Whack-a-mole: Asymmetric Conflict and Guerrilla Warfare in Web Security

Pern Hui Chia[1⋆], John Chuang[2], and Yanling Chen[3]

[1] Google
[2] UC Berkeley
[3] University of Duisburg-Essen
pernhc@google.com,chuang@ischool.berkeley.edu,yanling.chen@uni-due.de

Abstract. Many malicious and fraudulent endeavors on the web exhibit characteristics of asymmetric conflict and guerrilla warfare. Defenders work continuously to detect and take down malicious websites, while attackers respond by resisting takedowns, evading detection, or creating large numbers of new sites. This is reminiscent of the arcade game of whack-a-mole – the faster the moles pop in and out of the holes, the harder it becomes for the player to hit every one of them. In this work, we present the Colonel Blotto Web Security (CBWS) framework to model the asymmetric conflict and guerrilla warfare in web security. We find that even with a resource asymmetry disadvantage, an attacker can still realize significant utilities, provided that it can exploit an information asymmetry in its favor. In some cases, an attacker can realize a high utility with just a minimal number of websites that go undetected. In other cases, an attacker may realize little if any utility even after creating a large number of websites. The CBWS framework also allows us to model the effects of competition among multiple attackers. We find that competition weakens the effects of information asymmetry, and leads to a degradation of attacker utilities, even as more malicious sites are created.

Keywords: Web Security, Colonel Blotto, Attacker Competition

1 Introduction

Despite widespread attention and significant technology advancements, web security remains a daunting challenge. Cyber-criminal activities such as phishing, drive-by downloads, illegal online pharmacies, child pornography distribution continue unabated, sustaining a thriving underground ecosystem. Whenever malicious and fraudulent websites are detected and removed, attackers create new ones to replenish the old ones. Large numbers of websites are created at high frequencies to evade detection and to stretch the defenders. Security specialists are hired by financial institutions, service providers and government agencies to

⋆ Part of the research was conducted when first and third authors were affiliated to Norwegian University of Science and Technology.

detect and take down these websites. However, many of these websites remain online for long enough, undetected or resisting takedown, to victimize unsuspecting users.

The continuous cycle of create-detect and resist-takedown is most evident with phishing. Two common vectors of phishing websites are compromised web servers and free web hosting services [32]. Researchers note that system administrators and hosting companies are usually cooperative and quick to take down the phishing pages once notified; however, detecting the phishes in the first place is challenging [32]. Attackers apply various tricks to extend the uptime of their sites. Some attackers configure the phishing sites not to resolve on every access to misguide the defender. Others temporarily withdraw from a compromised web server to avoid further actions from the administrator [4,32]. Meanwhile, resourceful phishers leverage sophisticated technology to exploit malware-infested machines to resist takedown. They use the 'fast flux' method to map a domain name to different IP addresses of different bot machines by changing the DNS records at a high frequency.

It is not surprising that other web perpetrators will exploit the same techniques. For example, the fast flux method has also been used by the 'Avalanche' gang for perpetuating drive-by downloads and distributing the Zeus malware [4]. Several months after Microsoft executed the takedown of the Kelihos botnet, which exploits user machines to deliver spam and steal user credentials, a new variant of the Kelihos attack re-emerged with fast flux techniques [1]. This makes takedown difficult especially given the limited control of the ISPs on bot machines. Even without access to sophisticated technologies, web perpetrators can still overwhelm the defender with large numbers of attacks, to evade detection and to stretch the takedown resources. As we will show in this work, attackers can systematically quantify the optimal number of attacks to launch, so to maximize their payoffs.

Web Security vs. Network Security. Use of game theoretical analysis in security has gained popularity in recent years. An early work is by Liu and Zang [28], which advocates the use of game theory to model and infer attacker intent, objectives, and strategies. A comprehensive survey of game theoretical literature for security and privacy can be found in [29]. In particular, the dynamics between attackers and defenders have been studied in a variety of network security contexts. Clark and Konrad considers a 'weakest link' security game where the attacker only needs to win one front out of multiple fronts [13]. Others extend the analysis to multiple defenders and different interdependency classes, including best-shot, total-effort, and weakest-target games [38,18,15]. Several studies model the intrusions into a known set of network systems (e.g., [2,5,6]) or denial-of-service attacks on specific network resources (e.g., [3,9]). Kiekintveld et al. propose a Stackelberg Security Game where the defender first commits to a security policy (which may involve multiple assets to defend), and the attacker conducts surveillance to learn the defender's policy before launching an attack [22]. The FlipIt game considers the dynamics when an attacker can compromise or re-compromise a system without immediate detection by the defender,

and the defender can reclaim the system with or without detecting a compromise [37]. The FlipThem game extends it to a known set of multiple resources, where the attacker seeks to compromise either one or all resources [25].

The dynamics between attackers and defenders in the context of web security is different from those in network security or cyber-physical system security. While network attackers target a known set of systems or resources, malicious websites are created stealthily by the attackers. The web defender is thus limited to reactive strategies that detect and take down malicious sites created by the perpetrators. As we will show, large numbers of malicious websites can stretch the resources of the defender and alter the game play endogenously.

Contribution. The above motivates the current work to develop the Colonel Blotto Web Security (CBWS) framework for analyzing guerrilla warfare on the web. Our contributions in this paper are two-fold:

- First, we develop the CBWS model in Section 3 and analyze in Section 4 the strategies and payoffs of a monopolist attacker under three different combinations of attacker benefit and cost functions, namely: (i) a ratio (proportion) based benefit function with linear costs, (ii) a ratio based benefit function with a fixed cost, and (iii) linear benefit and cost functions. The model generalizes the rudimentary Colonel Blotto Phishing game we introduced in [10].
- Second, we extend our model to evaluate the effect of competition among multiple attackers in Section 5. This is an important departure from the assumption of a monopolist attacker. We show how a duopoly or an oligopoly increases the number of malicious sites created by each attacker, but nonetheless leads to reduced attacker utilities. We also show that collusion yields a higher utility for the attackers.

2 Background

Colonel Blotto is a two-player constant-sum game, where players strategically distribute a finite amount of resources over n battlefields [7,8,17]. The player who expends a higher amount of resources wins a particular battlefield. The game has been largely neglected arguably due to the complexity of its asymmetrical version, until the work by Roberson [34] which successfully characterized the unique equilibrium payoffs under different configurations of resource asymmetry.

Let n be the number of battlefields, where R_a and R_b denote the resources of player a and b such that $R_a \leq R_b$ and π_a and π_b denote the unique equilibrium payoffs of the players measured in the expected proportion on battlefields won. Table 1 then outlines the unique equilibrium payoffs [34].

We refer interested readers to Roberson [34] for details. In essence, player b uses a *stochastic complete coverage* strategy which expends non-zero resources in all battlefields. In case (ii) and (iii), player b will in fact lock down a random subset of battlefields by allocating R_a resources to each of them. On the other hand, player a uses a *stochastic guerrilla strategy* which optimally abandons a random subset of the battlefields. Despite having less resources, player a can

Table 1: Equilibrium payoffs per different resource asymmetry [34].

	Resource Asymmetry	Unique Equilibrium Payoff
case (i)	$\frac{2}{n} \leq \frac{R_a}{R_b} \leq 1$	$\pi_a = \frac{R_a}{2R_b}$, $\pi_b = 1 - \pi_a$
case (ii)	$\frac{1}{n-1} \leq \frac{R_a}{R_b} < \frac{2}{n}$	$\pi_a = \frac{2}{n} - \frac{2R_b}{n^2 R_a}$, $\pi_b = 1 - \pi_a$
case (iii)	$\frac{1}{n} < \frac{R_a}{R_b} < \frac{1}{n-1}$	$\pi_a = \frac{2m-2}{mn^2}$, $\pi_b = 1 - \pi_a$, $m = \lceil \frac{R_a}{R_b - R_a(n-1)} \rceil$
case (iv)	$\frac{R_a}{R_b} \leq \frac{1}{n}$	π_a=0, π_b=1

expect to win a non-zero proportion of the battlefields, except when in case (iv) where player b can trivially lock down all battlefields.

Notice that the proportion of battlefields won by player a is a function of n in the case (ii) and (iii). Kovenock et al. [23] present a *two-stage Colonel Blotto* game which allows the players to create additional battlefields in the 'pre-conflict' stage. They showed that with such possibility, player a will optimally increase the number of battlefields if cost is low and if resource asymmetry falls under case (ii) or (iii). Additional battlefields thin the player b's resources, reducing the number of battlefields he can lock down in the 'conflict' stage. Our earlier work [10] extends this two-stage game by introducing information asymmetry between the players. Specifically, if player b can only detect a fraction of new battlefields created by player a, then player a will automatically win the undetected battlefields. Gupta et al. extends the game to three players and three stages, allowing two defenders to form alliances and transfer resources before the conflict stage, but under conditions of perfect information [19].

3 Colonel Blotto Web Security (CBWS)

We construct the CBWS framework to model asymmetric conflict and guerrilla warfare in web security, with emphasis on resource asymmetry and information asymmetry between the attacker and defender.

Actors $\{a, b\}$. We consider a two-player zero-sum game between the attacker (a) and the defender (Colonel Blotto, b). The defender can be a security vendor or a takedown specialist. Takedown companies are typically contracted by clients, including banks and popular brand owners in the case of phishing, or government agencies in the case of illegal online pharmacies, to remove the malicious or fraudulent sites on the web. On the other hand, the attacker plays to launch new attacks and keep alive their websites.

Asymmetrical Finite Resources $\{R_a, R_b \mid R_a \leq R_b\}$. Finite resources is an important constraint in the context of web security. Furthermore, we assume the attacker (a) to be less resourceful than the defender (Colonel Blotto, b). While this assumption is not needed, such resource asymmetry is reasonable in practice. Defenders such as takedown companies usually maintain good relationships with and can get assistance from the ISPs, law enforcement agencies, registrars

and registries. Resources is thus defined to be technologies (e.g., fast flux skills), infrastructure (e.g., botnet access), time and manpower, *not* financial resources. While the attacker can acquire new resources with financial investment in practice, this is not captured in our framework. Thus, resources are different from the notion of cost. Resources are perishable – unused resources give no value to the players at the end of the game, different from the cost for launching a new attack.

Endogenous Number of Battlefields $\mathbb{S} = \{s_1, s_2, .., s_n\}$. We define a battlefield to be a malicious site with a fully qualified domain name or IP address, or a site on a shared hosting service. We consider different URLs directing to the same malicious site, crafted to evade spam filters or to trick URL-based security toolbars, to be the same battlefield. Defined in this way, creating a battlefield hence involves some costs that can be low (e.g., register a subdomain on a shared hosting service) or high (e.g., register a new domain name, compromise a vulnerable web server). The number of battlefields is endogenous. The attacker creates large numbers of sites to thin the defender's resources, but they come at a cost. We assume the number of battlefields to be bounded by n_{min} and n_{max}.

Unknown Battlefields: Information Asymmetry P_d. The framework is parameterized with an expected probability of detection P_d to model that not all malicious sites are detected by the defender in practice. We are most interested with how P_d interacts with other factors, including the cost-to-benefit ratio of malicious sites and resource asymmetry, in influencing the attacker's decision. P_d can be endogenous and determined by the number of sites the attacker creates. For simplicity, we regard P_d to be exogenous in this paper and expect the attacker to learn about the detection rate through experience.

Detect & Takedown: Action Asymmetry. We model the asymmetrical actions between the defender and attacker in two stages: (i) create–detect, (ii) resist–takedown.

Stage 1: Create–Detect. The game starts with the attacker creating a number of malicious sites (n_a) with an objective to stretch the defender and to increase the victimization rate. As the attacker spam-advertises the sites, some of them will become detected by the defender. In practice, takedown companies reactively learn about malicious attacks through their infrastructures and feeds provided by the ISPs or clearinghouses. We assume that the attacker will realize which of his sites have been detected, denoted as $\mathbb{S}_d$. This is possible as the attacker can refer to blacklists available online (e.g., myWOT.com, PhishTank.com, LegitScript.com) or security warnings in browsers (e.g., Google Safe Browsing feature in FireFox and Chrome).

Stage 2: Resist–Takedown. The attacker and defender then strive to protect or takedown the set of detected malicious sites using their respective resources.

We assume that the attacker will expend all his resources[4] to extend[5] the uptime of the detected sites. Accordingly, $\varepsilon \approx 0$ resources are allocated to the undetected ones. For each given site, the winner is the player who expends a higher amount of resources in this site, either by keeping it alive beyond a threshold of uptime, or taking it down within the same time threshold. As for undetected sites $\forall s \notin \mathbb{S}_d$, the attacker wins with $\varepsilon \approx 0$ resources.

Utilities. Let n_i and $\mathbf{x}_i$ denote the number of malicious sites created and the resource allocations across all sites by player i, and correspondingly by his opponent $-i$. Let $B(\cdot)$ and $C(\cdot)$ denote the benefit and cost functions, and given the exogenous P_d and $\frac{R_a}{R_b}$, the utility of player i can be written as:

$$U_i = B(n_i, n_{-i}, \mathbf{x}_i, \mathbf{x}_{-i}, P_d, \tfrac{R_a}{R_b}) - C(n_i)$$

As aforementioned, the defender will not create any malicious sites (n_b^*=0), and is reactive in this framework. The attacker creates the optimal number of malicious sites n_a^* that maximizes his utility U_a^*. The solution concept we use is the subgame perfect equilibrium. First, we can work out the fraction of undetected sites given P_d, and the expected proportion of battlefields won in the resist–takedown stage $E(\pi_a)$ according to Table 1. Then, solving backwards, the optimization problem of the attacker in the create–detect stage becomes:

$$\max_{n_a} E(U_a|n_a) = B[E(\pi_a) \cdot P_d n_a + (1 - P_d) \cdot n_a] - C(n_a)$$

where

$$E(\pi_a) = \begin{cases} \frac{R_a}{2R_b} & \text{if} \quad n_a \geq \frac{2R_b}{P_d R_a} \\ \frac{2}{P_d n_a} - \frac{2R_b}{(P_d n_a)^2 R_a} & \text{if } \frac{R_b}{P_d R_a} < \ n_a \ < \frac{2R_b}{P_d R_a} \\ 0 & \text{if} \quad n_a \leq \frac{R_b}{P_d R_a} \end{cases}$$

Notice that the framework has left open the choice of benefit and cost functions. We explore a few plausible candidates in Section 4. Notice also that we have simplistically absorbed case (iii) of Table 1 into case (ii). Case (iii) is a relatively small region with points of discontinuity, and has the equilibrium payoffs which equal that of case (ii) as the resource asymmetry reduces.

[4] Recall that we define resources to be technologies, infrastructure, time and manpower, *not* financial resources. Unused resources give no value to the players at the end of the game (use-it-or-lose-it).

[5] For example using the fast flux method that maps a domain name to different IP addresses (of bot machines) by changing the DNS records at a high frequency, making the take down effort difficult [4]. Clearly such technology is only available to the resourceful miscreants. Less resourceful attackers may however also use strategies such as to not resolving a malicious site on every access or temporarily withdrawing from a compromised server to misguide the defenders [4,32]. The APWG found that 10% of phishes were re-activated after being down for more than an hour [4].

4 Analysis: A Monopolist Attacker

We consider three plausible sets of benefit and cost functions of a monopolist attacker. Table 2 shows the utility function and optimal number of malicious sites to create in each model. We first discuss the potential application of each model, before proceeding to analyze the effect of information asymmetry, resource asymmetry and cost-to-benefit ratio on the attacker strategies.

- *Linear Benefit and Cost (LBC).* We start by assuming a linear benefit for having sites with extensive uptime and a linear cost for creating malicious sites. The model offers a straightforward cost-to-benefit analysis from the perspective of a web attacker.
- *Ratio Benefit with Linear Cost (RBLC).* Instead of the absolute number of sites, this model considers the fraction of the sites capable of withstanding prompt removal by the defender. Optimizing the ratio value is appropriate in two cases: (i) if we consider the attacker's intention is to defeat the defender by winning a certain fraction of battlefields, or (ii) if we consider a relatively constant number of gullible victims in practice[6], and that the fraction of sites withstanding detection and takedown is proportional to the fraction of victims an attacker victimize. The model is suitable for modeling attacker competition.
- *Ratio Benefit with Fixed Cost (RBFC).* Same as RBLC. But, instead of linear cost, this model can be appropriate if we consider the situation where the attacker can create a large number of malicious sites with negligible marginal cost.

Figure 1(a), 1(b) and 1(c) plot the LBC, RBLC and RBFC models respectively. Figure 1(d) is a special case of RBLC where the conflict starts with the attacker having n_0 malicious sites that are known to the defender. This corresponds to the model studied in [10], where the attacker decides whether to create additional battlefields given a set of existing ones. Without loss of generality, we represent the cost-to-benefit ratio $k{=}c/b$ in our analysis.[7]

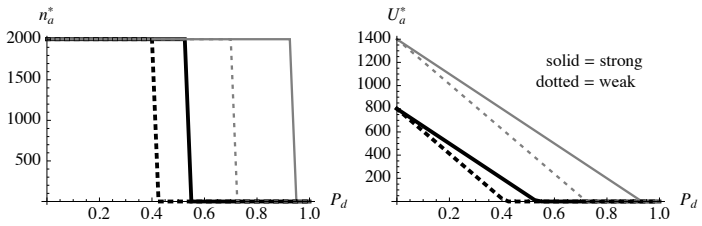
Across the LBC, RBLC and RBFC models, we see that the attacker utility U_a^* falls (mostly linearly) with the detection probability P_d. This speaks to the importance of the defenders to invest in improved technologies to detect malicious websites. On the other hand, when malicious websites can easily evade detection (i.e., $P_d{\to}0$), even weak attackers can obtain significant utility. In fact, in cases with ratio benefits (RBLC and RBFC), the weak attackers can achieve comparable utility levels as the strong attackers.

[6] As victims learn from their experiences, new users become the targets of web perpetrators. Herley and Florêncio estimated a phishing victim rate of 0.37% out of 165 millions online users in the US, and that half of them (0.185%) actually lose money to phishing activities [21].

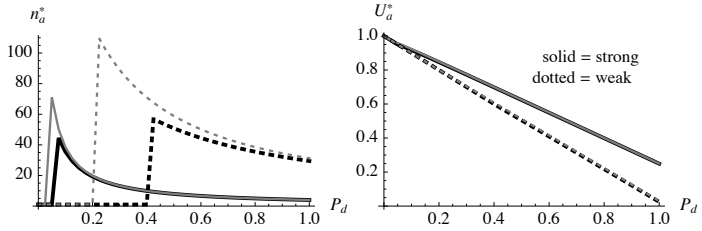
[7] Note that k should be interpreted differently in each model.

	Linear Benefit Cost (LBC)	Ratio Benefit Linear Cost (RBLC)	Ratio Benefit Fixed Cost (RBFC)
Utility U_a	$b[E(\pi_a) \cdot P_d n_a + (1-P_d)n_a] - cn_a$	$\frac{b}{n_a}[E(\pi_a) \cdot P_d n_a + (1-P_d)n_a] - cn_a$	$\frac{b}{n_a}[E(\pi_a) \cdot P_d n_a + (1-P_d)n_a] - c$
let $k{=}c/b$	$E(\pi_a) \cdot P_d n_a + (1-P_d)n_a - kn_a$	$\frac{1}{n_a}[E(\pi_a) \cdot P_d n_a + (1-P_d)n_a] - kn_a$	$\frac{1}{n_a}[E(\pi_a) \cdot P_d n_a + (1-P_d)n_a] - k$
Optimal n_a^*	if $k > 1 - P_d + \frac{1}{t}$	if $k > \frac{32}{27t^2}$	$n_a^* = t$
with $t{=}\frac{2R_b}{P_d R_a}$	$n_a^* = n_{min}$	$n_a^* = n_{min}$	
	else	else	
	$n_a^* = n_{max}$	$n_a^* = \sqrt[3]{t/k + \sqrt{\Delta}} + \sqrt[3]{t/k - \sqrt{\Delta}}$	
		with $\Delta = (\frac{t}{k})^2 + (\frac{2}{3k})^3$ and $\frac{t}{2} \leq n_a^* \leq t$	

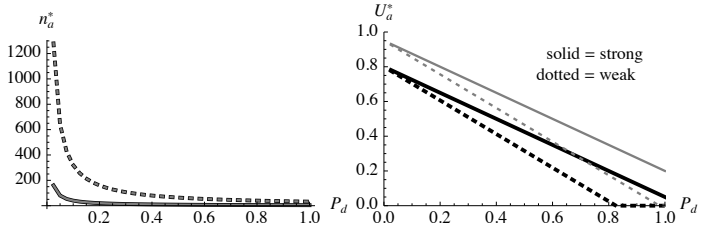
Table 2: Optimal number of malicious sites to create n_a^* and utility U_a^* with different cost and benefit functions. We include the proof for the RBLC model in Appendix A; results for LBC and RBFC are easier to prove, and can be worked out similarly.



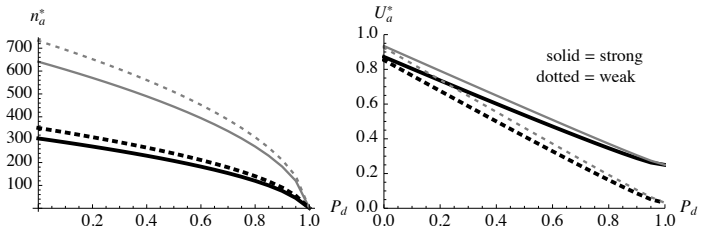
(a) Linear Benefit and Cost (LBC)



(b) Ratio Benefit Linear Cost (RBLC)



(c) Ratio Benefit Fixed Cost (RBFC)



(d) RBLC with $n_0 > 0$

Fig. 1: Optimal number of malicious sites to create n_a^* and the corresponding utility U_a^* of a monopolist attacker. Solid and dotted lines plot the case of a strong attacker with $\frac{R_a}{R_b} = \frac{1}{2}$ and a weak attacker with $\frac{R_a}{R_b} = \frac{1}{16}$. Cost-to-benefit ratio $k = \frac{c}{b}$ decreases going from thick-black to thin-gray lines. $k = \{0.6, 0.3\}$ in subfigure-(a), $\{0.2, 0.05\}$ in (c), and $\{2{\times}10^{-4}, 5{\times}10^{-5}\}$ in (b) and (d). $n_{max} = 2000$ in subfigure-(a). The initial number of battlefields in subfigure-(d) $n_0 = 30$, putting the strong attacker and the weak attacker in case (i) and (ii) of the classical Colonel Blotto game respectively.

4.1 Information Asymmetry, $P_d \to 0, 1$

When all malicious sites can be detected by the defender (i.e., P_d=1), the optimal number of malicious sites to create, n_a^*, depends on both the resource ratio $\frac{R_a}{R_b}$ and cost-to-benefit ratio k=$\frac{c}{b}$ of the attacker. Although n_a^* can be more than 0 even in the case of perfect detection, the U_a^* of the attacker, especially the weak attacker (dotted lines), is minimal as shown in Figure 1 across (a) to (d).

At the same time, we see that the lower the detection probability, the more malicious sites the attacker will want to create across the different models. The effect is most pronounced in the fixed cost model (RBFC) where the optimal number of sites increases quickly as $P_d \to 0$. As for the linear benefit model (LBC), given $k<1$, n_a^* becomes solely bounded by n_{max} as $P_d \to 0$. This is interesting – the attacker will not settle with having a target number or fraction of undetected sites. Instead, he will exploit the weakness in detection to the fullest as each additional undetected site adds to his utility. The same applies to the RBLC model. The number of malicious sites to create increases with decreasing P_d, particularly when $n_0>0$ as shown in Figure 1(d). Without an initial set of battlefields, a decreasing P_d also increases n_a^*. But there exists a threshold where the attacker switches his strategy. As depicted in Figure 1(b), when the detection probability falls below a threshold where $k>\frac{32}{27t^2}$ i.e., when $P_d^2<\frac{27kR_b^2}{8R_a^2}$, the attacker can maximize his utility by creating just n_{min}=1 site.

Across the different models, we also find that the utility gap between a strong and a weak attacker widens as P_d increases. Improving on P_d thus hurts a weak attacker more than a strong attacker, who can leverage his resources to keep alive his malicious sites. This in turn implies that an attacker will do better to up his resources when P_d is high.

4.2 Cost-to-Benefit Ratio, $k \to 0$

An increased cost-to-benefit ratio reduces the optimal number of malicious sites an attacker will create, other than in the case of fixed costs as exemplified by the RBFC model. This can be seen by comparing the thick-dark lines to the thin-gray lines in Figure 1, except 1(c).

Focusing on the RBLC model, we see that the effect of the cost-to-benefit ratio is magnified when P_d is low. This is particularly evident in Figure 1(d) which models the case where the attacker has a set of malicious sites known to the defender at the start of the game, i.e., $n_0>0$. Comparing Figure 1(d) to 1(b), we see that the existence of some known battlefields pushes up the optimal number of malicious sites to create n_a^* dramatically. As the optimal number of sites to create increases, a smaller cost-to-benefit ratio can generate a noticeable saving to the attacker. On the other hand, the saving in utility in Figure 1(b) is negligible due to the relatively small n_a^*. Combining with earlier result, we can thus expect the attacker to optimally vary his strategies to (i) increase his resources to match the defender's if P_d is high, or (ii) lower the cost-to-benefit ratio when he should optimally create larger numbers of malicious sites as P_d decreases.

4.3 Resource Asymmetry, $\frac{R_a}{R_b} \to 0, 1$

Counter-intuitively, we find that the number of malicious sites created by an attacker does not always follow the level of resources at its disposal. In fact, in the RBLC and RBFC models, the weak attacker (dotted lines) may actually create more sites than the strong attacker (solid lines). This is surprising as large-scale web attacks are more often associated with resourceful attackers. For example, the 'Avalanche' gang was found to be responsible for 84,250 out of 126,697 phishing attacks recorded by APWG from June to December 2009 [4].

There are several possible explanations for this apparent contradiction. First, if there is indeed a strong resource asymmetry between the weak attacker and the defender, it is likely for the weak attacker to be operating in a regime where it should either create only n_{min} sites, or to exit the game altogether in practice. In the LBC model, this regime exists for high P_d. In the RBLC model, it exists for low P_d. The stronger the resource asymmetry, the larger the range of these regimes. Interestingly, in the LBC model, the attacker creates few if any sites and realizes little if any positive utility, because most of its sites will be detected by the defender. In contrast, in the RBLC model, the attacker only needs to create a minimal number of sites to realize very high utility, because these sites are highly likely to evade detection. Second, it is possible that competition among attackers may force the weaker attackers out of the game. We now turn to studying the effects of competition.

5 Analysis: Competition among Attackers

Are malicious activities on the web profitable? Back in 2007, Gartner estimated a loss of $3.2 billion due to phishing in the United States with 3.6 million victims and a $886 average per person loss [16]. Researchers have since disputed the astronomical figure. Herley and Florêncio estimate phishing losses in the US amounts to $61 million annually [21]. They argue that phishing is a classic example of the Tragedy of the Commons where the less resourceful attackers suffer from low profitability, and provided a macroscopic analysis.

In this section, we will extend our CBWS framework to evaluate how the presence of competition changes the incentives and strategies of individual attackers. In particular we will integrate Cournot competition into our framework and evaluate how the presence of multiple attackers affects the optimal number of malicious sites to create and the corresponding utility. We consider the case where multiple attackers compete with the same level of resources and that the defender treats the attackers indiscriminately.

5.1 Competitive Colonel Blotto Web Security

Let $n_{a,j}$ denote the number of malicious sites created by attacker j when facing the common defender (Colonel Blotto, b). Consider also that the attackers are homogenous in terms of benefit and cost functions as well as resources $R_{a,j}$.

Adapting from the case of a monopolist attacker, the utility of attacker j in the presence of $m-1$ other attackers, denoted as the group $-j$, can be written as:

$$U_{a,j} = B(n_{a,j}, n_{a,-j}, P_d, \tfrac{R_{a,j}}{R_b}) - C(n_{a,j})$$

We regard a ratio benefit function to be appropriate for evaluating the competition effects, assuming a constant number of victims in practice, and that the attackers compete to increase their share of online malicious sites which proportionally increases their expected victimization rate. Considering Cournot competition where attackers create malicious sites simultaneously, we can write the optimization problem of attacker j in the competitive CBWS framework as:

$$\begin{aligned}&\max_{n_{a,j}} E(U_{a,j}|n_{a,j}, n^*_{a,-j})\\ &= \tfrac{n_{a,j}}{n_{a,j}+n^*_{a,-j}}[E(\pi_{a,j}) \cdot P_d + (1-P_d)] - c \cdot n_{a,j}\end{aligned}$$

We further consider that the defender treats the attackers indiscriminately, and distributes the resources against the attackers equally. Thus, $E(\pi_{a,j})$ is the expected fraction of malicious sites the attacker j keeps alive, out of $P_d n_{a,j}$ he created and being detected in the resist–takedown stage, given his resources $R_{a,j}$ and the defender uses $\frac{R_b}{m}$ resources on him.

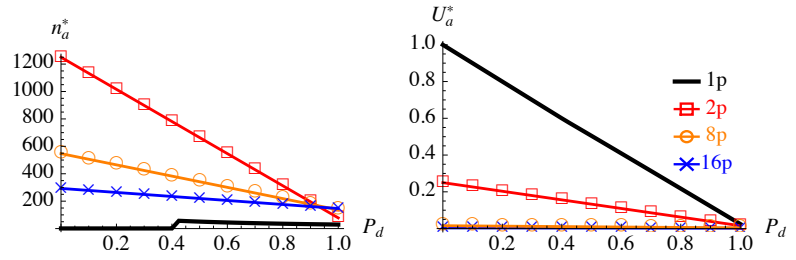
5.2 Oligopoly: Tragedy of the Commons and Collusion

Figure 2 plots the optimal number of malicious sites and the corresponding utility in the presence of 2 (red), 8 (orange) and 16 (blue) competing attackers as compared to the case of a monopolist attacker (black). The resource asymmetry between each attacker and the defender is high with $\frac{R_{a,j}}{R_b} = \frac{1}{16}$. Figure 2(a) and 2(b) shows the optimal n^*_a and U^*_a for individual attackers, while Figure 2(c) and 2(d) shows the summation of the optimal values.

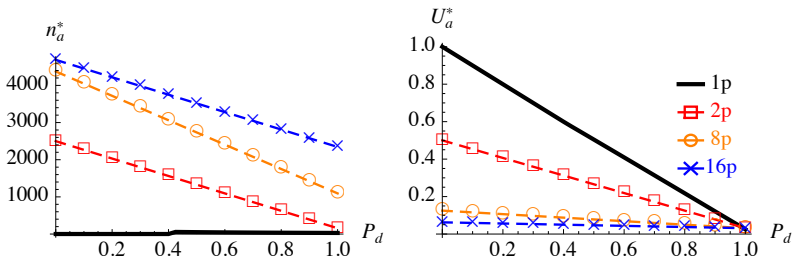
Let us start with the case of duopoly (red lines). Notice that in the presence of Cournot duopoly, both attackers create much more malicious sites individually compared to a monopolist attacker (black line). This drives down the utility of both attackers. The increase in the number of malicious sites to create is intuitive as both of them compete to maximize their respective share of malicious sites with extensive uptime.

The reaction functions of attacker a_1 (solid lines) and a_2 (dotted lines) in Cournot duopoly are plotted in Figure 3. The cost-to-benefit ratio for creating a malicious site k decreases going from thick-black to normal and thin-gray lines. Multiple lines of same thickness and grayscale depict the effect of a decreasing P_d (from left to right and bottom to top). Observe that given the same k, both attackers create the same number of malicious sites $n^*_{a1} = n^*_{a2}$ in equilibrium. However, when ratio k differs, the attacker with a lower k creates much more sites than the other.

Depicted by the orange and blue lines in Figure 2(a), the presence of more than two attackers drives down the optimal number of malicious sites to create per attacker. Yet, while the number of malicious sites created per attacker



(a) n_a^* against P_d (b) U_a^* against P_d



(c) $\sum n_a^*$ against P_d (d) $\sum U_a^*$ against P_d

Fig. 2: Optimal number of malicious sites n_a^* and utility U_a^* in oligopoly. Different colors plot the case of monopoly (black) and Cournot competition between 2 (red), 8 (orange) and 16 (blue) homogenous attackers. Each attacker j has the same level of resources with $\frac{R_{a,j}}{R_b} = \frac{1}{16}$. $k = 2{\times}10^{-4}$. Dashed lines plot the $\sum n_a^*$ and $\sum U_a^*$ of the competing attackers.

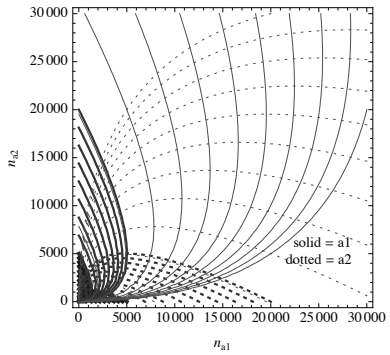


Fig. 3: Number of malicious sites to create n_{a1} and n_{a2} in Cournot duopoly. Solid and dotted lines plot the reaction functions of attacker a_1 and a_2 respectively, with $\frac{R_{a1}}{R_b} = \frac{R_{a2}}{R_b} = \frac{1}{16}$. Cost-to-benefit ratio k decreases going from thick-black to thin-gray lines. Of the lines with the same color and pattern, P_d decreases from 1→0, going from left→right and bottom→top.

reduces, the overall sum of sites created is higher than the case of duopoly as shown in Figure 2(c). Intensified competition reduces the utility of each attacker to be almost zero, see Figure 2(b). Considering a relatively constant number of gullible victims on the web, the presence of multiple attackers thus depresses profitability. As depicted in Figure 2(d), when $P_d \ll 1$, the utility of a single monopolist attacker is even higher than the sum of utility of multiple attackers. This is despite the fact that the sum of resources of multiple attackers, if put together, is manifold higher than that of the monopolist. Essentially, a competitive Colonel Blotto Web Security game exhibits the classic case of Tragedy of Commons [21,20].

The low profitability may drive the less resourceful attackers out of their malicious endeavors or encourage them to collude. We sketch how two colluding attackers will always fare better than two competitors in Appendix B. Given that the sum of utility actually decreases with the number of competing attackers, and that the utility of an attacker increases with more resources (as colluders join forces), collusion is always better than competition for the perpetrators.

In addition to depressing attacker utility, an increased level of competition also reduces the effect of information asymmetry. This can be seen in Figure 2(d) where the sum of utility of 8 (orange) and 16 (blue) competing attackers actually flattens out despite a varying detection rate P_d.

6 Discussion: Implications to Web Defense

Having analyzed the optimal strategies of the attackers, we now turn our attention to potential mitigation measures by the defender. It is important to start by acknowledging that the defender is disadvantaged in the current detect and takedown mode of operation. As captured by our CBWS framework, the defender suffers from not knowing the battlefields created and is limited to reactive measures. We discuss several factors that can potentially mitigate the disadvantages.

Increase cost-to-benefit ratio $k=\frac{c}{b}$. As shown in our analysis for a monopolist attacker, an increased cost-to-benefit ratio of malicious sites will hurt the attacker, especially when the attacker needs to create a large number of sites. Depending on the type of malicious or fraudulent activities, defenders could work to raise the cost c for various support centers, including access to compromised hosts, networking and hosting, fake accounts and human services (e.g., solving CAPTCHA) [36]. Yet, increasing the cost of attacks is not a trivial undertaking. APWG reports that as the weakest registrar or registry beefs up its security features, the attackers will simply move on and exploit the next cheapest or easiest domain name services [4]. Many malicious domain names are bought using stolen credit cards. Worse, a large percentage of malicious sites are actually hosted on compromised servers of innocent and unsuspecting owners. The liability of patching a large number of vulnerable machines may be best assigned to the ISPs [27], but this may not be a straightforward process especially in locations where the risks of excess centralized control are resisted. In parallel,

any effort to reduce the potential benefits reaped from malicious sites can also be helpful to the defender. A comprehensive survey of various profit sources of miscreants, including spamvertised products, ransomware, click fraud, financial fraud and banking theft, can be found in [36]. Disrupting the flow of money to attackers may be an effective measure [36]. For example, researchers found that only three banks were responsible for processing the payments of 95% of spam URLs [26], while intervention by brand holders disrupted the payment to miscreants for months [30].

Increase detection probability P_d. Attackers innovate on techniques to evade detection. For example, popular use of URL shortening services and social media (e.g., Twitter, Facebook posts) increases the challenge of detecting malicious online activities. At the same time, competition among security vendors reduces incentives for data sharing among them [31]. We believe there is an opportunity for open systems based on contributions by volunteers to improve detection probability. Community based services such as Web of Trust (WOT), PhishTank.com and VirusTotal.com are already harnessing user reporting and evaluation against malicious sites. Indeed, studies have found that volunteering efforts in WOT was more comprehensive than automated security evaluations [12], and discussed potential ways for improvement [11]. OpenDNS has called for expert volunteers to help in tagging malicious domains [33]. Features on browsers or mail clients to encourage regular users to report malicious URL links and emails as they encounter them may also be helpful.

Increase resource asymmetry $(1 - \frac{R_a}{R_b})$. Recall that when facing a resourceful defender, it is optimal for a weak attacker to create only minimal malicious sites, or to exit the game altogether. Initiatives to bring together legal, law enforcers, industrial and research communities to pool the resources of the defenders will thus help. In fact, defenders have had also successes in taking down crucial resources of the attackers such as infiltrating the command and control systems to dismantle or take over botnets. Unfortunately compromised machines do not seem to be the resource bottleneck of the attackers; botnets re-emerge despite numerous notable botnet takedown efforts [36].

Discourage attacker collusion. We have seen that intensified attacker competition results in low utility for individual attackers. While it may be unethical to induce such competition, we might have already done so unwittingly. Over-estimated figures of cybercrime profitability widely reported in the media may have served to attract many new attackers. While this may appear to be a positive externality, competition causes a large number of malicious sites, which in turn stresses the defense mechanisms. A more appropriate approach will be to work towards preventing the collusion or collaboration of multiple attackers, particularly those with complementary resources. This may be possible, for example, by going after a specific important piece of infrastructure, or by infiltrating the communication channels (e.g., IRC chatrooms) where underground contacts and bartering take place. FBI's approach to set up a fake market [14] and infiltration into the underground networks may have induced distrust among the attackers. Another possibility to disrupt the frail underground relationship

is to hit on the payment flow between criminals; several currency operators e.g., E-gold and LibertyReserve have been dismantled by law enforcers for money laundering and facilitating payments between criminals [36].

7 Summary

We present a generalized Colonel Blotto Web Security (CBWS) framework for analyzing web security in the presence of resource asymmetry between attacker and defender, and information asymmetry due to the ability of the attacker to create new battlefields (i.e., launch malicious websites) that may be undetected by the defender.

We find that the number of malicious websites created, and the resulting attacker utility, depend on the interactions between a number of different factors. They include the cost and benefit functions associated with website creation, the resource levels of the attacker and defender, the probability that each created website will be detected, and the number of competing attackers.

Even with a resource asymmetry disadvantage, an attacker can still realize significant utilities when information asymmetry is in its favor. In some cases, an attacker can realize a high utility with just a minimal number of websites. In other cases, an attacker may realize little if any utility even after creating a large number of websites.

We also find that competition among the attackers weakens the effects of information asymmetry, and in general, the competing attackers will be worse off, even as more malicious sites are created. The framework can be extended to consider heterogenous battlefields and victims, to model targeted attacks such as spear-phishing, or to consider heterogenous competing attackers. Recent results on heterogeneous Colonel Blotto games [35,24] may be extended to account for information asymmetries such as the creation of unknown new battlefields.

We find that many of the observations made in this paper are not too surprising in retrospect. This suggests that the CBWS framework paints a realistic picture of the dynamics of attack and defense on the web today. We hope our work has laid the foundation for future models and mechanism design – it is high time for us to reflect on the 'whack-a-mole' strategy and to possibly engineer a different, more effective dynamics of web defense.

References

1. Abuse.ch. Kelihos Back In Town Using Fast Flux, Mar 2012. `http://www.abuse.ch/?p=3658`.
2. T. Alpcan and T. Başar. A game theoretic approach to decision and analysis in network intrusion detection. In *Proc. of the 42nd IEEE Conference on Decision and Control*, pages 2595–2600, Dec 2003.
3. E. Altman, K. Avrachenkov, and A. Gamaev. Jamming in wireless networks: the case of several jammers. In *Proc. of the First ICST international conference on Game Theory for Networks*, GameNets'09, pages 585–592. IEEE Press, 2009.

4. Anti-Phishing Working Group. Global phishing survey: Trends and domain name use (2H2009, 2H2010, 2H2011). Half yearly reports available at: `http://www.antiphishing.org/resources.html#apwg`.
5. A. Årnes, K. Sallhammar, K. Haslum, T. Brekne, M. Moe, and S. Knapskog. Real-time risk assessment with network sensors and intrusion detection systems. In *Computational Intelligence and Security*, LNCS, pages 388–397. Springer, 2005.
6. R. Böhme and T. Moore. The iterated weakest link. *IEEE Security & Privacy*, 8(1):53–55, 2010.
7. E. Borel. La théorie du jeu les équations intégrales à noyau symétrique. *Comptes Rendus de l'Académie des Sciences*, 173:1304–1308, 1921. English translation by Savage, L. (1953) The theory of play and integral equations with skew symmetric kernels, Econometrica 21:97–100.
8. E. Borel and J. Ville. Application de la théorie des probabilitiés aux jeux de hasard. 1938. Reprinted in E. Borel, A. Chéron, Théorie mathematique du bridge à la portée de tous, Editions Jacques Gabay, Paris, 1991.
9. R. Chen, J.-M. Park, and J. H. Reed. Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, 2008.
10. P. H. Chia and J. Chuang. Colonel blotto in the phishing war. In *Decision and Game Theory for Security*, LNCS, pages 201–218. Springer, 2011.
11. P. H. Chia and J. Chuang. Community-based web security: complementary roles of the serious and casual contributors. In *Proc. of the 2012 ACM Conference on Computer Supported Cooperative Work (CSCW)*, pages 1023–1032, 2012.
12. P. H. Chia and S. J. Knapskog. Re-evaluating the wisdom of crowds in assessing web security. In *Financial Cryptography and Data Security*, LNCS, pages 299–314. Springer, 2012.
13. D. Clark and K. Konrad. Asymmetric conflict: Weakest link against best shot. *Journal of Conflict Resolution*, 51(3):457–469, 2007.
14. Federal Bureau of Investigation. 'Dark Market' Takedown: Exclusive Cyber Club for Crooks Exposed, Oct 2008. `http://www.fbi.gov/news/stories/2008/october/darkmarket_102008`.
15. N. Fultz and J. Grossklags. Blue versus red: Towards a model of distributed security attacks. In *Financial Cryptography and Data Security*, LNCS. Springer, 2009.
16. Gartner, Inc. Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks, Dec 2007. `http://www.gartner.com/it/page.jsp?id=565125`.
17. O. A. Gross and R. A. Wagner. A continuous colonel blotto game. *RAND Corporation RM–408*, 1950.
18. J. Grossklags, N. Christin, and J. Chuang. Secure or insure? A game-theoretic analysis of information security games. In *Proc. of the 17th International Conference on World Wide Web*. ACM, 2008.
19. A. Gupta, G. Schwartz, C. Langbort, S. S. Sastry, and T. Basar. A three-stage colonel blotto game with applications to cyber-physical security. In *Proc. of American Control Conference (ACC), 2014*, pages 3820 – 3825. IEEE, 2014.
20. C. Herley. Small world: Collisions among attackers in a finite population. In *Workshop on Economics and Information Security*, 2013.
21. C. Herley and D. Florêncio. A profitless endeavor: phishing as tragedy of the commons. In *Proc. of the Workshop on New Security Paradigms (NSPW)*, pages 59–70. ACM, 2008.

22. C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordonez, and M. Tambe. Computing optimal randomized resource allocations for massive security games. In *8th International Conference on Autonomous Agents and Multiagent Systems*, pages 689–696. ACM, 2009.
23. D. Kovenock, M. J. Mauboussin, and B. Roberson. Asymmetric conflicts with endogenous dimensionality. *The Korean Economic Review*, 26:287–305, 2010.
24. D. Kovenock and B. Roberson. Generalizations of the general lotto and colonel blotto games. Cesifo working paper series no. 5291, 2015. Available at: `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2597975`.
25. A. Laszka, G. Horvath, M. Felegyhazi, and L. Buttyan. Flipthem: Modeling targeted attacks with flipit for multiple resources. In *Decision and Game Theory for Security*, LNCS, pages 175–194. Springer, 2014.
26. K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G. M. Voelker, and S. Savage. Click trajectories: End-to-end analysis of the spam value chain. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, SP '11, pages 431–446, Washington, DC, USA, 2011. IEEE Computer Society.
27. D. G. Lichtman and E. A. Posner. Holding internet service providers accountable. *U Chicago Law & Economics, Olin Working Paper No. 217*, July 2004. Available at SSRN: `http://ssrn.com/abstract=573502`.
28. P. Liu and W. Hang. Incentive-based modeling and inference of attacker intent, objectives, and strategies. In *ACM Conference on Computer and Communications Security*, pages 179–189, 2003.
29. M. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys*, 45(3):25, 2013.
30. D. McCoy, H. Dharmdasani, C. Kreibich, G. M. Voelker, and S. Savage. Priceless: The role of payments in abuse-advertised goods. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 845–856, New York, NY, USA, 2012. ACM.
31. T. Moore and R. Clayton. The consequence of noncooperation in the fight against phishing. In *Proc. of the 3rd APWG eCrime Researchers Summit*, pages 1–14, 2008.
32. T. Moore and R. Clayton. The impact of incentives on notice and takedown. In M. Johnson, editor, *Managing Information Risk and the Economics of Security*, 2008.
33. OpenDNS. Calling all elite security experts: Apply to be among the first malware domain taggers, Jul 2012. `http://blog.opendns.com/2012/07/19/calling-all-elite-security-experts-apply-to-be-among-the-first-malware-domain-taggers/`.
34. B. Roberson. The colonel blotto game. *Economic Theory*, 29(1):1–24, Sep 2006.
35. G. Schwartz, P. Loiseau, and S. S. Sastry. The heterogeneous colonel blotto game. In *Proc. of NETGCOOP 2014, International Conference on Network Games, Control and Optimization*, 2014.
36. K. Thomas, D. Huang, D. Wang, E. Bursztein, C. Grier, T. J. Holt, C. Kruegel, D. McCoy, S. Savage, and G. Vigna. Framing dependencies introduced by underground commoditization. In *Workshop on the Economics of Information Security*, 2015.
37. M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest. Flipit: The game of "stealthy takeover". *Journal of Cryptology*, 26(4):655–713, 2013.

38. H. Varian. System reliability and free riding. In L. Camp and S. Lewis, editors, *Economics of Information Security*, volume 12 of *Advances in Information Security*, pages 1–15. Springer, 2004.

A Deriving n_a^* in Ratio Benefit and Linear Cost (RBLC)

To find n_a^*, we first compute the optimal n_a and U_a in the separate cases of $E(\pi_a)$. Denoting $\frac{2R_b}{P_d R_a}$ as t, we have:

case (i): $n_a \geq t$

$$\begin{aligned} U_a^i &= \tfrac{1}{n_a}[P_d n_a \cdot \tfrac{R_a}{2R_b} + (1-P_d)n_a] - kn_a \\ &= \tfrac{1}{t} + (1-P_d) - kn_a \quad \text{[linearly decreasing]} \end{aligned}$$

Thus, $n_a^{i*} = t$, $U_a^{i*} = \frac{1}{t} + (1-P_d) - kt$.

case (ii): $\frac{t}{2} \leq n_a \leq t$

$$\begin{aligned} U_a^{ii} &= \tfrac{2}{n_a} - \tfrac{t}{n_a^2} + (1-P_d) - kn_a \\ U_a^{ii'} &= -\tfrac{2}{n_a^2} + \tfrac{2t}{n_a^3} - k \\ U_a^{ii''} &= \tfrac{4}{n_a^3} - \tfrac{6t}{n_a^4} = \tfrac{2}{n_a^3}(2 - \tfrac{3t}{n_a}) \end{aligned}$$

Given $\frac{t}{2} \leq n_a \leq t$, $U_a^{ii''} < 0$ (i.e., concave). Let $U_a^{ii'} = 0$, we have $kn_a{}^3 + 2n_a - 2t = 0$. To solve for cubic roots using Cardano's method, we first compute $\Delta = (\frac{t}{k})^2 + (\frac{2}{3k})^3$. Since $\Delta > 0$ given $t \geq 2$ and $k > 0$, there is only one real cubic root. If it falls within the range of case (ii), we have $n_a^{ii*} = g_1 + g_2$, where $g_1 = (\frac{t}{k} + \sqrt{\Delta})^{\frac{1}{3}}$ and $g_2 = (\frac{t}{k} - \sqrt{\Delta})^{\frac{1}{3}}$.

case (iv): $n_a \leq \frac{t}{2}$

$$U_a^{iv} = (1-P_d) - kn_a \quad \text{[linearly decreasing]}$$

Let $n_{min} = 0$, we have $n_a^{iv*} = n_{min}$, $U_a^{iv*} = 1 - P_d$. Next, to compare the utility in each case, we compute $U_a^{ii'}$ at the extreme ends of $\frac{t}{2}$ and t:

$$U_a^{ii'}(t) = -\tfrac{2}{(t)^2} + \tfrac{2t}{(t)^3} - k = -k < 0$$

This implies that the utility of case (ii) is always decreasing before entering case (i). In other words, $U_a^{ii*} > U_a^{i*}$.

$$U_a^{ii'}(\tfrac{t}{2}) = -\tfrac{2}{(\frac{t}{2})^2} + \tfrac{2t}{(\frac{t}{2})^3} - k = \tfrac{8}{t^2} - k$$

If $k > \frac{8}{t^2}$, the U_a^{ii} is decreasing at the connecting point with case (iv), implying that $U_a^{iv*} > U_a^{ii*}$. Else, there exists a stationary point in case (ii), and we will test if $U_a^{iv*} < U_a^{ii*}$. Knowing $U_a^{ii'}(g_1 + g_2) = 0$ and that $2g_1g_2 = -\frac{4}{3k}$, we get:

$$g_1{}^2 + g_2{}^2 = \frac{1}{k}(\frac{2t}{g_1+g_2} - \frac{2}{3}) \tag{1}$$

Simplify also U_a^{ii*} with $U_a^{ii'}(g_1 + g_2) = 0$. If $U_a^{iv*} < U_a^{ii*}$:

$$\begin{aligned} 1 - P_d &< \frac{1}{g_1+g_2} - \frac{3k}{2}(g_1 + g_2) + 1 - P_d \\ g_1{}^2 + g_2{}^2 &< \frac{2}{3k} + \frac{4}{3k} = \frac{2}{k} \end{aligned} \tag{2}$$

Substituting (1) into (2), we have $U_a^{iv*} < U_a^{ii*}$ iff $n_a^{ii*} = g_1 + g_2 > \frac{3t}{4}$. Equivalently, we know that $n_a^{ii*} > \frac{3t}{4}$ iff:

$$U_a^{ii'}(\tfrac{3t}{4}) < 0 \quad \text{i.e.,} \quad k < \tfrac{32}{27t^2} \quad \text{[proof completed]}$$

B Showing that $U^*_{collude} > \sum U^*_{compete}$ in Cournot duopoly

We show that the sum of two competing attackers j=$\{1, 2\}$, each has $R_{a,j} = \frac{R_a}{2}$ resources and confronted by $R_{b,j} = \frac{R_b}{2}$ of the defender, is less than the optimal U_a of two colluding attacker (i.e., an attacker with combined resources R_a). We will start with case (i) and (iv) of $E(\pi_{a,j})$, before proceeding to case (ii). We denote $t = \frac{2R_b}{P_d R_a} = \frac{2R_b/2}{P_d R_a/2}$.

<u>case (i) (competing):</u> $n_{a,j} \geq t$

$$\begin{aligned} U^i_{a,j} &= \frac{n_{a,j}}{n_{a,j}+n^*_{a,-j}}[\tfrac{1}{t} + (1 - P_d)] - k \cdot n_{a,j} \\ U^{i'}_{a,j} &= \frac{n^*_{a,-j}}{(n_{a,j}+n^*_{a,-j})^2}[\tfrac{1}{t} + (1 - P_d)] - k \end{aligned}$$

Observe that $U^{i''}_{a,j} < 0$. Solve $U^{i'}_{a,j} = 0$ for $j = \{1, 2\}$. Given the attackers are homogenous, we have $n^{i*}_{a1} = n^{i*}_{a2} = \frac{1}{4k}[\frac{1}{t} + (1 - P_d)]$. Thus, the sum of utility in duopoly $\sum U^{i*}_{a,j} = \frac{1}{2}[\frac{1}{t} + (1 - P_d)]$. This assumes that the stationary point is $\geq t$, or:

$$k \leq \tfrac{1}{4}[\tfrac{1-P_d}{t} + \tfrac{1}{t^2}] \tag{3}$$

Recall from Appendix A that $U^{i*}_{collude} = \frac{1}{t} + (1 - P_d) - kt$, we can easily show that $\sum U^{i*}_{a,j} < U^{i*}_{collude}$ when condition (3) is satisfied. Meanwhile, when the stationary point is out of range, we have $n^{i*}_{a1} = n^{i*}_{a2} = t$ and $\sum U^{i*}_{a,j} = \frac{1}{t} + (1 - P_d) - 2kt$, which is also less than $U^{i*}_{collude}$.

case (iv) (competing): $n_{a,j} \leq \frac{t}{2}$

$$U^{iv}_{a,j} = \frac{n_{a,j}(1-P_d)}{n_{a,j}+n^*_{a,-j}} - k \cdot n_{a,j}$$
$$U^{iv'}_{a,j} = \frac{n^*_{a,-j}(1-P_d)}{(n_{a,j}+n^*_{a,-j})^2} - k$$

Observe that $U^{iv''}_{a,j} < 0$. Solving $U^{iv'}_{a,j} = 0$ for $j = \{1, 2\}$, and given homogenous attackers, we have $n^{iv*}_{a1} = n^{iv*}_{a2} = \frac{1-P_d}{4k}$. Thus, $\sum U^{iv*}_{a,j} = \frac{1}{2}(1 - P_d)$ if the stationary point is $\leq \frac{t}{2}$, or:

$$k \geq \frac{1-P_d}{2t} \tag{4}$$

Else, we have $n^{iv*}_{a1} = n^{iv*}_{a2} = \frac{t}{2}$ and $\sum U^{iv*}_{a,j} = (1 - P_d) - kt$. Notice that in both cases, $\sum U^{iv*}_{a,j} < U^{iv*}_{collude} = (1 - P_d)$.

case (ii) (competing): $\frac{t}{2} \leq n_{a,j} \leq t$

$$U^{ii}_{a,j} = \frac{1}{n_{a,j}+n^*_{a,-j}}[2 - \frac{t}{n_{a,j}}] + \frac{n_{a,j}(1-P_d)}{n_{a,j}+n^*_{a,-j}} - k \cdot n_{a,j}$$
$$U^{ii'}_{a,j} = \frac{[(1-P_d)(n^*_{a,-j})-2](n_{a,j})^2+t[2n_{a,j}+n^*_{a,-j}]}{(n_{a,j})^2(n_{a,j}+n^*_{a,-j})^2} - k$$
$$U^{ii''}_{a,j} = \frac{[2(1-P_d)n^*_{a,-j}-4](n_{a,j})^3+2t[3(n_{a,j})^2+3n_{a,j}n^*_{a,-j}+(n^*_{a,-j})^2]}{-(n_{a,j})^3(n_{a,j}+n^*_{a,-j})^3}$$

Given $n_{a,j} \leq t$, we have $2t(3n_{a,j})^2 \geq 4(n_{a,j})^3$ and $U^{ii''}_{a,j} < 0$. Thus $U^{ii}_{a,j}$ is concave. We then compute $U^{ii'}_{a,j}$ at $n_{a,j} = t$ and $\frac{t}{2}$ to determine if the conditions for which the stationary point lies outside the range of case (ii). We find that $U^{ii'}_{a,j}(t) > 0$ if $k < \frac{1}{4t^2} + \frac{1-P_d}{4t}$, which is exactly condition (3). Thus, if the stationary point is $\geq t$, we have $U^{i*}_{a,j} \geq U^{ii*}_{a,j}$. Correspondingly, we find that $U^{ii'}_{a,j}(\frac{t}{2}) < 0$ if $k > \frac{4}{t^2} + \frac{1-P_d}{2t}$, which is satisfied only if condition (4) is true. Put in words, if the stationary point is $\leq \frac{t}{2}$, we have $U^{iv*}_{a,j} \geq U^{ii*}_{a,j}$.

We have seen that $U^*_{collude} > \sum U^*_{compete}$ in case (i) and (iv) respectively. This implies that we need only to check the utility of the competing attackers when $\frac{1}{4t^2} + \frac{1-P_d}{4t} < k < \frac{4}{t^2} + \frac{1-P_d}{2t}$. Equating $n^{ii*}_{a,j}$ and $n^{ii*}_{a,-j}$, the stationary point can be obtained by solving the cubic equation:

$$0 = 4k(n^{ii*}_{a,j})^3 - (1 - P_d)(n^{ii*}_{a,j})^2 + 2n^{ii*}_{a,j} - 3t$$

and verifying that $\sum U^*_{compete}$ at the cubic root of the above equation is indeed lower than $U^*_{collude}$.