^{N} \phi^x_{jk} v^x_j \qquad \text{(Objective)}$$

subject to the constraint, limiting number of actions:

$$\sum_{k \in P} \sum_{j=1}^{N} \phi^x_{jk} c^x_j \leq C^x_P \qquad \text{(Constraint)}$$

The constrained optimization problem above can work in opposition or adversarial ways for two agents x, y having a direct conflict of interest, such as when x is the attacker and y is the defender (see [10] for details).

The problem of optimizing equation (Objective) subject to constraint (Constraint), is nothing more than an instance of *the Weighted Knapsack Problem*. The Weighted Knapsack problem is heuristically solvable in efficient time by use of binary programming for most realistic settings. The unbounded weighted knapsack is known to be an NP-complete problem in general; however, this is not the case for us given our relatively low constraints which impose choices of what actions are required.

B. When are efforts surges useful?

An *effort surge*, can be thought of as slight modulation upward of one's capacity in order to achieve a real or perceived high-value target. Similarly, *an effort back-off* can be thought of as a slight modulation downward of the capacity. The simplest study considers two players x, y, their dual objectives Φ^x, Φ^y, and then considers two parameter scenarios, only differing slightly in the input effort that one player (say player x) can apply. This would lead to two specific parameter regimes, P and P_x that can be thought of as a baseline and a surge effort by player x, as they differ only by some additional level of input (β) that player x applies. We assume that modulations are within an *elastic range*, for example, $\beta = 0.15$, which corresponds to asking a team for 15% extra effort. Note that extreme surge efforts can induce inelastic effects such as loss of critical members, team impairment, or destruction; however, inelastic range situations fall outside the scope of our current study.

The primary question asked here is, when does an effort surge make sense? And what if players implement a range of strategies from oblivious to strategic (i.e., by implementing heuristic solutions to weighted knapsack)?

To address this question we consider a problem parameters as:

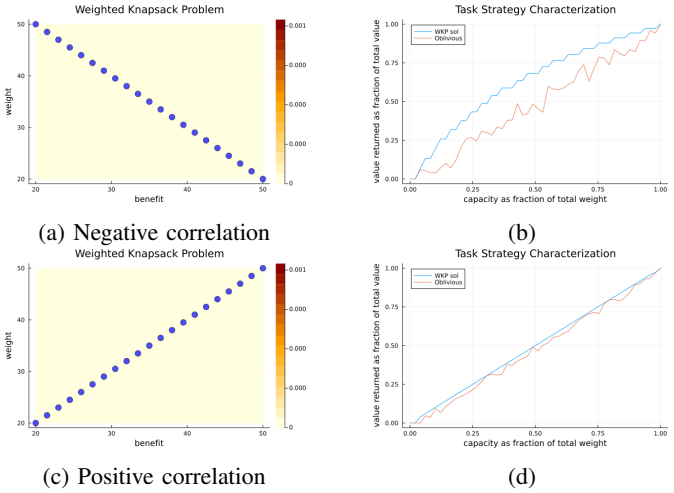
$$P = \langle \bar{h}, \bar{c}, \bar{v}, (C^x, C^y) \rangle, P_x = \langle \bar{h}, \bar{c}, \bar{v}, ((1+\beta)C^x, C^y) \rangle$$

Letting β be an elastic parameter (eg. $\beta \approx 0.15$), we consider the following variants of P

V. Simulating the Macro Model

To address the question of when effort surges are useful we consider the marginal returns in value that additional resources can secure. To explore this, we construct WKP with three different types of cost/value distributions and perform computational optimization for planning. Interestingly, our simulation studies indicate that not only qualitative answers are possible, but also the close connection between the joint distribution of (value, cost) for tactical options (plotted as points in the value $\times$ cost plane) and the convexity of the returned value function. Additionally, when assumptions that measurements are accurate, our WKP solver [10] can calculate quantitative answers to this as well.

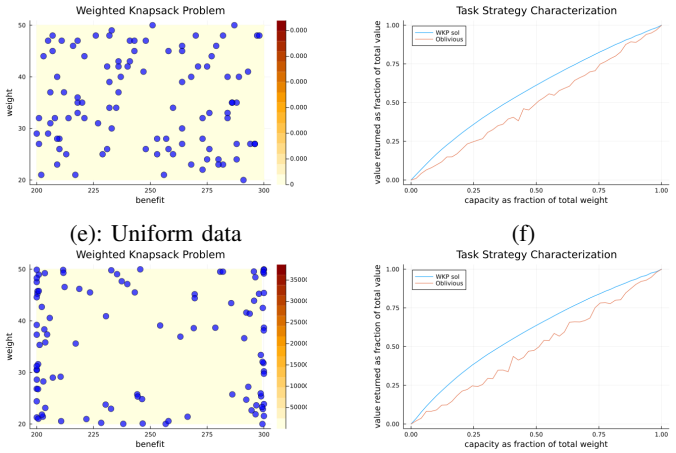
In Figure 2, 3, and 4, the central question, which addresses the different value returned outcomes for P vs P_x, can be seen by considering two capacities (points on the x-axis) and their corresponding value returned plotted within the Task Strategy Characterization Graphs. Since we are interested in characterizing the efficient use of resources, we consider solutions to WKP and compare them to random (or oblivious) tasking strategies. In Figure 2 we show the value-return dependency of the distribution of tactical options in the value $\times$ cost plane. Staring with linear relationships between cost and value, we note that the value return of strategic planning with negative slope is pretty good compared to oblivious selection. This can be seen with the separation between the two value curves. Interestingly for strategic planning the value returned



(a) Negative correlation (b)

(c) Positive correlation (d)

Fig. 2: *Strategic Planning Efficacy depends on the distribution (value, cost) pairs for various tasks.* Above we demonstrate several potential distributions for tasks with regards to their benefit/cost values. In (a) we consider negative correlation between cost and value, in (b) we analyze strategic planning by solving WKP with binary programming (blue) vs random/oblivious planning. In this case the separation of curves indicates that strategic planning enable planners do better than random planning. In (c) we consider positively correlated cost and value, surprisingly in (d) little difference between strategic and oblivious planning is observed.



(e): Uniform data (f)

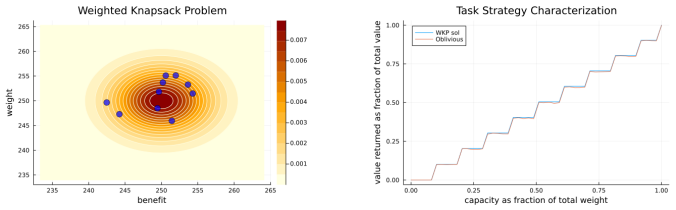
(g): product of beta (h)

Fig. 3: *Strategic Planning Efficacy with random and beta distributions (value, cost) pairs for various tasks.* In (e) we consider uniform distribution between cost and value, in (f) we analyze strategic planning by solving WKP with binary programming (blue) vs random/oblivious planning. In (g) we consider cost and value as a product of beta$(0.5, 0.5)$ distributions thereby concentrating tasks into four categories (low cost, low value), (low cost, high value), (high cost, high value), and (high cost, low value), unsurprisingly in (h) strategic planning outperforms oblivious planning.

in P_x compared to P is diminishing, this is because WKP in general selects best values first. In (c) a positive sloped relation between benefit and cost yields a less intuitive result. First of all there appears to be meager advantage to strategic planning compared to oblivious planning as both generally provide linear returned value in the cost of operations. As a result the marginal gain from additional resourcing is a linear response and thereby better than the diminishing returns found for strategic planning found in (b) for distribution of tactical options found in (a).

With simple linear examples exhausted we consider more realistic examples. In Figure 3 we consider uniform random distribution of tactical options in the value $\times$ cost plane, noting again the improvements which strategic planning can offer. Again a law of diminishing returns will apply to P_x vs P. The situation is amplified in (g) a distribution which is the product of beta$(0.5, 0.5)$ distributions. This distribution concentrates options to the four corners, thereby rendering four main types of tasks: (low value, low cost), (high value, high cost), (high value, high cost), and (low value, high cost).

Finally, when tactical options are distributed as a multivariate normal distribution in the value $\times$ cost plane. In Figure 4 we plot such a distribution in (i) and demonstrate in (j). Note the close resemblance to returned value to the case when options have positively correlation (see Figure 2(c)). In this case the value returned by strategic planning is only slightly better than random planning, as such we have a return to P_x yielding a linear proportional value improvement (proportional to $beta$) for both oblivious and strategic planning.



(i): Multi-Variate data (j)

Fig. 4: *Strategic Planning Efficacy with Multivariate Normal distributions for (value, cost) pairs for various tasks.* In (i) we consider Multi-Variate Normal distribution between cost and value, in (j) we analyze strategic planning by solving WKP with binary programming (blue) vs random/oblivious planning. Surprisingly we determine meager advantage for strategic planning over oblivious planning.

Summary: Our simulations highlight the importance of the distribution of tactical options in the value $\times$ cost plane. In so far as what to expect from effort surges when various planning optimization is active, we can conclude that returned value will depend on the distribution of options. Further our simulations indicate that a qualitatively the answer will depend on a mathematical relation between distribution of options and the curvature of strategic optimized value return curve. Moreover when (value, cost) estimations can be assumed accurate the algorithmic methods, solving WKP and simulation can be utilized for more qualitative solutions.

A. Analysis and Discussion

Computational solution yields various answers: What more do you get if you ask 15% more inputs, What less do

you get if you ask 15% less. Sometimes, for example when cost and benefits are negatively correlated, is maybe worth it, however note the marginal declining value, other times for example when cost and benefit are tightly correlated it maybe not. Critically, the assumptions hinge on accurate measures of notions such as: threat, hazard, etc. ... rejoin any open discussions of how U.S. forces handle these notions vis-a-vis other Nation states. If a tactical cyber operator gets one more hour, the operator may be able to deny/degrade the ability for one CVE an adversary uses. Depending on the adversary, the operator may be able to cut down a large percentage of their resource allocation.

VI. Conclusion

We have shown that there is a tipping point for return on investment for tactical cyber operations. While we provide insights into resource-constrained tactical cyber operations, a limitation is the lack of empirical data on the frequency of suboptimal time-based decisions made by leaders today. This gap in knowledge hinders the ability to fully validate our theoretical models and assumptions. However, our first-hand experiences provide anecdotal support for such sub-optimization. Future research should prioritize the gathering of real-world data to better understand decision-making processes and improve the practical applicability of our findings. Our analysis acknowledges that one potential solution to mitigate time constraints is to hire additional personnel. However, it is crucial to base such decisions on empirical data to determine whether this approach is indeed optimal. Moreover, not every aspect of cyber operations is limited by the size of the workforce but also the time available for machines to perform pre-operation planning and real-time automation.

We discussed resources and state transitions and its intersection. We believe we can extend the state transition diagrams to micro, meso, and macro scales. Each of the state transitions have a specific probability and cost for the transitions and are encapsulated within its own scale. In addition, we also believe specific to the scale and transitions there is game theory that can be played. We recommend that key decision makers receive training game theory beyond basic decision calculus to help them optimize resource allocation. The development of malicious software will likely evolve over time with the advent of AI technologies integrated into the software development process [16]–[18]. Additionally, as a counter to aid in defense, AI will be influencing the defense process [19].

The movement from one state to another in performing a cyber operations is opportunistic from an adversary and perceived random from the defender. In either cases the discovery, realization and exploitation of vulnerabilities is a game that both the attacker and defender play as shown in figure 1(a) and figure 1(b). Since not all vulnerabilities are known when they are uncovered and exploited there is a stochastic feeling about it. In the future this can be modeled as a stochastic process. The probabilities can be linked to likelihood probabilities and therefore linked to Risk Assessment [20]. In future work we propose Markovian Bayesian probabilities as a game interlinked with therisk assessment would allow decision makers to ascertain risk to there systems while conducting or defending against an attack [21].

References

[1] M. Smeets, "The strategic promise of offensive cyber operations," *Strategic Studies Quarterly*, vol. 12, no. 3, pp. 90–113, 2018.

[2] Chairman of the Joint Chiefs of Staff, "JP 3-12, Joint Cyberspace Operations," 2022.

[3] C. L. Paul and J. Dykstra, "Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations," *Journal of Information Warfare*, vol. 16, no. 2, pp. 1–11, 2017.

[4] T. of Bits, "How we fared in the cyber grand challenge," https://blog.trailofbits.com/ 2015/07/15/how-we-fared-in-the-cyber-grand-challenge/ , 2015, accessed: 2024-06-07.

[5] M. Smeets and J. Work, "Operational decision-making for cyber operations," *The Cyber Defense Review*, vol. 5, no. 1, pp. 95–114, 2020.

[6] T. Bao, Y. Shoshitaishvili, R. Wang, C. Kruegel, G. Vigna, and D. Brumley, "How shall we play a game?: A game-theoretical model for cyber-warfare games," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*. IEEE, 2017, pp. 7–21.

[7] E. N. Ciftcioglu, R. L. Hardy, L. M. Scott, and K. S. Chan, "Efficient chaff-aided obfuscation in resource constrained environments," in *IEEE Military Communications Conference (MILCOM)*. IEEE, 2017, pp. 97–102.

[8] O. Gross and R. Wagner, "A continuous colonel blotto game," Rand Project Air Force Santa Monica Ca, Tech. Rep., 1950.

[9] S. Hamman, J. Mewhirter, R. Harknett, J. Vicic, and P. White, "Deciphering cyber operations: The use of methods and simulations for studying military strategic concepts in cyberspace," *The Cyber Defense Review*, vol. 5, no. 1, pp. 135–152, 2020.

[10] J. Goohs, G. Savin, L. Starks, J. Dykstra, and W. Casey, "Adversarial knapsack and secondary effects of common information for cyber operations," arXiv Preprint, 2024, arXiv:2403.10789

[11] E. Borghard and S. Lonergan, "Cyber operations as imperfect tools of escalation," *Strategic Studies Quarterly*, vol. 13, no. 3, pp. 122–45, 2019.

[12] C. Vlados and D. Chatzinikolaou, "Macro, meso, and micro policies for strengthening entrepreneurship: Towards an integrated competitiveness policy," *Journal of Business & Economic Policy*, vol. 7, no. 1, pp. 1–12, 2020.

[13] A. V. Outkin, P. V. Schulz, T. Schulz, T. D. Tarman, and A. Pinar, "Defender policy evaluation and resource allocation with MITRE ATT&CK evaluations data," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[14] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "MITRE ATT&CK: Design and Philosophy," in *Technical report*. The MITRE Corporation, 2018.

[15] MITRE, "MITRE D3FEND," https://d3fend.mitre.org/, 2023, accessed: 2024-06-07.

[16] T. F. Blauth, O. J. Gstrein, and A. Zwitter, "Artificial intelligence crime: An overview of malicious use and abuse of ai," *Ieee Access*, vol. 10, pp. 77 110–77 122, 2022.

[17] V. Ubavić, M. Jovanović-Milenković, O. Popović, and M. Boranijašević, "The use of the chatgpt language model in the creation of malicious programs," *BizInfo (Blace) Journal of Economics, Management and Informatics*, vol. 14, no. 2, pp. 127–136, 2023.

[18] Y. M. Pa Pa, S. Tanizaki, T. Kou, M. Van Eeten, K. Yoshioka, and T. Matsumoto, "An attacker's dream? exploring the capabilities of chatgpt for developing malware," in *Proceedings of the 16th Cyber Security Experimentation and Test Workshop*, 2023, pp. 10–18.

[19] M. Charfeddine, H. M. Kammoun, B. Hamdaoui, and M. Guizani, "Chatgpt's security risks and benefits: Offensive and defensive use-cases, mitigation measures, and future implications," *IEEE Access*, vol. 12, pp. 30 263–30 310, 2024.

[20] K. Tam and K. Jones, "Macra: a model-based framework for maritime cyber-risk assessment," *WMU Journal of Maritime Affairs*, vol. 18, pp. 129–163, 2019.

[21] N. Leveson, "Stpa (system-theoretic process analysis) compliance with mil-std-882e and other army safety standards," *Online URL: http://sunnyday. mit. edu/compliance-with-882. pdf*, 2016.