Received: 10 October 2022 | Revised: 30 January 2023 | Accepted: 11 March 2023 | Published on: 29 March 2023

DOI: 10.1002/nav.22106

RESEARCH ARTICLE

WILEY

Resource allocation in two-layered cyber-defense

Michael P. Atkinson | Moshe Kress

Operations Research Department, Naval Postgraduate School, Monterey, California, USA

Correspondence
Michael P. Atkinson, Operations Research Department, Naval Postgraduate School, Monterey, CA, USA.
Email: mpatkins@nps.edu

Abstract

A common network security approach is to create a De-Militarized Zone (DMZ) comprising two layers of network defense. The DMZ structure provides an extra layer of security between the sensitive information in a network (e.g., research and development files) and the component of the network that must interface with the general internet (e.g., the mail server). We consider a cyber-attack on a DMZ network where both attacker and defender have limited resources and capabilities to attack and defend, respectively. We study two optimization problems and one game-theoretic problem. Given that the attacker (defender) knows the potential capabilities of the defender (attacker) in the two layers, we obtain the optimal allocation of resources for the attacker (defender). The two-optimization problems are not symmetrical. Absent any knowledge regarding the allocation of the adversary's resources, we solve a game-theoretic problem and obtain some operational insights regarding the effect of combat (e.g., cyber) capabilities and their optimal allocation.

KEYWORDS

allocation game, cyber, de-militarized zone, stochastic duel

1 | INTRODUCTION

Layered defense is a key concept in computer networks defense (IBM, 2023). Specifically, a common network security approach is to utilize a De-Militarized Zone (DMZ) structure (Dadheech et al., 2018; Rababah et al., 2018), which generates two layers of network defense. The DMZ itself consists of the portions of the enterprise network between the internet and the enterprise's intranet (Dadheech et al., 2018). The intranet contains sensitive files such as personal information, financial records, and research and development plans. The DMZ contains the parts of the network that must interface with the internet (e.g., mail server). We focus on the two defensive layers of the DMZ that border the DMZ – the outer layer facing the internet, and the inner layer facing the intranet. A cyber-attacker, attempting to penetrate a computer network of the enterprise and access its intranet, needs to successfully breach these two layers of defense, without being detected by the defender, in order to successfully achieve its attacking goal. More generally, we consider a conflict situation in which the attacker (Red) proceeds to sequentially infiltrate the defender's (Blue) two layers of defense. Red prevails as the victor if it wins both battles. Otherwise, Blue wins. This conflict situation is modeled as a one-on-two combat model, where a single Red attacker engages two layers of Blue defense and Red must sequentially beat them both in order to win. Given that Red (Blue) has limited attack (defense) resources, the question is how should the two sides allocate their respective resources, where Red wants to maximize the probability of a win, and Blue wishes to minimize it.

While we focus on the cyber domain as our motivating case in this paper, our model is also appropriate for other scenarios. For example, physical locations (e.g., military bases, banks, museums) protected by layers of security that require different skills and/or tools to penetrate. In the museum scenario the attacker would need to first breach the exterior defenses of the museum (e.g., locks, patrollers), and then would need to avoid detection by guards, cameras, and sensors in the interior of the museum to successfully steal the artifact.

Mathematical models representing related armed conflicts comprise a large body of research that ranges between aggregate combat models, that is, *Lanchester models*, which address large-formation engagements (Kress, 2009; Lanchester, 1916; Taylor, 1983; Washburn & Kress, 2009), and more detailed probabilistic models, that is, *stochastic duels*, which describe small-scale engagements (Friedman, 1977; Gafarian & Ancker Jr., 1984; Kress, 1987; Kress, 1992; Williams & Ancker Jr., 1963).

Colonel Blotto games consider a similar scenario where Red and Blue allocate resources across multiple battlefields (Blackett, 1958; Roberson, 2006; Shubik & Weber, 1981). While both our model and Blotto games are resource allocation models, there are several important differences. In contrast to our setting, most Blotto models assume the battlefields are homogenous and contested simultaneously, Red and Blue have equivalent capabilities, and the resources are discrete (e.g., military units). While Blotto assumes all battlefields are engaged in parallel, our setting can be viewed as a series-system from Red's perspective as Red must succeed in both layers to prevail. (Bier et al., 2005) examines game theoretic interactions in a series-system, however there are many differences between our scenario and the one in (Bier et al., 2005). For example, only Red would choose their resource allocation under the framework in (Bier et al., 2005), whereas both Red and Blue make resource allocation decisions in our model.

Our setting is similar to missile defense where Red fires at Blue targets and Blue responds by launching a series of salvos to intercept the Red threats (Hughes Jr, 1995; Karasakal, 2008; Orlin, 1987). Red must sequentially penetrate several layers of Blue defense (interception salvos at long, medium, short range) to hit the targets. Blue only needs to successfully intercept Red in one of the salvos. While most of the work in missile defense is prescriptive, there are some descriptive models that analyze the number of threats that survive each layer (Armstrong, 2005; Armstrong, 2014; Menq et al., 2007; Nunn et al., 1982). There are some crucial differences between our setting and the missile defense scenario. The missile defense problem is usually analyzed from Blue's perspective. While Red may have a decision about which targets to fire at, Red does not allocate resources across the defensive layers. Furthermore, most work in missile defense examines the weapon target assignment (WTA) problem, which considers the assignment of specific interceptors against specific threats at specific ranges (Cai et al., 2006; Davis et al., 2017; Jaiswal et al., 1993). The WTA is a nonlinear integer optimization problem, and most research focuses on developing heuristics (Kline et al., 2019). Our model is much simpler and provides insight into the resource allocation of both Red and Blue across the two layers, and how that allocation varies with key input parameters.

Traditionally, combat models have been applied to violent "kinetic" conflicts where attacks are conducted with lethal weapons and attrition is physical. However, combat models can also be applied to "soft kill" settings, such as cyber-warfare, where missiles and bullets are replaced by lines of code. In such situations, attrition is manifested in loss of valuable information and/or disruptions in the operation of the computer network. Cyber warfare has drawn the attention of the research community (Musman et al., 2011; Rid, 2012), and in particular, its potential impact on kinetic warfare (Hartmann & Steup, 2013; Yildiz, 2014). Moreover, the operations-research community has addressed cyber-related modeling challenges by combining combat and epidemic models (Draeger & Ottl, 2018; Schramm & Gaver, 2013; Yildiz, 2014), analyzing the development and employment of munitions against exploits (Schramm et al., 2014), and applying exploration-exploitation models (Kronzilber, 2017). A recent survey paper (Enayaty-Ahangar et al., 2020) reviews studies that apply optimization to the design of cyber infrastructure.

Game-theoretic approaches for modeling cyber warfare are reported in (Rao et al., 2016) and references therein. The setting in (Colbert et al., 2020) is similar to ours with two layers of a cyber defense. However, the model in (Colbert et al., 2020) considers many discrete attack and defense options with varying costs, which leads to an intractable non-zero-sum game that is analyzed with various heuristics. In contrast, we derive analytic results that provide insight into how the inputs drive the results.

Unlike most of the work reported in the cyber-warfare literature, we explicitly address the layered-defense feature that characterizes many computer networks in the form of the DMZ structure. The question we study in this paper is that of resource allocation, both by the Red and Blue, between the two layers of defense. This study also naturally leads to game-theoretic situations.

The rest of the paper is organized as follows. We describe the model in Section 2 and present results in Sections 3–5 for various scenarios where either Blue or Red or both make resource allocation decisions. Sections 6 and 7 consider extensions to the model where Red does not need to necessarily penetrate both layers to accomplish its objectives. Section 8 expands the game theoretic results from Section 5 to *N* layers.

2 | MODEL

We base our model on the fundamental stochastic duel, where one Blue shooter and one Red shooter repeatedly fire at each other until one is hit (Williams & Ancker Jr., 1963). There are many extensions to the basic model, including multiple shooters and tactical considerations (Friedman, 1977; Gafarian & Ancker Jr., 1984; Kress, 1987; Kress, 1992). In most duel models the time until a shooter scores a successful hit follows an exponential distribution (Friedman, 1977; Gafarian & Ancker Jr., 1984; Kress, 1987). Our problem can be viewed as two sequential duels – one at each layer. Red, the attacker, wins if it successfully penetrates the two layers. Blue wins if it detects Red in one of the layers. As in the duel literature, we model Red's penetration time and Blue's detection time as exponential random variables.

Although we later on somewhat relax it, we assume that the two layers of defense require different attack and defense capabilities. For example, hacking layer 1 requires a much different set of skills than hacking layer 2. Therefore, both Red and Blue have to decide how to allocate their respective cyber-resources (money and manpower) between the two layers. Obviously, Red must allocate non-zero resources to each one of the two layers in order to have a non-zero probability to win.

If Blue and Red allocate x_i and y_i of their respective resources to attack and defend layer $i, i = 1, 2,$, respectively, then the expected time until Red penetrates layer i and Blue detects the attack on that layer, are $\frac{1}{\mu_i y_i}$ and $\frac{1}{\lambda_i x_i}$, respectively. We normalize resources to unitless parameters such that $0 \leq x_i, y_i \leq 1, i = 1, 2.$ and $x_1+x_2 = y_1+y_2 = 1$. The last condition simply says that not utilizing all of one's resources is a dominated strategy. Otherwise, Red (Blue) should simply allocate the remaining resources to either layer and the probability of successful penetration will increase (decrease).

The parameters λ_i and μ_i incorporate two factors. The first is Blue's (Red's) intrinsic, or "per-capita", effectiveness (e.g., cyber qualifications and experience of individual computer analysts) in layer i. As mentioned earlier, the characteristics of the two layers might be very different, and so Blue could be effective at defending one layer but not the other (e.g., $\lambda_1 \gg \lambda_2$). The second factor is the overall level of resources (e.g., number of computer analysts) at Blue's (Red's) disposal. Recall that we normalize resources to lie within [0,1] and so while $x_i = 0.5$ and $y_i = 0.5$ are equivalent from a relative standpoint, they might differ substantially from an absolute perspective. The units of λ_i and μ_i are 1/(time) since the resources x_i and y_i are unitless. $\frac{1}{\lambda_i}$ $(\frac{1}{\mu_i})$ is the expected amount of time for Blue (Red) to defend (penetrate) layer i when Blue (Red) utilizes all available resources in layer i. In this paper, we only consider linear functions of resources: $\lambda_i x_i$ and $\mu_i y_i$. We leave for future work analysis of non-linear relationships between resources and the rates.

Recall that the engagement is asymmetric: Red must successfully defeat both layers to achieve its objective, whereas Blue only needs to detect Red in one layer. Assuming the layers are independent, the probability Red wins is:

$$\begin{aligned} P[\text{Red wins}] &= \frac{\mu_1 y_1}{\mu_1 y_1 + \lambda_1 x_1} \times \frac{\mu_2 y_2}{\mu_2 y_2 + \lambda_2 x_2} \\ &= \frac{\alpha_1 y_1}{\alpha_1 y_1 + x_1} \times \frac{\alpha_2 y_2}{\alpha_2 y_2 + x_2} \end{aligned} \tag{1}$$

where $\alpha_i \equiv \frac{\mu_i}{\lambda_i}$ is the Red-Blue *effectiveness ratio* at layer $i, i = 1, 2$. Recall from the discussion above that the α_i ratio incorporates both the quality and quantity aspects of the two adversaries. Note also that if $y_i = 0$, in some layer, then $P[\text{Red wins}] = 0$ regardless of what Blue does.

Recall we assume the two layers of defense require different types of resources (e.g., cyber skills or tools). However, this may not always be the case; cyber personnel who successfully hack layer 1 may be able to also hack layer 2. Although we primarily focus on the situation where resources cannot be reused ($x_1 + x_2 = 1$, $y_1 + y_2 = 1$), we will show some numerical examples where one side, say Blue, can fully reuse its resources (e.g., $x_1 = x_2 = 1$).

We first consider one-sided situations in Sections 3 and 4 where we fix y_i (x_i) and optimize x_i (y_i) and then study a simultaneous game in Section 5. We conclude this section by presenting the model parameters in Table 1.

3 | BLUE'S DEFENSE ALLOCATION

In this section we assume Red's allocation is fixed to y_1 and y_2, and Blue knows the values of $\mu_1 y_1$ and $\mu_2 y_2$. Blue optimizes

TABLE 1 Model parameters.

Symbol	Range	Description
λ_i	$(0, \infty)$	Blue defensive effectiveness in layer i
μ_i	$(0, \infty)$	Red offensive effectiveness in layer i
α_i	$(0, \infty)$	$\alpha_i \equiv \frac{\mu_i}{\lambda_i}$: Red-Blue effectiveness ratio at layer i
C	$(0, \infty)$	$C \equiv \frac{\alpha_1}{\alpha_2}$: the effectiveness ratio in layer 1 relative to layer 2
D	$(0, 1)$	Partial reward for Red when Red stops after layer 1 (Section 6 only)
q	$(0, 1)$	Probability Red wins immediately after penetrating layer 1 (Section 7 only)
x_i	$[0, 1]$	Blue's defensive resource allocation in layer i
y_i	$[0, 1]$	Red's offensive resource allocation in layer i
x	$[0, 1]$	When x appears without a subscript, it is Blue's allocation in layer 1. In this case Blue allocates $1 - x$ to layer 2
y	$[0, 1]$	Red's allocation in layer 1. In this case Red allocates $1 - y$ to layer 2
$b\,(x; y_1, y_2)$	$[0, 1]$	Red win-probability when Blue allocates x in layer 1 and $(1 - x)$ in layer 2 and Red allocates y_i to layer i (Section 3 only)
$r\,(y; x_1, x_2)$	$[0, 1]$	Red win-probability when Blue allocates x_i to layer i and Red allocates y in layer 1 and $(1 - y)$ in layer 2 (Section 4 only)
$g(x, y)$	$[0, 1]$	Red win-probability when Blue allocates x in layer 1 and $(1 - x)$ in layer 2 and Red allocates y in layer 1 and $(1 - y)$ in layer 2 (Section 5 only)

the allocation x to layer 1, which determines the allocation $1 - x$ to layer 2, such that its detection and threat-elimination rates are $\lambda_1 x$ and $\lambda_2(1 - x)$ for layers 1 and 2, respectively. We first rewrite the Red win-probability in (1) to highlight the functional dependence on x:

$$P[\text{Red wins}] \equiv b\,(x; y_1, y_2) = \frac{\alpha_1 y_1}{\alpha_1 y_1 + x} \times \frac{\alpha_2 y_2}{\alpha_2 y_2 + (1 - x)} \quad (2)$$

Blue wishes to minimize $b\,(x; y_1, y_2)$ subject to $x \in [0, 1]$. This is equivalent to minimizing $\log b\,(x; y_1, y_2)$:

$$\log b\,(x; y_1, y_2) = \log \alpha_1 y_1 - \log(\alpha_1 y_1 + x) + \log \alpha_2 y_2 - \log(\alpha_2 y_2 + (1 - x)). \quad (3)$$

It is easily seen that $\log b\,(x; y_1, y_2)$ is convex in x. Setting the derivative of $\log b(x)$ to 0 yields the unconstrained minimizer of $b\,(x; y_1, y_2)$:

$$\hat{x} = \frac{\alpha_2 y_2 - \alpha_1 y_1 + 1}{2}. \quad (4)$$

Note that there are boundary conditions for $\hat{x}$ that are affected by the effectiveness ratios $\alpha_i, i = 1, 2$. Intuitively, Blue should concentrate its resources where it has a better chance of detecting Red. Specifically, if $\alpha_1 y_1 \geq 1 + \alpha_2 y_2$, then Blue should invest all its resources in protecting layer 2. Conversely, if $\alpha_2 y_2 \geq 1 + \alpha_1 y_1$, then Blue should only focus on layer 1. When $\alpha_1 y_1$ and $\alpha_2 y_2$ are more similar ($-1 < \alpha_2 y_2 - \alpha_1 y_1 < 1$) the interior solution $\hat{x}$ given by (4) is optimal, and Blue allocates resources to both layers. We summarize Blue's optimal allocation in the following proposition:

Proposition 1. *Blue's optimal defense allocation for layer 1 is*

$$x^* = \min(\max(\hat{x}, 0), 1). \quad (5)$$

where $\hat{x}$ is defined by (4).

The constrained minimizer x^* in Proposition 1 follows by combining the unconstrained minimizer $\hat{x}$ with the convexity of $\log b\,(x; y_1, y_2)$.

We conclude this section by examining the worst case scenario for Blue, when Red is able to reuse all of its resources allocated to layer 1 in layer 2, that is, $y_1 = y_2 = 1$. As discussed in Section 2, this could occur if Red is able to use the same personnel or tools to hack both layers. We do not have data to estimate the parameters – they are typically classified – however, fortunately, we only need the relative quantities α_i, which should be easier to estimate compared to individual parameters. Arguably, $\alpha_1 \geq \alpha_2$; as Red penetrates deeper into the network, it becomes more vulnerable to Blue's detection capabilities. Figure 1 presents the optimal allocation x^* for Blue, as a function of α_1 for several values of $C \equiv \frac{\alpha_1}{\alpha_2}$. The parameter ranges we consider in Figure 1 and the rest of the paper correspond to moderate settings where Blue and Red have similar capabilities (i.e., α_i do not assume extreme values) and one layer is not significantly more difficult to penetrate than the other (i.e., α_1 and α_2 have the same magnitude). For small values of α_1 the optimal allocation x^* is the unconstrained minimizer $\hat{x}$, which by inspection of (4) is just a line with an intercept of $\frac{1}{2}$ and a slope of $\frac{1}{2}\left(\frac{1}{C} - 1\right)$. Notice, as trivially observed from (4), that if the two layers have equal effectiveness ratios ($C = 1$), Blue should equally split its resources between the two layers, regardless of the actual value of the effectiveness ratio α_1. As C increases (i.e., the effectiveness ratio in layer 1 increases compared to layer 2), the fraction of Blue's resources directed to layer 1 decreases. For a given $C > 1$, as α_1 increases (i.e., Red becomes more effective compared to Blue in layer 1) x^* decreases to the point where Blue should abandon layer 1 and put all of its resources in layer 2 (e.g., when $C = 5$ and $\alpha_1 \geq 1.25$).

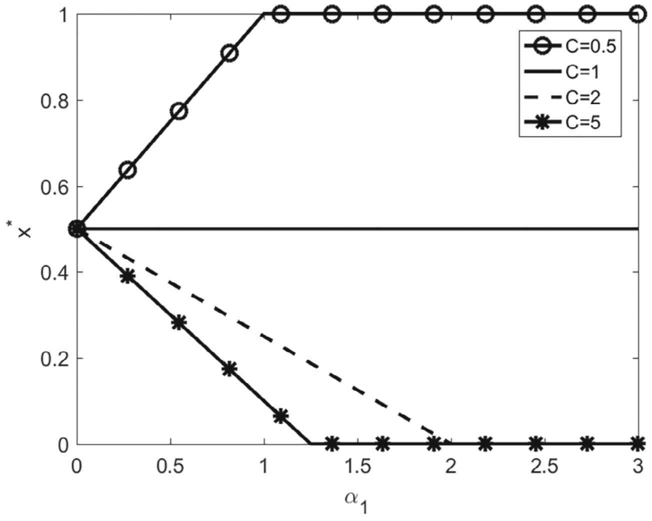


FIGURE 1 Blue's optimal allocation at layer 1, x^*, as a function of α_1 for several values of $C \equiv \frac{\alpha_1}{\alpha_2}$. Red is able to reuse all its resources from layer 1 in layer 2: $y_1 = y_2 = 1$.

As mentioned above, it is most likely that $C \geq 1$. The case $C < 1$ is presented in the plot just as a reference.

4 | RED'S ATTACK ALLOCATION

We now assume that Blue's allocation is fixed at x_1 and x_2 and Red optimizes its resource allocation while knowing the values of $\lambda_1 x_1$ and $\lambda_2 x_2$. Red optimizes y to layer 1 and $1 - y$ to layer 2. Thus, Red's problem is to choose y that maximizes

$$P[\text{Red wins}] \equiv r\,(y; x_1, x_2) = \frac{\alpha_1 y}{\alpha_1 y + x_1} \times \frac{\alpha_2(1 - y)}{\alpha_2(1 - y) + x_2}. \quad (6)$$

Equation (6) is a special case of (1). Note that $r\,(0; x_1, x_2) = r\,(1; x_1, x_2) = 0$ for any $x_1, x_2 \in [0, 1]$, whereas $r\,(y; x_1, x_2) > 0$ for any $0 < y < 1$. Hence unlike Blue, who might optimally concentrate all of its resources only in one layer (see Section 3), Red must allocate positive effort to each layer because otherwise $P[\text{Red wins}] = 0$. Thus, the optimal allocation must lie in the interior: $y^* \in (0, 1)$. The following proposition presents the optimal allocation.

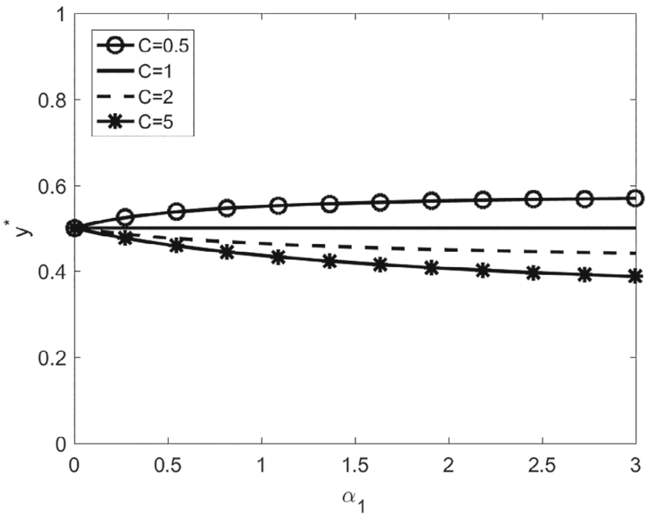


FIGURE 2 Red's optimal allocation at layer 1, y^*, as a function of α_1 for several values of $C \equiv \frac{\alpha_1}{\alpha_2}$. Blue is able to reuse all its resources from layer 1 in layer 2: $x_1 = x_2 = 1$.

Proposition 2. *Red's optimal attack allocation to layer 1 is*

$$y^* = \frac{-x_1(\alpha_2 + x_2) + \sqrt{x_1 x_2 (\alpha_1 + x_1)(\alpha_2 + x_2)}}{\alpha_1 x_2 - \alpha_2 x_1} \quad \text{for} \quad \frac{\alpha_1}{x_1} \neq \frac{\alpha_2}{x_2} \tag{7}$$

When the denominator of (7) is 0 $\left(\frac{\alpha_1}{x_1} = \frac{\alpha_2}{x_2}\right)$, $y^* = 0.5$.

The proof for Proposition 2 proceeds in a similar fashion to the logic in Section 3 for Blue's defense allocation. We show that $r(y; x_1, x_2)$ is a concave function of y and y^* in (7) satisfies the first order condition. Full details of the proof for Proposition 2 appears in Appendix B.2 of the Online Supporting Information.

As with Figure 1, Figure 2 displays the optimal resource allocation y^* for Red as a function of α_1 for six values of $C \equiv \frac{\alpha_1}{\alpha_2}$. Similarly to Figure 1, we assume a worst case for Red where Blue can fully reuse its resources in layer 2: $x_1 = x_2 = 1$. In the special case when the two layers are equal in terms of effectiveness ratios ($C = 1$), the optimal allocation is to equally split the resources between the two layers. Also, notice from Figure 2 that, unlike the case for Blue in Figure 1, Red's resource allocation is quite insensitive to both the effectiveness ratios α_i and the relative effectiveness between the two layers C. As observed above, Red has to engage in both layers to succeed, but Figure 2 shows that Red's level of engagement in the two layers is close to parity, unless both α_1 and C are very large.

5 | SIMULTANEOUS ALLOCATION

In the previous two sections we assume that Blue (Red) allocates its finite resource against a fixed Red (Blue) allocation. Suppose now that both sides choose how to allocate their limited resources between the two layers simultaneously. As in Sections 3 and 4, we assume that resources in layer 1 cannot be reused in layer 2: $x_1 + x_2 = y_1 + y_2 = 1$. Hence Blue (Red) only needs to choose its allocation x (y) in layer 1, with the remaining $1 - x$ ($1 - y$) going to layer 2. Both Blue and Red know the effectiveness ratios α_1, α_2, but do not know the allocation of effort (y, x) in the opposite side. In this case, Equation (1) can be written as

$$P[\text{Red wins}] \equiv g(x, y) = \frac{\alpha_1 y}{\alpha_1 y + x} \times \frac{\alpha_2(1-y)}{\alpha_2(1-y) + (1-x)}. \tag{8}$$

Red wishes to maximize $g(x, y)$ while Blue wants to minimize it. Examining the second derivative of $g(x, y)$ reveals that $g(x, y)$ is a strictly convex function of x for a fixed y, and strictly concave function of y for a fixed x. Therefore, we have a concave-convex game, which implies $g(x, y)$ has a saddle point, which is the solution of the allocation game of the cyber resources.

Proposition 3. *The unique solution of the simultaneous zero-sum allocation game between Red and Blue is*

$$x^* = y^* = \frac{1}{1 + \frac{\alpha_1 + 1}{\alpha_2 + 1}} \tag{9}$$

The value of the game – the probability that Red wins – is

$$v^* = \frac{\alpha_1}{\alpha_1 + 1} \times \frac{\alpha_2}{\alpha_2 + 1}. \tag{10}$$

Because we have a concave-convex game, we just need to verify that (x^*, y^*) in (9) satisfies the first order conditions. The complete proof of Proposition 3 appears in Appendix B.3 of the Online Supporting Information.

Figure 3 shows the layer 1 resource allocation for both Blue and Red. As in the one-sided cases, we see that if the effectiveness ratios are the same in both layers ($C = 1$) then the allocation is equal in the two layers, regardless of the actual

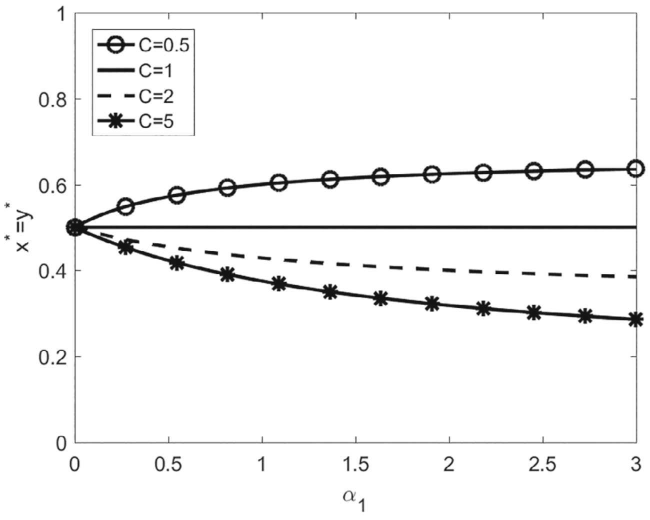


FIGURE 3 Blue and Red's optimal allocation at layer 1 as a function of α_1 for several values of $C \equiv \frac{\alpha_1}{\alpha_2}$.

value of the ratio α_1. When the effectiveness ratio tilts, as one would expect, toward Blue at the second layer (i.e., C increases), the allocation of resources also tilts toward layer 2, albeit in moderate manner, as shown in Figure 3. The minimum fraction of resources Red (and Blue) must put in layer 1 is $\frac{1}{1+C}$ (when $C > 1$). Even if $\alpha_1 >> \alpha_2$ Red must still allocate some resources to layer 1 to penetrate it.

6 | PARTIAL REWARD FOR RED

Thus far we assume a binary situation: either Red successfully penetrates undetected the two defense layers of Blue, in which case Red is the winner, or Red is intercepted by Blue, either in layer 1 or layer 2, and Blue is the winner. Now suppose that Red can choose to stop after penetrating layer 1 and collect some partial reward $D < 1$. For example, a hacker can stop after penetrating the DMZ and just download email messages. If Red decides to continue to layer 2 after successfully penetrating layer 1, Red will collect a reward of 1 if not intercepted by Blue in layer 2. Red receives a reward of 0 if Blue intercepts Red in either layer. That is, Red forfeits the D collected in layer 1 if Red continues to layer 2 and Blue intercepts Red at layer 2. So, the question here is regarding Red's stopping rule: shall Red stop after penetrating layer 1 or should Red continue to layer 2. Now in addition to Red and Blue choosing their resource allocations, Red must also choose whether to stop after layer 1. More specifically, we consider the simultaneous game situation where Blue decides on the value of x, and Red chooses both the value of y and whether to stop after layer 1 or proceed to layer 2. We use the nomenclature "choose layer 1" or "choose layer 2" to denote Red's options for its stop/continue decision.

Define $f_i(x, y)$ as the game payoff (Red expected reward) if Red chooses layer i with allocation y and Blue uses allocation x.

$$f_1(x, y) \equiv \frac{\alpha_1 y}{\alpha_1 y + x} D \tag{11}$$

$$f_2(x, y) \equiv \frac{\alpha_1 y}{\alpha_1 y + x} \frac{\alpha_2(1-y)}{\alpha_2(1-y) + (1-x)} \tag{12}$$

For a small value of D, Red gains little benefit from stopping after layer 1 and thus Red chooses layer 2; therefore the solution is the same as in Proposition 3. For larger values of D, Red plays a mixed strategy; with some probability Red only attacks layer 1 and obviously puts all its resources in that layer. Otherwise, Red plans to attack layer 2 too and allocates resources to both layers.

Proposition 4. *If*

$$D < \frac{\alpha_2}{\alpha_2 + 1} \times \frac{\alpha_1 + \alpha_2 + 1}{\alpha_1 + \alpha_2 + 2} \tag{13}$$

then the solution of the game is the same as in Proposition 3. That is, Red chooses layer 2 and the resource allocation between the two layers will be the same for Red and Blue as in Equation (9). Otherwise, Red plays a mixed strategy across two options:

- *With probability p^* Red chooses to allocate all of its resources to layer 1 ($y = 1$).*
- *With probability $1 - p^*$ Red chooses layer 2 and only allocates a fraction y^* to layer 1.*

Blue uses a pure strategy and allocates x^* to layer 1. The triple (x^*, y^*, p^*) satisfies the following simultaneous equations

$$y = \frac{-x\,(\alpha_2 + (1-x)) + \sqrt{x(1-x)\,(\alpha_1 + x)\,(\alpha_2 + (1-x))}}{\alpha_1(1-x) - \alpha_2 x} \tag{14}$$

$$p = \frac{\alpha_2 y(1-y)(\alpha_1 + x)^2\,((\alpha_1 y + x) - (\alpha_2(1-y) + (1-x)))}{\alpha_2 y(1-y)(\alpha_1 + x)^2\,((\alpha_1 y + x) - (\alpha_2(1-y) + (1-x))) + D(\alpha_1 y + x)^2(\alpha_2(1-y) + (1-x))^2} \tag{15}$$

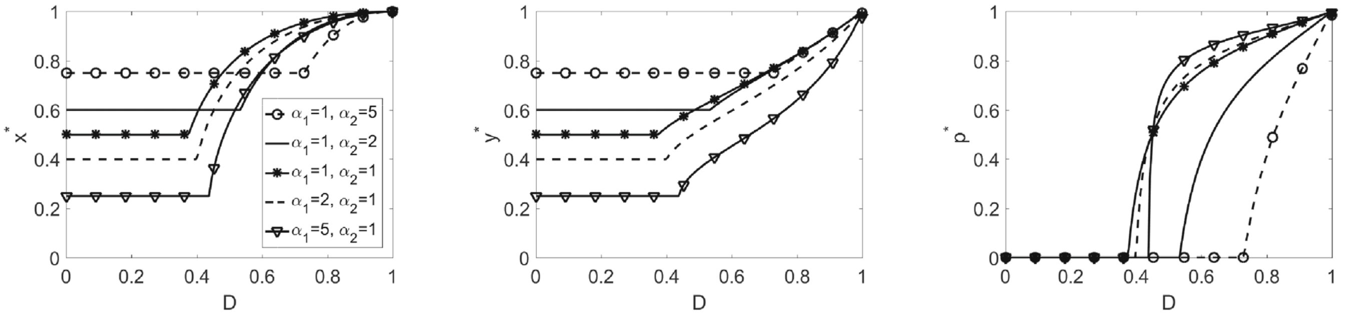
$$D\,(\alpha_1 y + x)\,(\alpha_2(1-y) + (1-x)) = \alpha_2 y(1-y)\,(\alpha_1 + x) \tag{16}$$

The proof of Proposition 4 appears in Appendix A of the Online Supporting Information. Equation (14) determines Red's best allocation y when choosing layer 2 if Blue allocates x. Equation (15) dictates Blue's best response to Red mixing with probability p and allocating y when Red chooses layer 2. Equation (16) equalizes the payoff between choosing layer 1 and layer 2 ($f_1(x^*, 1) = f_2(x^*, y^*)$), which allows for a Red mixed strategy to be optimal.

The threshold for D in (13) that determines whether Red solely chooses layer 2 is driven primarily by α_2. When Red is very effective in layer 2 (large α_2), then Red will attempt to penetrate layer 2 unless D is close to 1. For smaller values of α_2, Red is more likely to be satisfied with collecting D and stopping at layer 1.

While there is no closed form solution for (x^*, y^*, p^*) in (14)–(16), solving for these three parameters numerically is very straightforward as we only need to perform a grid-search over x, which fully determines the solutions for y and p via (14)–(15). We describe the grid-search approach in Appendix A.2.1 of the Online Supporting Information. Figure 4 plots (x^*, y^*, p^*) from (14) to (16) versus D for different values of α_1 and α_2. The curves are flat when D is less than the threshold in (13) and the solution is given by Proposition 3. As D increases, layer 1 becomes more enticing for Red as there is little marginal benefit to risking layer 2. However, as Proposition 4 reveals, Red never fully commits to layer 1 for $D < 1$. Figure 4 illustrates that, while theoretically Red never fully commits to layer 1 with certainty, practically, Red (and Blue) do put all the effort into layer 1 as $D \to 1$ since $x^*, y^*, p^* \to 1$.

x^* and y^* no longer equal each other once D increases beyond the threshold specified in (13). x^* more quickly



(A) x^* vs. D (B) y^* vs. D (C) p^* vs. D

FIGURE 4 Blue (x^*) and Red's (y^*, p^*) optimal strategy as a function of D for several combinations of (α_1, α_2).

increases to 1 than y^*. This occurs partly because x^* needs to account for Blue's response to Red choosing either layer 1 or layer 2, whereas y^* is the solution conditioned on Red choosing layer 2. Red also shifts its focus to layer 1 via its mixing probability p^* as D increases. x^* increases more quickly also because of the asymmetric nature of the engagement: Blue only needs to intercept in one layer, whereas Red needs to succeed in both, so Red cannot be as aggressive shifting toward layer 1.

7 | EARLY VICTORY

We consider here a similar situation to the one described in Section 6. Instead of partial reward D, we assume that there is a probability q that Red wins – it attains its attack goals – immediately after penetrating layer 1. In that case, Red does not need to proceed to layer 2, in which a successful attack guarantees a win. In the cyber DMZ scenario this could occur if a critical file, targeted by Red, is mistakenly moved by Blue into the DMZ. Such a situation could occur, for example, when an individual needs to work at home and emails themselves the critical file; once the file is on the email server, Red can gain access to it without penetrating layer 2. For the museum scenario, Red's target artifact has been moved to a less secure location in the museum for cleaning. This early victory setting represents Red getting lucky and only needing to exploit the outermost layer to win. For arbitrary Blue allocation (x_1, x_2) and Red allocation (y_1, y_2) the Red win-probability in (1) generalizes to:

$$P[\text{Red wins}] = \frac{\alpha_1 y_1}{\alpha_1 y_1 + x_1}\left(q + (1-q)\frac{\alpha_2 y_2}{\alpha_2 y_2 + x_2}\right) \tag{17}$$

The term outside the parentheses is the probability Red is successful in layer 1; Red still must penetrate layer 1 to win. If Red succeeds in layer 1, then with probability q Red wins, otherwise Red proceeds to layer 2 and must succeed in layer 2 to win. We assume that q is a fixed constant; future work could examine the situation where Red or Blue could modify q via resource allocation.

We extend the results from Sections 3–5 in the following three subsections.

7.1 | Blue's defense problem

Given fixed Red allocation (y_1, y_2), Blue's problem is to minimize

$$P[\text{Red wins}] = \frac{\alpha_1 y_1}{\alpha_1 y_1 + x}\left(q + (1-q)\frac{\alpha_2 y_2}{\alpha_2 y_2 + (1-x)}\right) \tag{18}$$

Define:

$$\widetilde{x} = \frac{q + \alpha_2 y_2 - \sqrt{\alpha_2 y_2 (1-q)\left(q\left(1 + \alpha_1 y_1\right) + \alpha_2 y_2\right)}}{q}. \tag{19}$$

Proposition 5. *Blue's optimal defense allocation for layer 1 is*

$$x^* = \min(\max(\widetilde{x}, 0), 1). \tag{20}$$

where $\widetilde{x}$ is defined by (19).

The proof of Proposition 5 appears in Appendix B.1of the Online Supporting Information.

7.2 | Red's attack problem

Given fixed Blue allocation (x_1, x_2), Red's problem is to maximize

$$P[\text{Red wins}] = \frac{\alpha_1 y}{\alpha_1 y + x_1}\left(q + (1-q)\frac{\alpha_2(1-y)}{\alpha_2(1-y) + x_2}\right) \tag{21}$$

Define:

$$\widetilde{y} = \frac{\alpha_2 x_1\left(\alpha_2 + x_2\right) - \sqrt{\alpha_2 x_1 x_2\left(\alpha_2 + x_2\right)(1-q)\left(\alpha_1 x_2 q + \left(\alpha_1 + x_1\right)\alpha_2\right)}}{\alpha_2\left(\alpha_2 x_1 - \alpha_1 x_2 (1-q)\right)}. \tag{22}$$

In the special case when the denominator of (22) equals 0, $\widetilde{y}$ simplifies to

$$\widetilde{y} = \frac{1}{2} + \frac{x_2 q}{2\alpha_2} \tag{23}$$

Proposition 6. *Red's optimal attack allocation for layer 1 is*

$$y^* = \min(\widetilde{y}, 1). \tag{24}$$

where $\widetilde{y}$ is defined by (22)–(23).

The proof of Proposition 6 appears in Appendix B.2. In the original formulation with $q = 0$ in Section 4, Red had to optimally allocate a positive amount to both layers. With $q > 0$, Red must still allocate a positive amount to layer 1. However, if q is large enough, Red might neglect layer 2 and allocate everything to layer 1 in the hope that the early victory occurs.

7.3 | Simultaneous allocation

When both Blue and Red optimally allocate their resources, then Red and Blue are engaged in a zero-sum game: Red wants to maximize and Blue minimize the following value

$$P[\text{Red wins}] = \frac{\alpha_1 y}{\alpha_1 y + x}\left(q + (1-q)\frac{\alpha_2(1-y)}{\alpha_2(1-y) + (1-x)}\right) \tag{25}$$

Proposition 7. *The unique solution of the simultaneous zero-sum game is*

$$x^* = y^* = \frac{q(\alpha_2+1)^2 + (1-q)\alpha_2\,(\alpha_2+1))}{q(\alpha_2+1)^2 + (1-q)\alpha_2\,(\alpha_1+\alpha_2+2)} \tag{26}$$

The game value (Red win-probability) is:

$$v^* = \frac{\alpha_1}{\alpha_1+1}\left(q + (1-q)\frac{\alpha_2}{\alpha_2+1}\right) \tag{27}$$

The proof of Proposition 7 appears in Appendix B.3 of the Online Supporting Information. Figure 5 plots the relationship between x^*, y^* and q for different values of α_1 and α_2. x^* and y^* start at the solution given in Proposition 3 at $q = 0$ and increase toward 1 in a near linear fashion. In particular, linearity is attained in the case of parity, $\alpha_1 = \alpha_2 = 1$, where the allocation is $x^* = y^* = \frac{q+1}{2}$, and the probability Red wins is $v^* = \frac{q+1}{4}$. More generally, the relationship is linear whenever $\alpha_2 = \frac{1}{\alpha_1}$, in which case $x^* = y^* = q + (1-q)\frac{1}{\alpha_1+1}$.

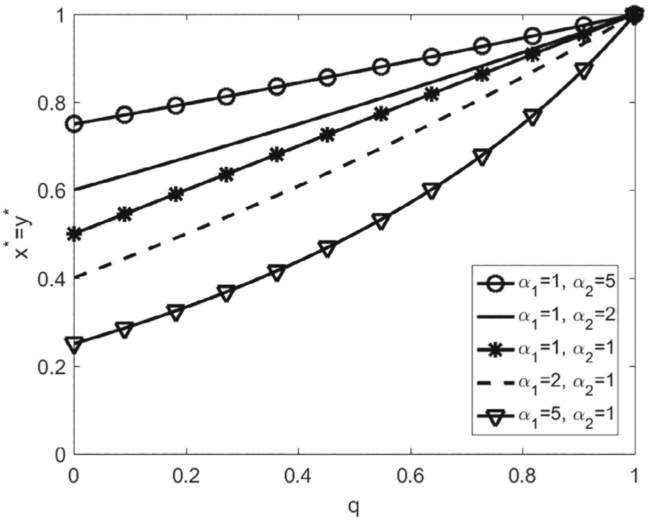


FIGURE 5 Blue and Red's optimal allocation at layer 1 as a function of q for several combinations of (α_1, α_2).

8 | N-LAYER SIMULTANEOUS GAME

In this section we extend the game theoretic model from Section 5 to N layers. Blue allocates $\mathbf{x} = (x_1, x_2, \dots, x_N)$ to defend the layers and Red allocates $\mathbf{y} = (y_1, y_2, \dots, y_N)$ to attack. Equation (1) generalizes to

$$g(\mathbf{x}, \mathbf{y}) \equiv P[\text{Red wins}] = \prod_{i=1}^{N} \frac{\alpha_i y_i}{\alpha_i y_i + x_i} \tag{28}$$

We assume resources cannot be reused across layers, that is, $\sum_{i=1}^{N} x_i = \sum_{i=1}^{N} y_i = 1, x_i, y_i \geq 0$. As in Section 5, the game payoff in (28) generates a concave-convex game and yields the following saddle point solution.

Proposition 8. *The unique optimal solution of the simultaneous zero-sum game is*

$$x_i^* = y_i^* = \frac{\frac{1}{\alpha_i+1}}{\sum_{j=1}^{N} \frac{1}{\alpha_j+1}} \tag{29}$$

The game value (Red win-probability) is:

$$v^* = \prod_{i=1}^{N} \frac{\alpha_i}{\alpha_i+1} \tag{30}$$

The proof of Proposition 8 appears in Appendix C of the Online Supporting Information. Proposition 8 generalizes Proposition 5.

If α_i is large compared to $\alpha_j, j \neq i$, then the optimal allocation x_i^* (y_i^*) is close to 0 for layer i. In this case Red is very effective relative to Blue in layer i, and so Blue essentially concedes layer i. If α_i is small compared to $\alpha_j, j \neq i$, (i.e., Blue is very effective relative to Red in layer i), then the resource allocations (x_i^*, y_i^*) increase, but do not approach 1. Red has to successfully penetrate every layer, so cannot allocate too much to any one layer. For example, if $\alpha_i \approx 0$, and $\alpha_j \equiv \alpha$ are equal across the remaining layers $j \neq i$, Equation (29) simplifies to

$$x_j^* = y_j^* = \begin{cases} \frac{\alpha+1}{N+\alpha} & \text{if} \quad j = i \\ \frac{1}{N+\alpha} & \text{if} \quad j \neq i \end{cases} \tag{31}$$

The resource allocation in layer i (where Red is ineffective) is $\alpha+1$ times greater than the allocation in any of the other layers. For example, with $N = 7$ layers and $\alpha = 8$, Blue and Red allocate $x_i^* = y_i^* = 0.6$ to layer i, which leaves a substantial amount of resources for the other layers.

9 | CONCLUSION

As in any contest, resource allocation in cyber warfare may determine the outcome of the confrontation. Specifically when cyber resources, either offensive or defensive, are limited, actors engaged in cyber warfare must optimize the deployment of those resources and/or modify their tactics. In this paper, we formulate a base model where Red needs to successfully penetrate both layers to achieve victory, whereas Blue only needs to detect Red in one of the layers. We also consider extensions where Red may achieve its objective without penetrating both layers. In the situation where Blue optimizes its allocation for a fixed Red allocation, Blue focuses all its resources on the layer where it has the advantage unless the relative effectiveness levels in the two layers are similar. This contrasts with the scenario when Red is the sole decision-maker against a fixed Blue allocation: Red always allocates resources to both layers in a nearly equal split that is fairly insensitive to the effectiveness of Red and Blue. In the game where both Red and Blue allocate resources, the allocation is symmetric and usually of moderate value; the allocation only approaches 0 or 1 when the two layers significantly differ in their effectiveness ratios. When Red can obtain rewards for just penetrating layer 1, both Red and Blue shift resources to layer 1. The models presented in this paper, combined with controlled Red Team/Blue Team exercises and wargames, can guide cyber combat developers in determining where would be the highest "bang for the buck" in allocating resources in cyber attack or defense.

There are many avenues for future research. One could examine the notion of reusable resources more carefully. For example, the resources could be split into three bins: those that apply solely to layer 1, those that apply solely to layer 2, and those that apply to both layer 1 and layer 2. Presumably, the resources that specialize to only one layer are more effective than the general resources that can be used in both. Another possible extension is to generalize the fixed early-victory parameter q in Section 7 to account for resources that may affect its value. Red might be easier to detect when Red allocates more resources to a layer. Therefore, Blue's overall defensive rate may depend upon y_i in addition to x_i. Another related approach would have Red allocate its resources between a speed component and a stealth component of its attack plan. We assume complete information framework where both sides know all parameters. Future work could develop a Bayesian game for an incomplete information setting. If Red repeatedly attacks, a learning component could be incorporated where Blue and Red update their beliefs about their opponent's parameters after each round. Cyber data sets exist (e.g., (Canadian Institute for Cybersecurity, 2023)), however most are meant to be benchmarks for machine learning classifiers trying to detect cyber intrusions. Future work could perform an empirical exercise to examine our model by collecting data via experiments or cyber competitions.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Michael P. Atkinson https://orcid.org/0000-0001-6606-8188

REFERENCES

Armstrong, M. J. (2005). A stochastic salvo model for naval surface combat. *Operations Research*, *53*, 830–841.

Armstrong, M. J. (2014). Modeling short-range ballistic missile defense and Israel's iron dome system. *Operations Research*, *62*, 1028–1039.

Bier, V. M., Nagaraj, A., & Abhichandani, V. (2005). Protection of simple series and parallel systems with components of different values. *Reliability Engineering & System Safety*, *87*, 315–323.

Blackett, D. W. (1958). Pure strategy solutions of blotto games. *Naval Research Logistics*, *5*, 107–109.

Cai, H., Liu, J., Chen, Y., & Wang, H. (2006). Survey of the research on dynamic weapon-target assignment problem. *Journal of Systems Engineering and Electronics*, *17*, 559–565.

Canadian Institute for Cybersecurity. (2023). University of New Brunswick. https://www.unb.ca/cic/datasets/index.html

Colbert, E. J., Kott, A., & Knachel, L. P. (2020). The game-theoretic model and experimental investigation of cyber wargaming. *The Journal of Defense Modeling and Simulation*, *17*, 21–38.

Dadheech, K., Choudhary, A., & Bhatia, G. (2018). De-militarized zone: A next level to network security. *Proceedings of the 2nd Intl. Conference on Inventive Communication and Computational Technologies*.

Davis, M. T., Robbins, M. J., & Lunday, B. J. (2017). Approximate dynamic programming for missile defense interceptor fire control. *European Journal of Operational Research*, *259*, 873–886.

Draeger, J., & Ottl, S. (2018). Malware epidemics effects in a Lanchester conflict model. Arxiv.

Enayaty-Ahangar, F., Albert, L. A., & DuBois, E. (2020). A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions*, *53*(2), 182–198.

Friedman, Y. (1977). Optimal strategy for the one-against-many-battle. *Operations Research*, *25*(5), 884–888.

Gafarian, A. V., & Ancker, C. J., Jr. (1984). The two-on-one stochastic duel. *Naval Research Logistics Quarterly*, *31*(2), 309–324.

Hartmann, K., & Steup, C. (2013). The vulnerability of UAVs to cyber attacks–An approach to the risk assessment. Paper presented at: 2013 5th international conference on cyber conflict (CYCON 2013), Tallinn, Estonia.

Hughes, W. P., Jr. (1995). A salvo model of warships in missile combat used to evaluate their staying power. *Naval Research Logistics*, *42*, 267–289.

IBM. (2023). The Layered Defense Approach to Security. https://www.ibm.com/docs/en/i/7.3?topic=security-layered-defense-approach

Jaiswal, N. K., Shrotri, P. K., & Nagabhushana, B. S. (1993). Optimal weapon mix, deployment and allocation problems in multiple layer defense. *American Journal of Mathematical and Management Sciences*, *13*, 53–82.

Karasakal, O. (2008). Air defense missile-target allocation models for a naval task group. *Computers & Operations Research*, *35*, 1759–1770.

Kline, A., Ahner, D., & Hill, R. (2019). The weapon-target assignment problem. *Computers & Operations Research*, *105*, 226–236.

Kress, M. (1987). The many-on-one stochastic duel. *Naval Research Logistics*, *34*, 713–720.

Kress, M. (1992). A many-on-many stochastic duel model for mountain battle. *Naval Research Logistics*, *39*, 437–446.

Kress, M. (2009). Modeling armed conflicts. *Science*, *336*(6083), 865–869.

Kronzilber, D. (2017). Multi-armed bandit models of network intrusion in the cyber domain, Master's Thesis. Naval Postgraduate School.

Lanchester, F. (1916). Aircraft in warfare: The Dawn of the forth arm. Constable.

Menq, J. Y., Tuan, P. C., & Liu, T. S. (2007). Discrete Markov ballistic missile defense system modeling. *European Journal of Operational Research*, *178*, 560–578.

Musman, S., Tanner, M., Temin, A., Elsaesser, E., & Loren, L. (2011). Computing the impact of cyber attacks on complex missions. Paper presented at: 2011 IEEE International Systems Conference, Montreal, Canada. https://doi.org/10.1109/SYSCON.2011.5929055

Nunn, W. R., Glass, D. V., Hsu, I. C., & Perin, D. A. (1982). Analysis of a layered defense model. *Operations Research*, *30*, 595–599.

Orlin, D. (1987). Optimal weapons allocation against layered defenses. *Naval Research Logistics*, *34*, 605–617.

Rababah, B., Zhou, S., & Bader, M. (2018). Evaluation the performance of DMZ. *International Journal of Wireless and Microwave Technologies*, *1*, 1–13.

Rao, N. S. V., Poole, S. W., Ma, C. Y. T., He, F., Zhuang, J., & Yau, D. K. Y. (2016). Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. *Risk Analysis*, *36*(4), 694–710.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5–32.

Roberson, B. (2006). The Colonel Blotto Game. *Economic Theory*, *29*, 1–24.

Schramm, H. C., Alderson, D. L., Carlyle, W. M., & Dimitrov, N. B. (2014). A game theoretic model of strategic conflict in cyberspace. *Military Operations Research*, *19*(1), 5–17.

Schramm, H. C., & Gaver, D. P. (2013). Lanchester for cyber: The mixed epidemic-combat model. *Naval Research Logistics*, *60*(7), 599–605.

Shubik, M., & Weber, R. J. (1981). Systems defense games: Colonel blotto, command and control. *Naval Research Logistics*, *28*, 281–287.

Taylor, J. (1983). Lanchester models of warfare. Informs.

Washburn, A., & Kress, M. (2009). Combat modeling. Springer.

Williams, T. W., & Ancker, C. J., Jr. (1963). Stochastic duels. *Operations Research*, *11*(5), 803–817.

Yildiz, F. (2014). Modeling the effects of cyber operations on kinetic battles, Master's Thesis. Naval Postgraduate School.

SUPPORTING INFORMATION

Additional supporting information can be found online in the Supporting Information section at the end of this article.

How to cite this article: Atkinson, M. P., & Kress, M. (2023). Resource allocation in two-layered cyber-defense. *Naval Research Logistics (NRL)*, *70*(6), 574–583. https://doi.org/10.1002/nav.22106