Budapest University of Technology and Economics
Faculty of Electrical Engineering and Informatics
Department of Networked Systems and Services

Analyzing cyber conflicts: battlegrounds, resource asymmetry and real-world data

Scientific Students' Association Report

Author:

Róbert Mucsi

Advisor:

Dr. Gergely Biczók

2022

Contents

Abstract

Cyber-warfare is real: while IT security experts work on protecting their systems, there are also people on the opposite side with malicious intentions, trying to cause harm for their own benefit. As this struggle is relevant from the nation state level down to SMEs, it is of utmost importance to gain insight into its dynamics. A common trait of attacker-defender interactions in such context is the existence of multiple "battlefields" on which the conflict plays out.

Game theory lends itself naturally for the analysis of conflicts; specifically, the Colonel Blotto game is quite suitable to model such a multi-battleground interaction, to characterize the equilibrium behavior, to analyze the resulting payoffs and resource allocations, and to construct guidelines for defenders. A non-trivial step towards this objective is to parametrize the games in a realistic way: we analyze real-world underground cybercrime market datasets, extract parameters for real data, and set up several game instances corresponding to different existing attacker types and a middle-sized company as defender. Using epsilon-equilibrium as a solution concept, progressing from simpler to more elaborate scenarios, we characterize their likely outcome. First, we find that in case of heterogeneous battlefields, it is practically infeasible to defend against all types of attacks. Second, if the attacker has less resources than the defender, she will not be able to win the entire game but might still accomplish his objectives. Third, we show the existence of threshold points from which the defender experiences diminishing returns when increasing his resources allocated to specific battlefields. Last, we discuss the implications of our case studies which may be proven useful for a company planning their cyber-defense.

Chapter 1

Introduction

There is cyber-warfare in the world whether we care about it or not. Companies spend serious amounts of money to defend themselves. On the other hand, attackers are around every corner. Disgruntled employees, hacktivist groups, state- or competitor-sponsored attacks or just a guy with a laptop who has just acquired something dangerous and wants to try it out. And there is an enormous market behind it all, that we cannot even imagine. On the dark side of the Internet there is an ever growing community exchanging exploits for money, services, accounts and much more. This provides a serious source for anyone who wants to cause harm and has enough money to buy what she needs.

Cyberattacks happen and they can have major consequences regarding the fate of a company. For instance, we can say that there is a noticeable negative impact on the stock prices of the victim firm whenever the attack causes interruptions to the services provided by the firm to its customers [13]. The threat potential of a massive DDoS attack on critical Internet infrastructure elements can no longer be ignored. The possible direct and indirect financial loss for many Internet dependent companies must be considered in any complete business risk analysis [8]. A data breach constitutes an exogenous negative shock to a firm's reputation and has considerable short-term impact on firm value and trading. The lack of long-term effect on target firms' performance can be due to firms following the lead of their CEO who they support fully, through which they address this issue properly with necessary policy change [21]. So let it be data breach, DDoS attack or any kind of cyberattack it has an affect on the financial state of the company. In the short run for sure, and can also have negative effects in the long run.

As for global impact, let us see in numbers the cost of cybercrime. The global annual cost of cybercrime is estimated to be around $6 trillion per year, which is more than 1% of the global GDP[1]. There are 30 million SMEs in the USA and over 66% of all SMEs had at least 1 data breach incident between 2018-2020[2]. Just a few interesting stats that prove the reality and importance of this topic. Knowing this, it would be irresponsible to say that it is not a real problem, and something that companies should not care about. Unfortunately, the current mentality is not to prevent these attacks, or at least not for every firm. Maybe caring about this problem but not deeply enough is just a waste of money, so the main attitude is to do it well or not do it at all. Imagine a company spending 10% of their budget on precautionary measures and still suffering some sort of successful attack, now they are behind also with that 10% beyond the losses. Maybe the uncertainty inclines the firms to take the risk in hope of higher profit.

[1] https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/

[2] https://purplesec.us/resources/cyber-security-statistics/#Cybercrime

As Anderson and Moore say, consumers generally reward vendors for adding features, for being first to market, or for being dominant in an existing market – and especially so in platform markets with network externalities. These motivations clash with the task of writing more secure software, which requires time-consuming testing and a focus on simplicity [2]. This implies that there are motives behind having vulnerabilities in systems. Having vulnerabilities in our systems means that we can be the target of an attacker who wants to benefit from this fact. It is clear that to avoid such a scenario, we should take countermeasures. We can picture this two-sided struggle as a "game" of attackers versus defenders, measures versus countermeasures. Fortunately, in game theory there already exists a game called Colonel Blotto, which is particularly suitable to capture this resource allocation problem.

Two years ago the COVID-19 pandemic broke out, which had severe effects on our everyday life; but also on cybercrime. For example, there was a huge increase in the amount of phishing attacks [20]. As we know, most cyberattack campaigns start with a phishing attack. There are descriptions about several cyberattacks from the first few months of the pandemic, which serve as an example for what we are dealing with, and what sort of consequences we can expect, both from the firms' or the users' side. And definitely some sort of prize for the attacker. A few examples: health systems in Champaign Urbana Public Health District (IL, USA) affected by the netwalker ransomware; extortion campaign threatens to infect the recipient with COVID-19 unless a $4,000 bitcoin payment is made; SMS asks recipient to take a mandatory COVID-19 'preparation' test, points to website which downloads malware [14].

So in general, this topic is an ever-growing, never-ending story. Until the world stops going around, there will be people trying to make money in an easier way, or just want to harm their competitors or make a way to get some advantage and so on. Because of all that there is a need to find ways to make your defense better and be prepared for cyberattacks.

In this paper, we analyze multi-battleground cyber-conflicts of attackers and defenders using game theory; specifically the Colonel Blotto game. We model different attacker and defender types and their multi-battleground interaction, characterize their expected equilibrium behavior, analyze the resulting payoffs and resource allocations, and construct guidelines for defenders. Our contribution is multi-fold. First, a non-trivial step we take towards this objective is to parametrize the games in a realistic way: we analyze real-world underground cybercrime and IT security market datasets, extract parameters from real data, and set up several game instances corresponding to different existing attacker types and a middle-sized company as defender. Second, using epsilon-equilibrium as a solution concept, progressing from simpler to more elaborate scenarios, we characterize their likely outcome. We find that in case of heterogeneous battlefields, it is practically infeasible to defend against all type of attacks. Also, if the attacker has less resources than the defender, he will not be able to win the entire game but might still accomplish his objectives. Furthermore, we show the existence of threshold points from which the defender experiences diminishing returns when increasing his resources allocated to specific battlefields. Last, we discuss the implications of our case studies which may be proven for a company planning their cyber-defense.

This paper proceeds as follows. Section 2 presents relevant background and related work. Section 3 describes the data we compiled and used in our model for defining the ratios between the values and cost of the battlefields. Section 4 defines the models from the basic Colonel Blotto situation to the complex data-supported version with the assumptions we used. Section 5 analyzes our models, evaluate its likely equilibrium outcomes, and discusses

practical takeaways from the analysis. Finally, Section 6 outlines potential future work and concludes the paper.

Chapter 2

Background and Related Work

The Colonel Blotto game was first introduced in 1921 by Borel as a two-player constant-sum game, where the players strategically distribute a fixed and symmetrical amount of resources over a finite number of n contests (battlefields). The player who expends a higher amount of resources in a contest wins that particular battlefield, similar to an all-pay auction. The objective of the players is to maximize the number of battlefields won. [6] The case of asymmetric player resources and an arbitrary number of battlefields remained unsolved until 2006. Only then, Roberson [17] completely characterized the equilibria of a two-player Blotto game with any given number of identical battlefields and asymmetric player resources [19] .

Colonel Blotto is widely used in different situations. Commonly used as a metaphor for electoral competition, with two political parties devoting money or resources to attract the support of a fixed number of voters. Just like the voting system works, we can assume that every voter is a separated battlefield, or even a constituency. Even strategic hiring decisions can be supported with the Colonel Blotto game. You have your HR team which is your resource, consuming your budget, and trying to find the most appropriate employee, with the least resource. Even you can compete for the applicant with different companies, and you have to make the best offer (allocating the most valuable possibilities, from their perspective) for them. Furthermore, research and development can also adapt this game, how you allocate your workforce, budget, equipment for finding new solutions and techniques for solving a specific problem, but also have to care about already existing processes that you have develop. All this because in a competitive era you have to keep your advantage or reduce your handicap somehow, which can be achieved with new techniques and methods; similarly to the industrial revolution. Back then, the game was not defined but the problem existed and people did or tried to do this kind of optimization. Last but not least Colonel Blotto is also a great tool in cybersecurity.

The Colonel Blotto game has different parameters which greatly influence the complexity of the game. First, we differentiate between symmetric and asymmetric games. This describes the budget of the players, how much resources they have. We talk about symmetric if their budgets are equa,l or asymmetric if the parties have different amounts. Second, the type of the game is determined by the values of the battlefields, which can be the same for every battlefield or different, so the game would be homogeneous or heterogeneous respectively. Last, the way of the allocations also describes the game. The values that players allocate for the battlefields can have different constraints. The two main variants are the discrete and the continuous. In the first variant, only non-negative integers are allowed to be allocated; in the second variant they can allocate non-negative real numbers.

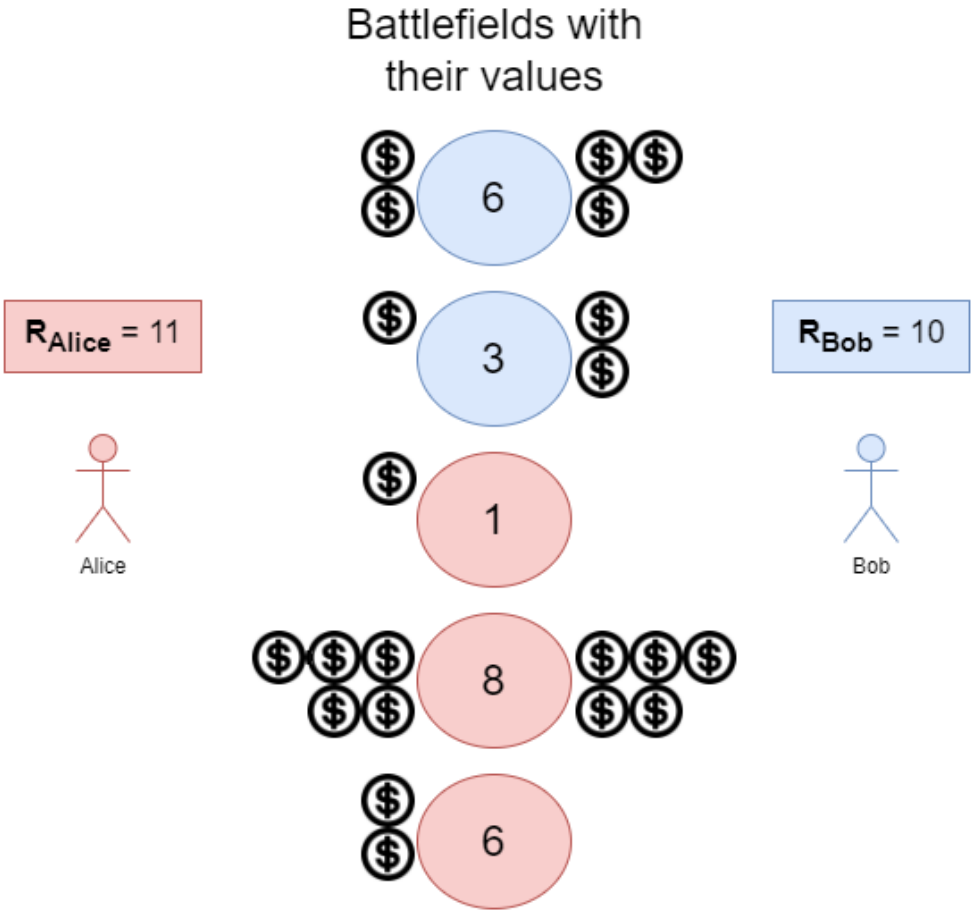

Figure 2.1: Example of a discrete heterogeneous asymmetric Colonel Blotto game

In general, the main rule is that, if both parties allocate the same amount for a battlefield, than one of them wins the draw, there is no splitting. It can be defined otherwise, we will use the situation where (in our interpretation the one with higher amount of resource in total) the defender will win these draws.

Several papers have studied cybersecurity games including Colonel Blotto. These works confirm that, Colonel Blotto is suitable for the purpose of modeling cyber-warfare [11]. Previously written papers are covering a wide range of uses the game. Nochenson and Heimann [16] empirically analyzed different attacker and defender strategies with simulations. Chia at al. [7] studied different plausible cost-benefit functions, which greatly encouraged this paper. Arce et al. [3] modeled a situation with an asymmetric weakest link game between terrorists and counter terrorist forces. Gupta at al. introduced a game, where there are two sides but more than two parties, and parties from the same side are allowed to cooperate in predefined ways [12] . Chia and Chuang defined a game which is consistent with Colonel Blotto and suits the specific problem of phishing very well [6] . Regarding empirical analysis, Min et al. wrote down important observations from the aspect of physical resources [15]. Also there are more complex possibilities how you can expand your model with extra elements such asthe Colonel Blotto version for N players and multi-dimensional private information [10]. The situations and the mapping of the status are unique just like in our model. We focus on a one-on-one game with asymmetric resources, heterogeneous battlefield valuations, and different utility functions according to different attacker models. Also, we compile and utilize different real-world datasets for seeding the models, to achieve empirical results that can help in practical decision-making.

Chapter 3

Datasets

There are several previous papers that used Colonel Blotto for modeling a cybersecurity issue. These are mainly theoretical with justified assumptions and excellent results. However, in this paper the main goal is to find real-life data that illustrates exact real life cybersecurity problems and situations. Using these we could determine which actions we should take and for which actions we should prepare. There are three main dataset we utilized and/or compiled.

Dataset 1: IMPaaS. The first one details a malicious offer that the attacker can use, called Impersonation-as-a-Service (IMPaaS) [5] . Someone can rent an account from a specific location for the platform she desires. In the paper there is a comprehensive analysis on the distribution of prices, which helps a lot estimating the cost of a useful credential. The data collection spans from Dec 2017 to March 2020, involving approximately $262,000$ user profiles. Most user profiles available on the same site, that offers this service and target only one browser, with the top 5% targeting three browsers. Only 35 user profiles report data for more than six browsers in our data. Cookie distribution is similarly skewed. Profiles are distributed globally across 213 countries, and prices range from 0.7 to 96 USD; 50% of the profiles cost at most 5 USD, whereas the priciest 5% are priced above 20 USD [5].

Dataset 2: Exploits. The second dataset concerns vulnerability trading and exploitation. The data is collected first-handedly from a prominent Russian cybercrime market where the trading of the most active attack tools reported by the security industry happens [5]. The dataset contains quality data points: 57 distinct CVE records were included in the list, labeled with price, publication date and so on (see Table 3.1). The market from where this data is originated passed several criteria. It has enforcement of market regulation mechanisms, like punishments, trade guarantors or escrows. Also, the trades that were made on this market is validated by evidence that points toward effective trade mechanisms that foster trading activity. Over and above in this market there were several exploit kits (e.g. Blackhole, RIG, Eleonore) and malware that led to numerous well-documented infection campaigns (e.g. Zeus, Citadel). This confirms the presence of prominent attack tools reported by the industry meaning this data captures real-life scenarios [1].

Table 3.1: Example from the exploit dataset

CVE	CWE	CVSS	CVE Pub Date	Price
CVE-2014-0497	Numeric Errors (CWE-189)	10	05/02/2014	1000$

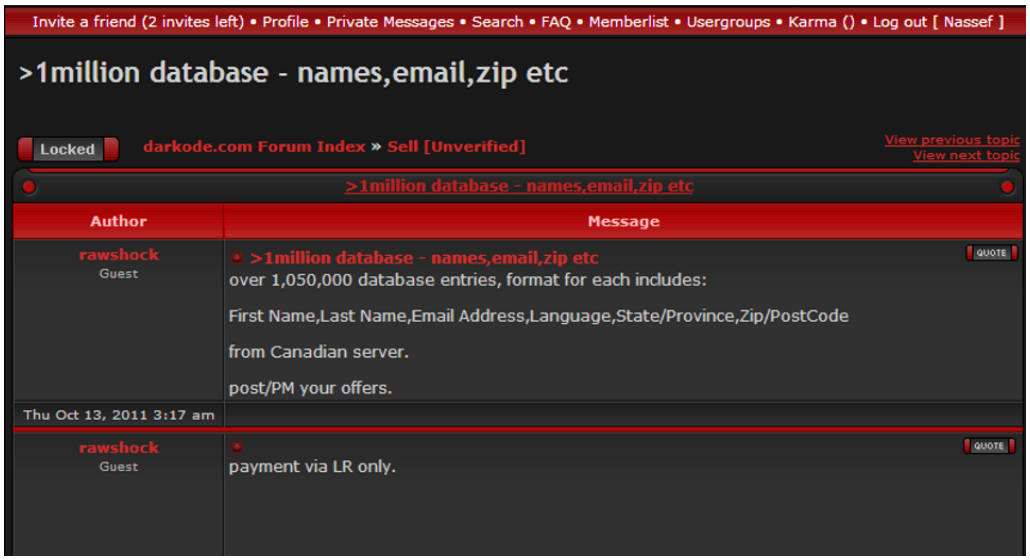

Figure 3.1: Preview screenshot about the ad

New Dataset 3: Darkode. And last but not least there was a forum named darkode. Someone made screenshots about it and made it publicly available[1]. There was a marketplace section, where members were able to post demands and supply so the corresponding party could react and contact each other (see Figure 3.1). This whole forum was moderated by administrators of the forum.

We processed the screenshots manually, and extracted data points to from a novel cybercrime dataset. Similarly to the previous cases, we were trying to evaluate the market and find out how reliable and descriptive that dataset is. Administrators and other users validate each other; and there are two different sections in the forum where people can sell or buy wares: the verified and unverified sections. As their name imply, verified members are more trusted to sell or buy the wares they are looking for. Users can advance by making deals and being loyal members of the forum. Those who just want to make a fraud will be revealed soon and their membership revoked. In our dataset we only use those records which has some sort of confirmation about a transaction (see Figure 3.2). Adhering to this criterion, there are more than 200 hundred posts and more than 40 items that can be considered as made deals. Furthermore, the items advertised on this forum were also identified by CVE-IDs and there were some posts where users talked about well-known exploits and vulnerabilities, which also grants evidence for that the data is related to the real life.

New Dataset 4: Defensive measures. From the defender's side there are countermeasures that she can take. Like educating employees in awareness, or hire someone to do a penetration test on the network or website. Paying for anti-DDoS services, monitoring the user activities etc. There are companies that provide services like these which are suitable for the actions mentioned above. Third parties that provide services like these for example: Intruder[2], TrustNet[3], and CloudFlare[4]. These services are sold in different packages, like paying monthly, monthly-by-user, annually, per use, etc. Therefore, it was essential to find a concrete common ground for the players to use their resources.

As stated above there are several ways that a company can choose to protect themselves or strengthen their defense. It is quite hard to express it quantitatively, both price- and

[1] https://darkode.cybercrime-tracker.net/
[2] https://www.intruder.io/
[3] https://www.trustnetinc.com/
[4] https://www.cloudflare.com/

Figure 3.2: Preview screenshot about the sell

benefit-wise. As stated in this paper, there can be serious problems with the employees' passwords which can lead to serious consequences. An information security awareness project was implemented in a company both by training and by subsequent auditing of the effectiveness and success of this training (which focused on password usage, password quality and compliance of employees with the password policies of the company). The project was conducted in a Turkish company with 2900 white-collar employees. By the end of the whole study, after the second audit (12 months in) the result was remarkable. At the beginning more than 98% of passwords could be brute-froced in 24 hours. By the end, this percentage dropped below 64%, a steady progress [9]. Regarding the aspects of penetration testing there are different techniques to test your system. Austin and Williams made a profound comparison across different techniques [4]. The results suggest that if one has limited time/budget to perform vulnerability discovery, one should conduct automated penetration testing to discover implementation bugs and systematic manual penetration testing to discover design flaws. These are just a few examples for the mentioned mitigation techniques, but there are much more beyond. This dataset collects prices of defensive measures. Note that data sources are not all recent, therefore prices are adjusted to 2022 present value[5]. After the corrections this whole set of data is adequate for our needs to determine the ratio of the different battlefields with different values (see more in Section 4.3).

The first three dataset used, can be found here.[6]

[5] https://www.minneapolisfed.org/about-us/monetary-policy/inflation-calculator

[6] https://drive.google.com/drive/folders/19JfMlXacXht5vyso3NQCphfPmAybxlRF?usp=share_link

Chapter 4

Game Model

4.1 Homogeneous Colonel Blotto

The basic concept of the homogeneous, asymmetric Colonel Blotto game fits quite well to the outlined situation. Let us define the elements of the game in this aspect.

4.1.1 Players

The zero-sum game is played in this case between two parties. There is a company whose main goal is to have some kind of webservice operating, e.g., a social media platform, or even a small webshop. In contrast, there is a malicious actor, an attacker whose goal is to cause harm to the other party. This can be done in the case when the attacker allocates more resources on a battlefield then the defender.

4.1.2 Resources

The resource is money, as a universal resource, as it can be converted into all sorts of services. In most cases, the malicious actor's motives are mostly financial, personal, espionage[1] to prove or force something. Thus, most of the time, the attacker does not have the advantage in resources, compared to its target. According to this, the asymmetry is in the defenders favor. The resources are, R_A and R_D are finite and $R_A \leq R_D$. The resources have the 'use-it-or-lose-it' nature, which means, unused resources are lost at the end of the game.

4.1.3 Battlefields.

Every platform and surface can be a battlefield, where the attacker and the defender can confront. For example, a server's uptime can be a battlefield, over which the participants can fight. The attacker can try to make the site unavailable with a DDoS attack, while the defender is fighting against it with firewalls, or by paying for an anti-DDoS service, which can jump in and take over the traffic. Also, there can be hoax propagation to destroy the reputation of the defender. Making social engineering attacks or using different vulnerabilities to make an exploit, etc. These are just a few examples but there are

[1] https://www.appknox.com/blog/why-do-hackers-hack

a multitude of ways (attack/defense vectors) how the parties can clash. Each way is considered as a different battlefield.

Every battlefield has a value. The sum of the values of the won battlefields are compared at the end and that the winner is whose value is greater. In the basic concept, the game is homogeneous which means that the value of each battlefield are equal. In a heterogeneous game the values are different [19] so that case is even more intricate in addition to, the homogeneous version which was completely unsolved for decades.

4.1.4 Objectives and Contests

The main objective for both the attacker and defender is to maximize the number of battlefields won. This defines their utility functions. Winning the battlefield is the same for both parties, just allocating more resources to it than the opponent. This implies that, for the appropriate amount of money an attacker can buy a zero-day exploit, or pay off an insider to help. At the same time, a defender can announce bug bounty programs, and treat the employees properly not to betray the company. To confirm the previous statement according to which the defender is more resourceful we assume, if there is a draw in resource allocation then the defender wins the affected battlefields. Let $r_{i,b}$ denote the amount of resources that player $i \in \{A, D\}$ allocated to the battlefield b . So then $\lambda_{i,b}$ will take the value of 1 if player i won the battlefield and 0 otherwise.

$$\lambda_{i,b}(r_{i,b}, r_{-i,b}) = \begin{cases} 0 \text{ if } r_{i,b} < r_{-i,b} \\ 1 \text{ if } r_{i,b} > r_{-i,b} \end{cases}$$

As previously mentioned, the game is symmetric: players have an identical objective on each battlefield (allocate more than the other to win) thus the utility functions of the players are similar.

$$U_i(\{r_i, n_i\}, \{r_{-i}, n_{-i}\}) = \frac{1}{n} \sum_{b \in B} \lambda_{i,b} \tag{4.1}$$

So this is how the basic Colonel Blotto game fits on our situation. Already at this point, we can make some statements about the model. We know that the weaker player has better chances if she is able to broaden the attack surface and open as many battlefields as possible [17]. So even though the defender has advantage in the amount of resource, but that advantage is fading away when there are a huge amount of battlefields. In our model, the game is symmetric and of full information: both parties are conscious of the battlefields and their valuation (unlike the Colonel Blotto Phising game [6]).

The already introduced utility function fits the defender and also the attacker. Examine firstly for the attacker. It depicts a hacktivist group's mentality, when the player does not even care about the values of the battlefields, just wants to overcome its opponent as much as possible and win. For hacktivists the battlefields are just proving grounds where they can show that they can defeat the other parties; it counts as a considerable win even if the losses caused are not substantial. From the defenders point of view, they want to win the overall game. They might lose some battlefields, but what matters to them is the aggregate game; this is the most common mindset for companies. As we can see in real life, there are several data breaches and successful attacks against companies, they are reacting to them, but still stay in the game afterwards.

However, there are several other aspects that can modify a real life scenario that we can not cover with this simple concept. The first main remark is that, the utility function represents the motives of the players. For this purpose we defined a quite simple function claiming that, winning more is the better. But real life is often more complex. As we mentioned before, the reasons behind an attack can vary, and also the defenders' approach can be diverse. We classify the attackers into classes simlarly to [18], and define utility functions per class.

$$U_i(\{r_i, n_i\}, \{r_{-i}, n_{-i}\}) = \begin{cases} 1 \text{ if } \sum_{b \in B} \lambda_{i,b}(r_{i,b}, r_{-i,b}) \geq 1 \\ 0 \text{ if } \sum_{b \in B} \lambda_{i,b}(r_{i,b}, r_{-i,b}) = 0 \end{cases} \tag{4.2}$$

According to Equation 4.2 this attacker's main goal is only winning a single battlefield. This characteristic is frequent in the case of script kiddies and disgruntled employees. The motive behind can be different for these two attacker classes but the goal is common. A script kiddie would try to win a battlefield somehow, for self-justification, or to prove something to upper hacker circles. On the other hand, a disgruntled employee wants to hurt its previous employer, or profit from causing some loss to them. These could be achieved easily by only prevailing on one battlefield. (Note that a disgruntled employee can have insider information about the system, can have unrevoked permissions that can help him in reaching their objectives. These factors do not appear in this model but will be discussed later.)

As a defender, winning the majority of the battlefields is not necessarily the optimal strategy. For instance, you secured your system so as no illegal outsider can access any information, but the public service is unreachable owing to a denial of service attack. From the financial aspect, this would be a lethal mistake against an aggressive attacker with the needed background. Also there can be companies who consider that they are not up against attackers like this, so this is the main reason that different companies may be represented with different utility functions.

According to the above mentioned reasons we need to define a utility function for the companies who want a comprehensive protection: winning each battleground, not only the overall game.

$$U_i(\{r_i, n_i\}, \{r_{-i}, n_{-i}\}) = \begin{cases} 1 \text{ if } \sum_{b \in B} \lambda_{i,b}(r_{i,b}, r_{-i,b}) = n \\ 0 \text{ if } \sum_{b \in B} \lambda_{i,b}(r_{i,b}, r_{-i,b}) < n \end{cases} \tag{4.3}$$

Note that these functions only operate with the number of battlefields won, not with the value of the battlefield. This is because of the homogeneity of the game, as every battlefield has the same value; thus only the number of battlefields won (defined by λ) matters.

4.2 Heterogeneous Colonel Blotto

In real life, different battlefields can have diverse valuations. Just for instance, the attacker is able to profit from distributing several scamming spam emails in the name of the company. There is a chance for the attacker to commit a successful fraud but the expected value is quite low. Not zero, because that would result in the disappearance of scam, but much less compared to a zero-day exploit. This implies that there are different value groups for battlefields [17, 19].

Table 4.1: Notations

Notation	Meaning
n	notes the amount of battlefield, or the n-th battlefield
i and $-i$	i notes one player from the two, $-i$ notes the other
$b \in B$	b is a battlefield from the set of battlefields B
$r_{i,b}$	notes the amount of resource (r) that player i allocated to b battlefield
$\lambda_{i,b}$	notes that, whether player i won the b battlefield. 1 if yes 0 if no.
V_b	V notes the value vector of the battlefields, indexed with $_b$ means the value of the b battlefield

The utility functions from the previous section are fitting to this model as well. Representing the script kiddie or the disgruntled employee, causing loss of any kind is the goal of the attacker. Even the defender's approach is suitable: winning all battlefields also implies that she does not suffer any losses. However, real life is not so black and white. With the diversity of the battlefields there can be several ways to win the game: owning the few biggest battlefields to have the bigger portion of the obtainable value or allocating according to our opponent's strategy to win only those battlefields that she wants to win, allocating at random, and so on. Another strategy should be taken into the formula: the attacker's goal is to cause the largest possible harm or loss to the defender. This scenario can be matched to the state sponsored actor or the cybercrime organization attacker model. Some sort of competitor who gains an advantage of any kind from its opponents drawbacks.

To represent the above let us introduce a new utility function which aims at causing as big harm as possible (and conversely, protecting as many aggregate value as possible):

$$U_i(\{r_i, n_i\}, \{r_{-i}, n_{-i}\}) = \sum_{b \in B} \lambda_{-i,b}(r_{i,b}, r_{-i,b}) * V_b. \tag{4.4}$$

After defining all interesting utility functions, we provide a brief summary about the notations used in Table 4.1.

4.3 Game parameters from the datasets

Based on the three cybercrime datasets we noted that products accessible to would-be attackers are priced in a way that follows market thinking. Therefore, the assumption that the ratio of the corresponding battlefield's values have the same ratio as the prices of the respective attack tools do. If we think about, this is absolutely plausible: if the ratio differed, there would be at least one attack mode, that is more profitable than the others so as the appearance of those attacks would multiply at a high rate owing to its profitability; we have not found any reports on such phenomenon.

The differentiated ratios of the battlefields are defined by using the datasets processed before. The first and most inexpensive move that an attacker can perform is trying to do a fraud in the company's name or spread some sort of fake news about the company. For both actions the attacker needs a bunch of email addresses for which she will send the spams. In our dataset we found items for sale that are fit for these purposes: these mainly originated from smaller or bigger data breaches. Such email addresses are not sold individually but in batches: the approximate mean price for 1 million addresses is about 500$ (see, e.g., Figure 4.1).

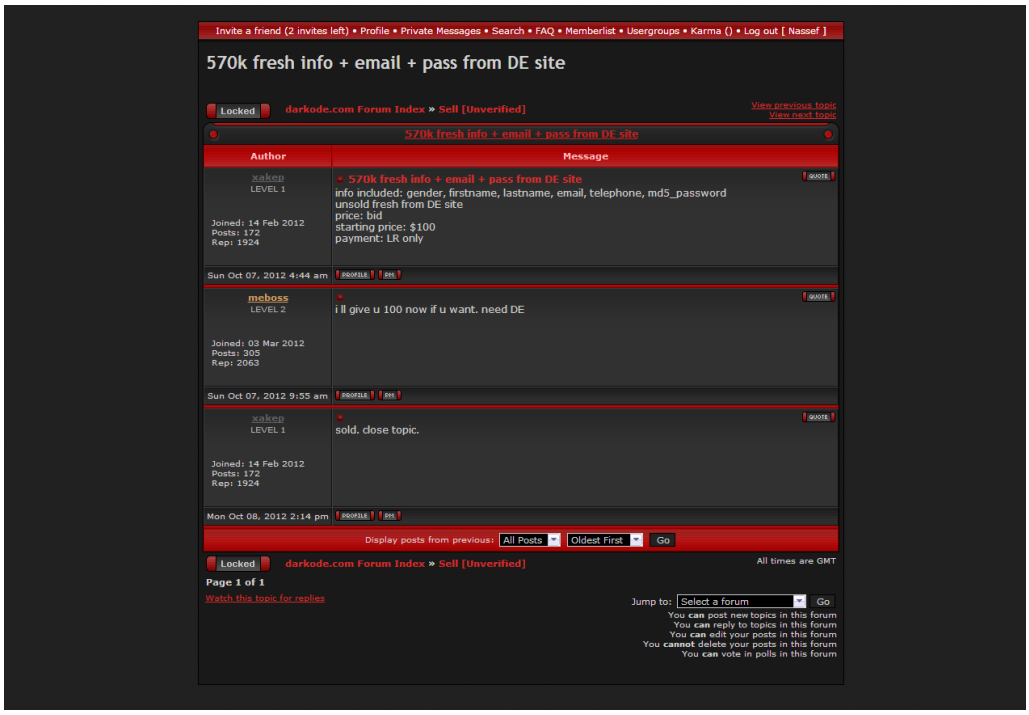

Figure 4.1: Preview screenshot about email addresses

The next significant items in the lists are the services and tools offered for sale are those needed for a DDoS attack. Such an attack can be accomplished by the attacker herself or she can buy a service package. The cost can vary depending on the way how it is executed. Factoring in the variations in price, this type of attack can be done against a medium-sized company for 2000$ (see Figure 4.2).

Adding to these, there can be different vulnerabilities in the system, by the lax IT operation policies of the defender company's or by the technology platforms they use. You can buy a single exploit of a known vulnerability, a zero-day (they are rare, see Figure 4.3) or a complete exploit kit; the cost may vary (see Table 4.2) but the mean price is around 4000$.

These attacks are originated from the outside, but it is easier if we can attack a system from the inside. Enlisting an insider or even just an insider account is not an easy task. It is very resource consuming, be it money or time. Buying every possible breached database and hoping that it will contain a credential we can use is generally not practical. You can try social engineering attacks but they might be expensive, and even, it can carry the risk of letting the target know someone is planning an attack. The another way is to bribe someone but it is very risky, resource consuming and uncertain. All together these make

Table 4.2: Zero-day vulnerabilities from the dataset

CVE	CWE	CVSS	CVE Pub Date	Pub Date on Darkode	Price
CVE-2014-0497	Numeric Errors (CWE-189)	10	05/02/2014	23/03/2014	1000$
CVE-2013-3918	Buffer Errors (CWE-119)	9	12/11/2013	20/12/2013	8000$
CVE-2010-0886	Insufficient Information (NVD-CWE-noinfo)	10	20/04/2010	23/03/2011	2000$

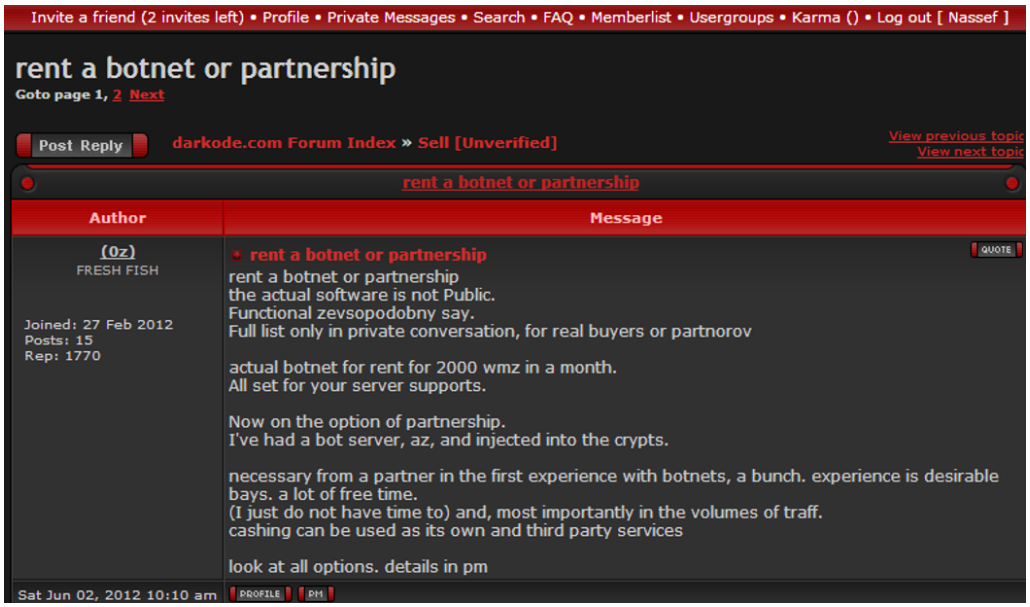

Figure 4.2: Screenshot on renting a botnet

Figure 4.3: Preview screenshot about a zero day exploit

this way of attacking the most expensive by defining it as the sum of every previous attack plus 1000$ to the exploit price: like zero-days multiplied by 2 to account for uncertainty. This comes out as 15000$ in total, for enlisting an insider. This equlas to 30 million credential pairs, a plausible equivalent value.

We also performed the same analysis concerning the defender's battlefields. The different offers and prices that can be found were the normative and we looked for parameters suitable for a medium sized company. These prices helped define the budget of the game. This task was not trivial, as for defenders there will be overlaps between different battlefields and countermeasures taken. E.g., mitigating the threat of vulnerabilities made by the company's developers can have effect on the stability of the system, thus it will be more resistant to DDoS attacks. This is a really complex area, and there are several possibilities to broaden the field of research. As a starting point we assumed that the company entrusted a third party with the management of their system through a service called managed security. We treat its price as fixed, not thinking about whether the third

party carries out its task properly. (Potential future work could include the third party making mistakes with a probability.) Adding to these, there are anti-DDoS services that can be purchased (e.g., Cloudflare). Educating your employees via awareness training regularly, and doing penetrations tests on your systems round out the usual set of standard defensive measures. The prices for these actions are coming from the different offers and prices found on the public web. Of course, when analyzing likely attacker-defender outcomes, we allow for some variations in monetary parameters, while still observing realistic minimum and maximum values based on our data.

Chapter 5

Analysis

When we plan to analyze this model there are several different sides from where we can approach. Firstly there is the expected payoff for the players. It can vary depending on the resource ratio between the parties which means who wins the game and by how much. Also there are the homogeneous and heterogeneous versions of the game which we analyze in this paper. Secondly there are the utility functions that we defined previously. We are investigating how different attackers can prevail, which means in our terms that analyzing the expected payoff's and the utility functions' relation with different parameters.

For the equilibrium analysis we ran simulations with the code and algorithm defined in [22]. This gives us an efficient computational method finding an *epsilon equilibrium*. Such an equilibrium is the likely outcome of a given attacker-defender game instance. The difference compared to a simple Nash Equilibrium is computational: we seek mutual best-responses from attacker and defender while allowing a small incentive for unilateral deviation to exist. This speeds up computation to a tolerable level; such near-equilibrium is the *de facto* solution concept in complicated games.

5.1 Homogeneous expected payoff

As the game is defined, when the players allocate the same amount of resource to a battlefield the defender is the winner. This means some sort of advantage for the defender but we can live this assumption, because in real life scenarios, allocating the same amount of money somewhere could easily mean that the winner is that who comes first, and in this case the defender is the one who was there first so she got the advantage. When analyzing the expected payoff it can be seen that the when the number of battlefields and the amount of resources are approximately the same in scale, this clause can mean a huge benefit for the defender. It is because that, when the parties managing their resources the attacker has to add 1 to the battlefield to achieve the same result as the defender. Allocating 0 to a battlefield from both parties to a battlefield means win for the defender and loss for the attacker. She has to spend to win. To eliminate this advantage the amount of allocatable resources should be two orders of magnitude larger than the number of battlefields, e.g., 100 battlefields for $10,000$ resource units.

In the homogeneous case the parameters were the following. Number of battlefields was set to 100, the resource amount to $15,000$ at the beginning for both parties and every battlefield's value to 1. It is important that the ratio of the players' resources greatly

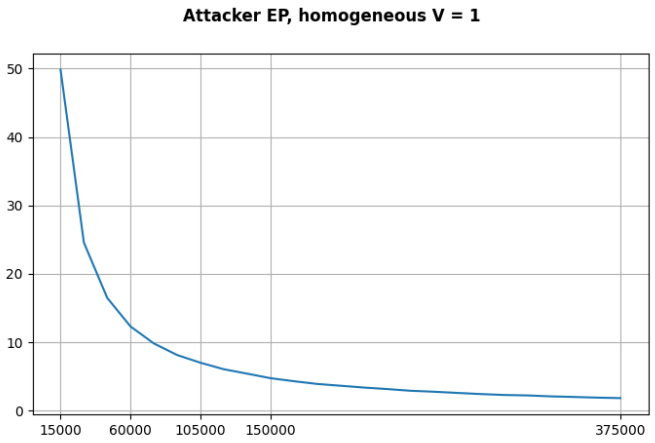

Figure 5.1: The attacker's expected payoff in a case where N = 100 and $\frac{R_A}{R_D}$ starts from $\frac{15000}{15000}$ and every battlefield's value is 1. X axis defender's total resource amount, Y axis percentage of the total amount of values, that the player can win (%).

influence the expected payoff (following Roberson [17]); the case we are investigating is that when the ratio is between these boundaries:

$$\frac{2}{N} \geq \frac{R_A}{R_D} \geq 1 \tag{5.1}$$

So we started from the upper bound. As expected when both parties had the same amount of resource there was only a small difference in the expected payoff which is caused by the advantage of the defender. As the resource advantage of the defender is increasing the expected payoff is also increasing proportionally, which is justified by the fact that the game is highly uniform. These results provide the fundamental background for more complex analysis, and grant possibility to expand it freely to approximate real life scenarios.

5.1.1 Attacker's utility functions

The utility function represents the strategy of the player, trying to map the motives that she wants to achieve. As discussed earlier in homogeneous version there are two utility function that we analyze.

The first utility about maximizing the amount of battlefields won (Equation 4.1). This is like some sort of hacktivist group that has a moderate resource budget and skilled members. The goal is winning the game overall. This is a bit harder one. Because of the advantage of the defender by winning every tie, and the resource asymmetry in the defender's favor, it makes it extremely hard to win as an attacker. The more you have the more you get as the change of the expected payoff is proportional.

The another one is the script kiddie/disgruntled employee's utility function when the attacker's motive is only to cause any kind of harm (Equation 4.2). In this case the attacker is not so resourceful so the main part where we should focus is around $\frac{2}{N}$. Here the expected payoff is going under 1 which means there are cases in which the attacker is unable to win any battlefield. Accordingly this means that, as in theoretical aspects winning the game totally is impossible when the $\frac{R_A}{R_D} > \frac{1}{2}$. However, maximizing the utility function is an absolutely feasible problem. The utility function is maximizable with

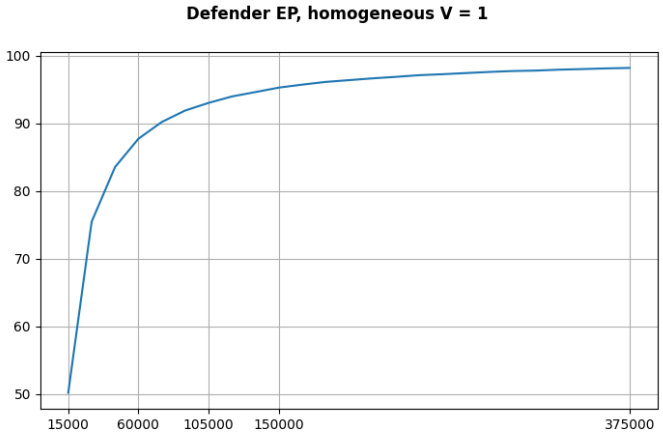

Figure 5.2: The defender's expected payoff in a case where N = 100 and $\frac{R_A}{R_D}$ starts from $\frac{15000}{15000}$ and every battlefield's value is 1. X axis defender's total resource amount, Y axis percentage of the total amount of values, that the player can win (%).

winning just 1 battlefield, but as mentioned previously, when the resource asymmetry is high enough, this also can be a hard problem.

It is absolutely plausible that winning the game (by definition) can be a goal for the attacker only if the resource ratio is around 1. Just like in real life, winning as an attacker would mean that the defender loses, meanwhile winning as a defender is to survive the attack and take some but preferably minimal losses.

5.1.2 Defender's utility functions

The defender has advantage in this game, but also winning is more crucial as a defender than an attacker. Losing as an attacker in the worst case means that you spent your budget but did not receive any payoff. In real life this would be a bit different as allocating your money for an attack would mean, e.g., buying an exploit kit. This means that after the game you still own the exploit kit and you can reuse it so its value is still present. This implies that there would be a reason to somehow analyze the case when there are multiple defenders and one or more attackers and using the same attacks against the defenders like this, so the resource they allocate can be used against every defender.

Losing as a defender in the worst case means that you spent your budget and took a loss so high that the company's fate is sealed. This is not impossible but really hard to reach to that point, in normal cases this will not occur, and the main scenario is that being successful - winning the game - in defending is easier than in attacking.

The first utility is the same as in the attacker's case, maximizing the battlefields won (Equation 4.1). In this interpretation this is an average company that deals with the problem of IT security. So we can say that as in this scenario they will have bigger amount of resource to allocate which can lead to definitely winning the game. That maximizes the utility function, also this utility can be maximized in that case if the player using this utility has a huge amount of resource. Even resource advantage or just having approximately high amount of resource compared to the opponent's budget.

The second utility function that is mapped to the defender is a very well-defined goal (Equation 4.3), which says that the main goal is winning every battlefield. This as a

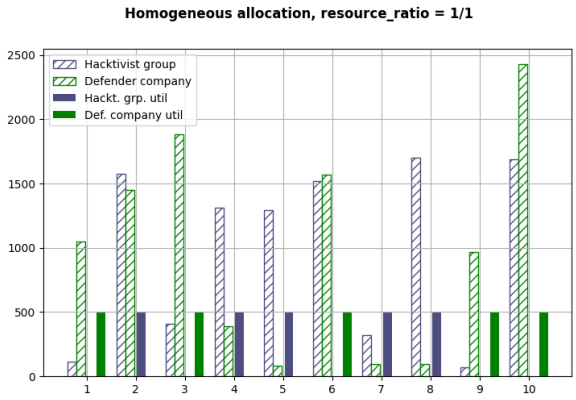

Figure 5.3: Homogeneous resource allocation when the resource ratio is $\frac{1}{1}$. X axis serial number of the battlefield, Y axis Values to win or spent ($).

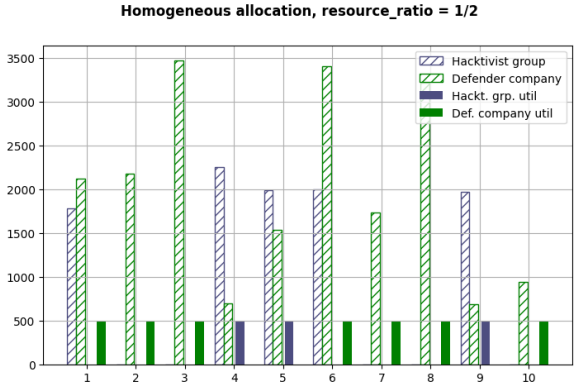

Figure 5.4: Homogeneous resource allocation when the resource ratio is $\frac{1}{2}$. X axis serial number of the battlefield, Y axis Values to win or spent ($).

stronger condition than just winning the overall Colonel Blotto game—satisfying this function is extremely hard as it requires a very big resource advantage. The most certain version is having more resources than $N * R_A$: this is the case when someone is able to allocate more resource to each battlefield than the enemy's total budget. Choosing this safe way demands a high price, but grants 100% chance of dominating the game. This is a typical option for those companies that have the budget for this and leakage or any kind of successful hacker attack can ruin the future of the company (e.g., companies in the military industry).

5.2 Example allocation for homogeneous case and equilibrium analysis

To present the game from closer, and also the tactics and the effect of changing the amount of resources in this section we will examine some games' outcome. Also talking about the relevant utilities to see how succesfull the players were, with the epsilon equlibria strategy. These simulations are sampled from the ones we get the expected payoffs, in a representative manner. Every battlefield is the same for the players, which means their values are 1. We sampled 10 battlefields with different resource ratios.

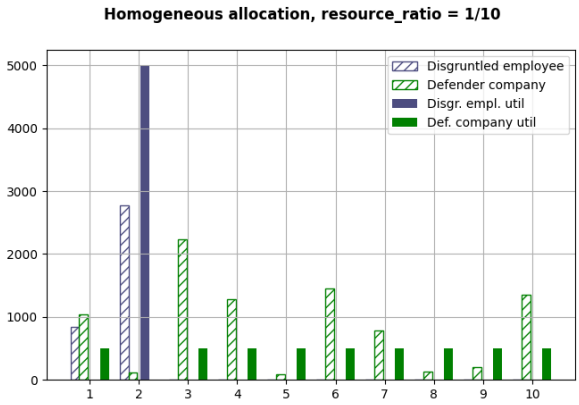

Figure 5.5: Homogeneous resource allocation when the resource ratio is $\frac{1}{10}$. X axis serial number of the battlefield, Y axis Values to win or spent ($).

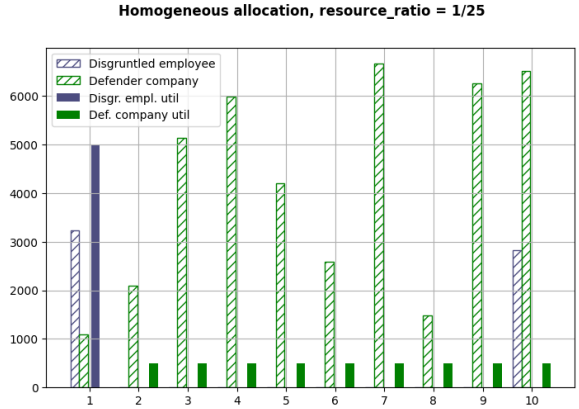

Figure 5.6: Homogeneous resource allocation when the resource ratio is $\frac{1}{25}$. X axis serial number of the battlefield, Y axis Values to win or spent ($).

First, we start with those cases where the resources are close to be the same. Maybe some hacktivist groups can be this resourceful because of their skilled members or they can have bigger amount of money from some sources. In these cases the two parties are in a quite even situation. In Figure 5.3 we can see the case, when both players had the same amount of resource and the expected payoffs at this point are around 50% in both cases. Figure 5.3 supports this expectation, because both the attacker and the defender wins 5 battlefields. Regarding their utility functions we can see the filled bars which is scaled to be presented on the same figure properly. As we discussed earlier the hacktivist group's utility is the number of the won battlefields, which means their main goal is to win. In this case its a draw (in this game) between them and the defender company. The defender company has the same utility. There is no clear winner, but I think causing this serious damage to a company is a bigger win for the hacktivist then to the company.

In Figure 5.4 the defender has twice as much resources to spend. The expected payoff is around 75-25% for the defender's favor. This assumption seems to be fulfilled, because the defender won 7 battlefields and the attacker only 3, which is quite close to this number. After several repeats in total it would be 7.5 and 2.5 in average. In total this means that the defender managed to win, despite some losses, but it was calculated into her strategy. Also, the hacktivist group earned some utility, but did not manage to win: it was impossible to do so with the resource disadvantage.

Now let us examine the case when the resource ratio becomes larger in the favor of the defender. These are those opportunities which are available for a disgruntled employee or a script kiddie. As we know by motivation, these attackers are absolutely satisfied with the outcome if there is at least one battlefield in which they can beat the company, and we can see there is one in both cases despite of the huge disadvantage. As mentioned before, this is a sampled dataset from the whole game, but there were battlefields in which the attacker won: there is one in Figure 5.5 and 5.6. And it can be only a small loss to the company but a loss that it can't fend off, because as shown in the expected payoff, there must be a huge advantage to make the attacker's payoff less then 1. Also, not shown in the figures are the utility of a company that is trying to set up an impenetrable defense (Equation 4.3). The reason is that, its utility would be 0 in all cases: until the attacker can win at least 1 battlefield the defender will never have higher utility than 0. As stated before this is only possible for sure if the defender's resource amount is at least N times greater than the attacker's. $\frac{1}{N} > \frac{R_A}{R_D}$.

So in total it can be said the homogeneous battlefield analysis supports the expected payoff's statements. In total, an average company whose main goal is not to lose the whole game, or not to lose that hard, these goals seem achievable.

5.3 Heterogeneous expected payoff

When analyzing the heterogeneous version there were 2 different scenarios that we aimed to investigate. A simple heterogeneous version, that differs in the valuation of the battlefields (Equation 4.4); and a version in which the valuation of the battlefields is supported by the datasets discussed earlier. In the first case there are 400 battlefields with the value vector $V(1, 2, 3, 4)$, meaning 100 battlefields of each value. When we defined the values by the dataset there were 480 battlefields and the value vector $V(1, 4, 8, 30)$. (Motivated by the fact, that a spam campaign could cause significantly less harm than access to an insider's account.)

We had two main corollaries regarding the heterogeneous game. The first one is that it will modify the chances in the weaker (less resourceful) player's favor. The second one is that the expected payoff's change will not be so consistent and proportional like in the homogeneous version, caused by the gaps in between the battlefields' valuations.

Important remark 1 on the edge of the boundary, around $\frac{2}{N}$ the expected payoff of the attacker does not go under 1, which means that it is more favorable for the attacker just as we expected.

Important remark 2, that the expected payoff is very similar to the previous case, there are no outlier data, it is strictly monotonically decreasing. The answer can be found in the strategy they use.

$$F_{A_i}(x) := \left(1 - \frac{1}{\lambda}\right) + \frac{x}{2\frac{v_i}{V_n}\lambda}\frac{1}{\lambda}, \forall x \in [0, 2\frac{v_i}{V_n}\lambda]$$

$$F_{B_i(x)} := \frac{x}{2\frac{v_i}{V_n}\lambda}\frac{1}{\lambda}, \forall x \in [0, 2\frac{v_i}{V_n}\lambda]$$

[22]

Player A is the attacker with less resource and B is the defender with more resource. Here in these equations the notations are the following. λ is the ratio of the players resources.

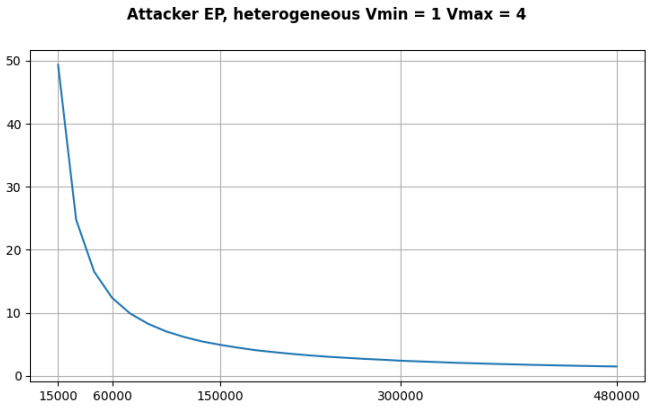

Figure 5.7: The attacker's expected payoff in a case where N = 400 and $\frac{R_A}{R_D}$ starts from $\frac{15000}{15000}$ and there are 100 battlefield with values {1,2,3,4}. X axis defender's total resource amount, Y axis percentage of the total amount of values, that the player can win (%).

v_i is the value of the current battlefield. V_n is the sum of every battlefields' value. x is random number between the boundaries written, The equations show that, players are allocating their resource to the battlefield depending on the resource ratio, and the value of the battlefield.

The strategy that they follow is made to maximize the importance of individual battlefields so it is always gradual, and there are no outliers and unexpected jumps because of this. So one of our corollaries was confirmed but the second one was refuted.

5.3.1 Attacker's utility functions

We analyze utilities the same way as in the homogeneous case. It is important because as we have seen there were noticeable important discrepancy in the results that must be examined and this is the most comparable way.

The first utility to examine is the script kiddie/disgruntled employee function (Equation 4.2). Potentially the resource amount of the attacker is still the same so the examined section is around $\frac{2}{N}$. In these scenarios with heterogeneous battlefield values the opportunities are better with a lower resource level. The goal is to win at least one battlefield, which is absolutely feasible according to the expected payoff. The diversity in the battlefields' valuation makes it harder for the defender to secure every field. Also it could be a different strategy from the examined but also giving up the epsilon-equilibria and allocating every resource to one battlefield that is not one from the most valuables could lead to winning that battlefield, which satisfies the utility function. However, in real life, the rationality of the players is clouded by the motivations. Which perfectly describes a disgruntled employee who just wants to cause harm and not behave rationally and lead by her anger. The same can be said about a script kiddie who just wants to achieve something not focusing on the best payoff, just wants to get some sort of payoff.

The hacktivist group's utility function (Equation 4.1) could not be interpreted in this manner, because that would mean that, the players see the game differently. From the attacker's viewpoint the game is homogeneous but heterogeneous from the aspect of the defender's. However, this should be investigated more deeply in future work, because the problem is real and can carry additional facts that come up to the surface only when

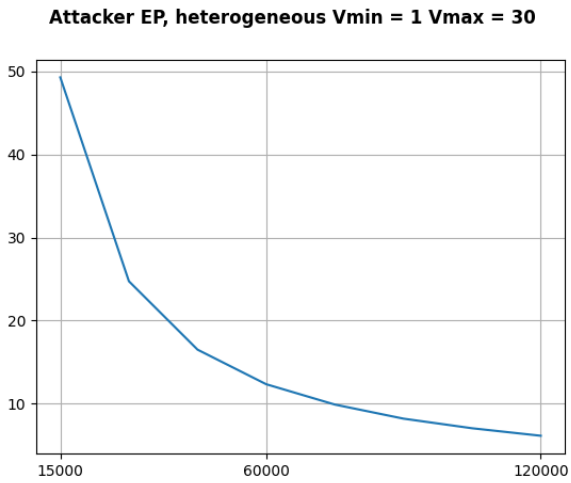

Figure 5.8: The attacker's expected payoff in a case where N = 480 and $\frac{R_A}{R_D}$ starts from $\frac{15000}{15000}$ and there are 120 battlefield with values {1,4,8,30}. X axis defender's total resource amount, Y axis percentage of the total amount of values, that the player can win (%).

examined precisely. That would mean the defender does not have to calculate with the preference of the attacker, but the attacker should calculate with the preference of the defender which implies that there would not be pure equilibria.

In the case of a state-/competitor-sponsored attacker, she would have quite similar amount of resource compared to its target. This means that, the upper boundary of the range should be in focus. The goal here is to win as big as possible which causes loss to the opponent, where $\frac{R_A}{R_D} \to 1$.

All in all we can say that, the heterogeneous version of the Colonel Blotto game is more favorable for the attacker than its homogeneous variant. Furthermore, according to our analysis this advantage does not vary with the value vector.

5.3.2 Defender's utility functions

Clearly the strengthening of the attacker means the weakening of the defender. As discussed earlier the same changes apply here regarding the relationship between the diverse valuation of the battlefields and the change of the expected payoff.

In the manner of the utility functions, we will start with which wants to secure every battlefield (Equation 4.3). This is a maximization problem. The utility comes from the number o battlefields won. This does not include the heterogeneous aspect of the game: it can occur that the player won every battlefield but one, and the utility is still zero even if the lost battlefields' value is from the smallest group. This utility function strives for perfectionism, which also means that if the opponent is a script kiddie/disgruntle employee, only one of them can achieve their objective. Important to note here that to satisfy this utility function the resource advantage should be enormous.

In the case of the previously seen company that deals with the problem of IT security, occurs the problem that we discussed at the attacker's utility, more precisely at the hacktivist group utility function.

And finally comes the utility function for the heterogeneous strategy, which is maximizing the gains, regarding to the values. This is the function that was made for maximizing the

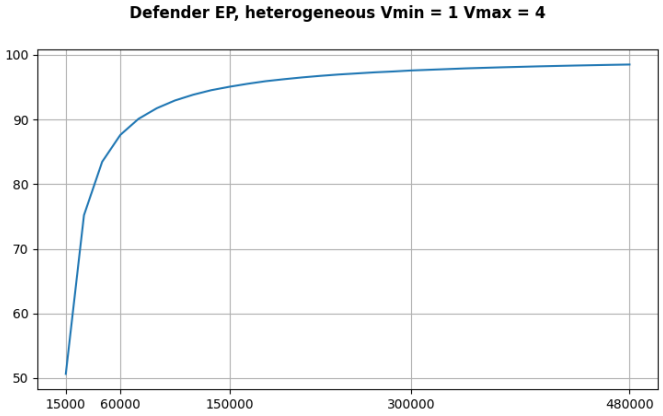

Figure 5.9: The defender's expected payoff in a case where N = 400 and $\frac{R_A}{R_D}$ starts from $\frac{15000}{15000}$ and there are 100 battlefield with values {1,2,3,4}. X axis defender's total resource amount, Y axis percentage of the total amount of values, that the player can win (%).

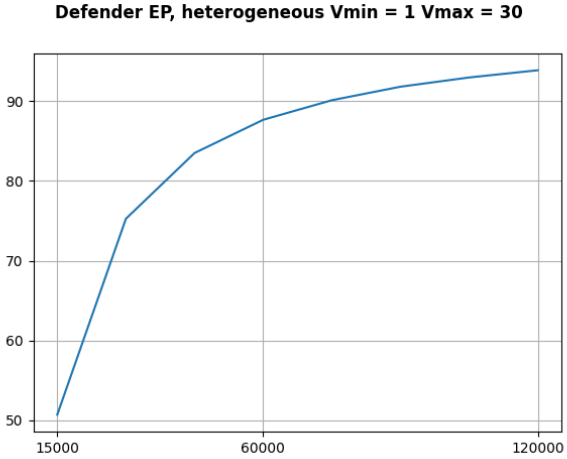

Figure 5.10: The defender's expected payoff in a case where N = 480 and $\frac{R_A}{R_D}$ starts from $\frac{15000}{15000}$ and there are 120 battlefield with values {1,4,8,30}. X axis defender's total resource amount, Y axis percentage of the total amount of values, that the player can win (%).

expected payoff. There could be different levels in the expected payoff, that we want to achieve. The defender always have some sort of resource advantage (remember the basic advantage) so to measure this utility function could be the easiest. But having resource advantage compared to the symmetric case increases the expected payoff dramatically. As mentioned before, win hands down is almost impossible without greater advantage than $\frac{1}{N}$ so this would be more practical to define different thresholds that the player wants to achieve in her expected payoff. As part of the analysis we define these limits at 75%, 90% 95% and 99% for the defender and 40% 25% 10% and 5% for the attacker. The defender can achieve these thresholds with the following multipliers respectively: 2, 5, 9 and 32. Which means for the attacker's thresholds the possible ratios respectively: $\frac{10}{11}, \frac{1}{2}, \frac{1}{5}$ and $\frac{1}{9}$. For the first ratio there was no concrete data point, we computed it through extrapolation.

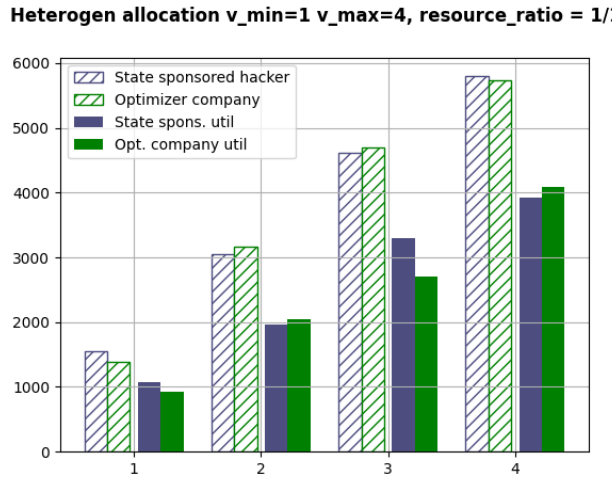

Figure 5.11: Heterogeneous(4) resource allocation when the resource ratio is $\frac{1}{1}$. X axis battlefields grouped by value, Y axis Values to win/spent ($).

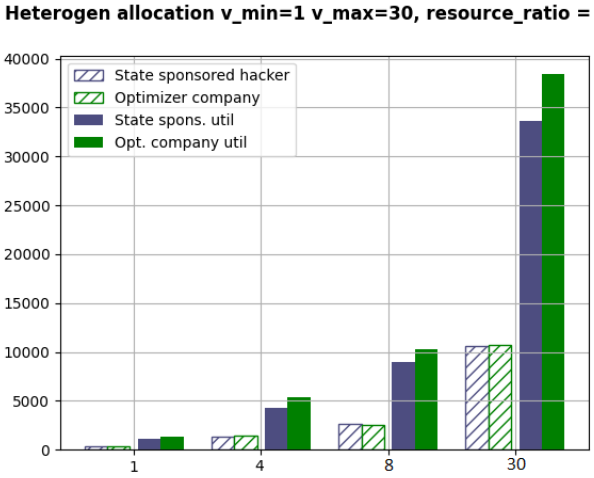

Figure 5.12: Heterogeneous(30) resource allocation when the resource ratio is $\frac{1}{1}$. X axis battlefields grouped by value, Y axis Values to win/spent ($).

5.4 Example allocation for heterogeneous cases and equilibrium analysis

So let us have a closer look on the heterogeneous cases in the same order as in the previous section. Now we have two different scenarios. One where the value vector of the battlefields is $V(1, 2, 3, 4)$ and another one where the value vector is $V(1, 4, 8, 30)$. These are noted as heterogeneous(4) and heterogeneous(30), respectively.

Here we will talk about a state-sponsored attacker (Equation 4.4) instead a hacktivist group, because the hacktivist group does not care about the values of different battlefields. A state-sponsored hacker is trying to optimize the damage caused to the defender country by maximizing their losses, so for her there is difference in the battlefields with different values. Also the average company is replaced with one which is trying to optimize just like the attacker, depending on the V vector. It is very well-observable how the allocation and utility ratios change in each Figure depending on the resource amount and the battlefield's values. The battlefields are grouped by the attack vector, and it can

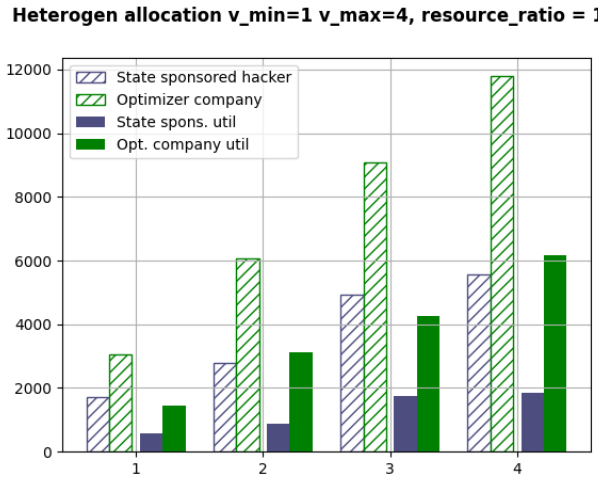

Figure 5.13: Heterogeneous(4) resource allocation when the resource ratio is $\frac{1}{2}$. X axis battlefields grouped by value, Y axis Values to win/spent ($).

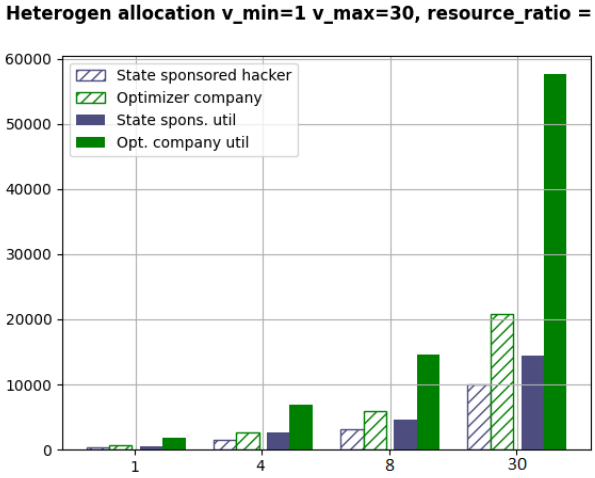

Figure 5.14: Heterogeneous(30) resource allocation when the resource ratio is $\frac{1}{2}$. X axis battlefields grouped by value, Y axis Values to win/spent ($).

be seen only in aggregate how much the parties allocated to the different value groups. The heterogeneous(4,$\frac{1}{1}$) scenario is won by the attacker: note how the different values and their ratio define the amount of resource allocated to the fields. Also interesting to notice, on the battlefields where v=3 the attacker's allocation is less than the defender's but the utility is significantly higher and its reason is the randomness in the allocation strategy. Also in the heterogeneous(30) cases' (Figures 5.12, 5.14, and 5.16) it is well shown, that the utility also scales with the values. Furthermore, it is interesting to notice that, in these cases, when the resource ratios are $\frac{1}{2}$, the utility ratios are varying depending on the V vector. In the heterogeneous(4) case the utility ratio is $\frac{5020}{14980}$ that we can say is around $\frac{1}{3}$. However, in the heterogeneous(30) case this rate is $\frac{22280}{80920}$ which is around $\frac{1}{4}$. *This shows that, when the ratio of the battlefields' value changes, the chances are getting more favorable for the defender.* From the aspect of an optimizing company this is a beneficial development, but at the same time they still lose battlefields from the most valuable ones, so it is still risky.

Let us have a look on the other side of our scale, when the company is facing someone with much less resources (see Figures 5.15-5.18). They have insight on the company's defense in

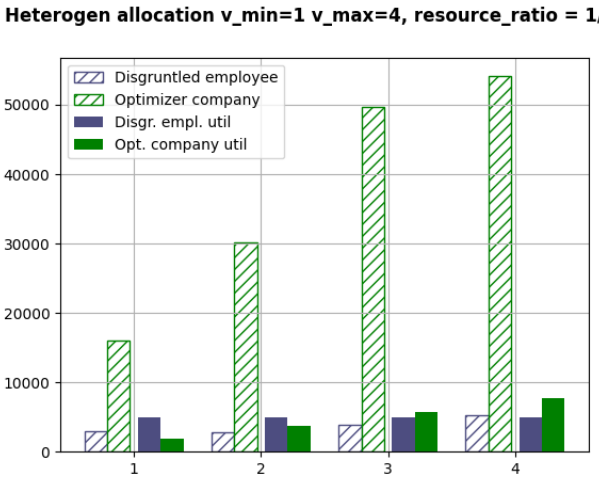

Figure 5.15: Heterogeneous(4) resource allocation when the resource ratio is $\frac{1}{10}$. X axis battlefields grouped by value, Y axis Values to win/spent ($).

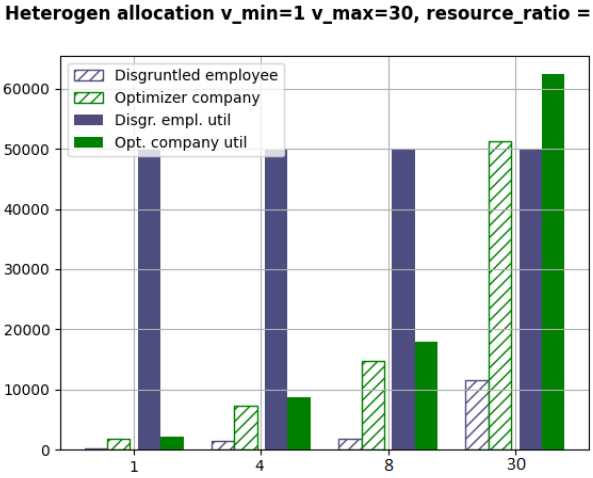

Figure 5.16: Heterogeneous(30) resource allocation when the resource ratio is $\frac{1}{5}$. X axis battlefields grouped by value, Y axis Values to win/spent ($).

that manner, they can see these different battlefields and their values, which means they can also sort the battlefields and plan their attack according to that. They still have the needed amount of resource to accomplish their goal. However, it would be interesting to examine whether they have the chance to harm the country above given thresholds. This holds in both heterogeneous cases. Also from the defender's side, it is still not possible to prevent suffering some damage, but it would be interesting whether is it possible with thresholds or some sort of clauses, like no loss of the most valuable battlefields, or no more than 5%. These could be mitigations in the secure company's utility or tightenings in the the optimizer company's utility. *Even in different cases, when the defender's advantage is huge, there is chance for the attacker.*

5.5 Discussion

There are multiple approaches of this problem, we can examine it from the attacker's perspective, to see different, rational actors how would allocate its resources. Which can

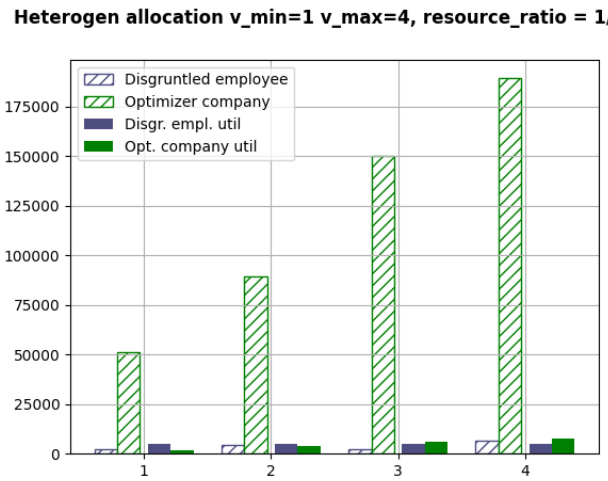

Figure 5.17: Heterogeneous(4) resource allocation when the resource ratio is $\frac{1}{32}$. X axis battlefields grouped by value, Y axis Values to win/spent ($).

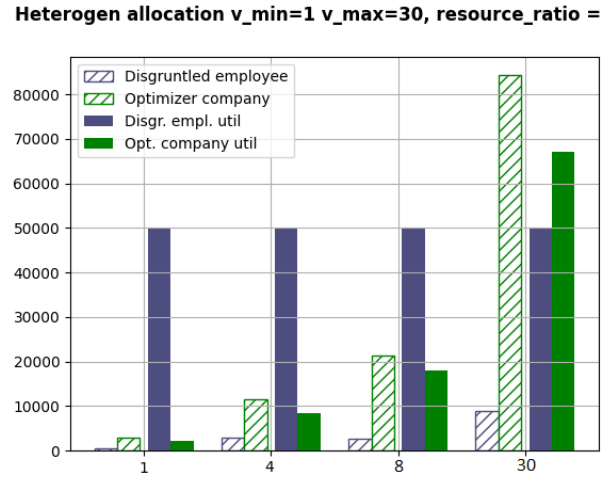

Figure 5.18: Heterogeneous(30) resource allocation when the resource ratio is $\frac{1}{8}$. X axis battlefields grouped by value, Y axis Values to win/spent ($).

lead us to prepare for these attacks. And the same can be said about the defender's side, how they could achieve the goal they set. This strategy shows us how they could profit from playing against different actors according to their utility.

It can mean that, if having a great advantage in resource ($\frac{1}{N} > \frac{R_A}{R_D}$) the chances of being successfully attacked by a script kiddie/disgruntled employee is zero. Nonetheless unfortunately we can not say that without this advantage we are safe against these actors (especially in heterogeneous cases, and as we see real life is heterogeneous) who are furthermore not completely rational. The motivation can cloud their mind which maintains the possibility of irrational moves. Also these results are based on that, the parties are having knowledge about their opponents budget. The defender only knows what type of attackers can try to attack her, and can prepare for in which cases what are the expected payoffs. In real life the attacker has less detailed picture about the targeted company's resource allocation, or at least not in all cases. A disgruntled employee can know something and with enough money and research it can be achieved to find out what you are up against. In a model where the resources are not works in a use-it-or-lose-it manner it would worth an investigation what is more profitable, spending the budget to secure our

system and try to avoid different attacks or just fake that we are securing our system, communicating it very firmly meanwhile not spending that much money just trying to discourage other parties with this strategy.

Even in homogeneous and heterogeneous case there is the strategy when the number of won battlefields count. In homogeneous case this utility depends on the resource ratio. In the heterogeneous case it is quite different because who treats the game homogeneous can not see difference between battlefields however who treats it as heterogeneous can focus on more valuable fields so can profit easily from this asymmetry. It is not defined in this case who wins the game. The one who sees every field as equal e.g. $V(1)$ and the maximum value she can collect is N, while who sees different values can easily collect more value, so a normalization is needed. This can be absolute a real life scenario and can show that the different motives how can differentiate the strategy.

In the heterogeneous case we can say that comes a utility that focuses on maximizing a value. This goal for the players is highly consistent with the strategy that tries to maximize the expected payoff. The slope of the function is very large between $\frac{1}{1}$ and $\frac{1}{3}$ so it could worth the defender to define her budget at least 3 times more than the possible attacker's one. Also from the attacker's point of view this can come in handy if she has a chance to deceive the defender when trying to approximate her budget, it worths to seem more harmless like really. This expand that, the defender has to make serious and thorough research regarding to the budget of the attacker because it can have crucial consequences.

Chapter 6

Conclusion

We have modeled a one-on-one cyberattacker-defender scenario with the help of the Colonel Blotto game framework. To parametrize the game with realistic inputs, we compiled several different cybercrime and IT security market data sources to support our model, and to make an empirical case study, which can be evaluated to serve as important information for real world companies, and even as a base for further research in the topic. Specifically, using epsilon-equilibrium as a solution concept, progressing from simpler to more elaborate scenarios, we characterize their likely outcome. First, we find that in case of heterogeneous battlefields, it is practically infeasible to defend against all type of attacks. Second, if the attacker has less resources than the defender, he will not be able to win the entire game but might still accomplish his objectives. Third, we show the existence of threshold points from which the defender experiences diminishing returns when increasing his resources allocated to specific battlefields. Last, we discuss the implications of our case studies which may be proven for a company planning their cyber-defense.

Future work

The model we created can be extended in several directions. It would be also interesting to see what results it brings to include more parties in the game; not only one against one, but with multiple defenders (with same or different utility functions) against 1 attacker. In this case, the attacker is weaker but can reuse the exploits and tools she possesses and use it against every defender and see whether it works or not. It can also work vice versa, more attackers against one or more defenders. This would describe better the real life where, as seen, attackers are having different agreements on different darknet forums. As mentioned previously it would make sense to model the game with resources that does not have the use-it-or-lose-it property. Furthermroe, the nature of the battlefields could be defined somehow differently. For example, a 3 battlefield game and this 3 would be the CIA attributes as Confidentiality, Integrity, Availability. These could include further battlefields and even can overlap with each other. On the more practical side, battlefields could represent different technological platforms or vendors whose products the companies use, and measure how vulnerable they are through these third party dependencies.

Bibliography

[1] Luca Allodi. Economic factors of vulnerability trade and exploitation. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pages 1483–1499, 2017.

[2] Ross Anderson and Tyler Moore. The economics of information security. *science*, 314 (5799):610–613, 2006.

[3] Daniel G Arce, Dan Kovenock, and Brian Roberson. Weakest-link attacker-defender games with multiple attack technologies. *Naval Research Logistics (NRL)*, 59(6): 457–469, 2012.

[4] Andrew Austin and Laurie Williams. One technique is not enough: A comparison of vulnerability discovery techniques. In *2011 International Symposium on Empirical Software Engineering and Measurement*, pages 97–106. IEEE, 2011.

[5] Michele Campobasso and Luca Allodi. Impersonation-as-a-service: Characterizing the emerging criminal infrastructure for user impersonation at scale. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 1665–1680, 2020.

[6] Pern Hui Chia and John Chuang. Colonel blotto in the phishing war. In *International Conference on Decision and Game Theory for Security*, pages 201–218. Springer, 2011.

[7] Pern Hui Chia, John Chuang, and Yanling Chen. Whack-a-mole: Asymmetric conflict and guerrilla warfare in web security. In *Proceedings of the 15th Annual Workshop on the Economics of Information Security*, 2016.

[8] Thomas Dubendorfer, Arno Wagner, and Bernhard Plattner. An economic damage model for large-scale internet attacks. In *13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pages 223–228. IEEE, 2004.

[9] Mete Eminağaoğlu, Erdem Uçar, and Şaban Eren. The positive outcomes of information security awareness training in companies–a case study. *information security technical report*, 14(4):223–229, 2009.

[10] Christian Ewerhart and Dan Kovenock. A class of n-player colonel blotto games with multidimensional private information. *Operations Research Letters*, 49(3):418–425, 2021.

[11] Aidin Ferdowsi, Walid Saad, Behrouz Maham, and Narayan B Mandayam. A colonel blotto game for interdependence-aware cyber-physical systems security in smart cities. In *Proceedings of the 2nd international workshop on science of smart city operations and platforms engineering*, pages 7–12, 2017.

[12] Abhishek Gupta, Galina Schwartz, Cédric Langbort, S Shankar Sastry, and Tamer Bařar. A three-stage colonel blotto game with applications to cyberphysical security. In *2014 American Control Conference*, pages 3820–3825. IEEE, 2014.

[13] Reinoud Joosten, Lambert JM Nieuwenhuis, et al. Analysing the impact of a ddos attack announcement on victim stock prices. In *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, pages 354–362. IEEE, 2017.

[14] Harjinder Singh Lallie, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105:102248, 2021.

[15] Minghui Min, Liang Xiao, Caixia Xie, Mohammad Hajimirsadeghi, and Narayan B Mandayam. Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach. *IEEE Internet of Things Journal*, 5(6):4250–4261, 2018.

[16] Alan Nochenson and CF Heimann. Simulation and game-theoretic analysis of an attacker-defender game. In *International Conference on Decision and Game Theory for Security*, pages 138–151. Springer, 2012.

[17] Brian Roberson. The colonel blotto game. *Economic Theory*, 29(1):1–24, 2006.

[18] Regner Sabillon, Victor Cavaller, Jeimy Cano, and Jordi Serra-Ruiz. Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, pages 1–9. IEEE, 2016.

[19] Galina Schwartz, Patrick Loiseau, and Shankar S. Sastry. The heterogeneous colonel blotto game. In *2014 7th International Conference on NETwork Games, COntrol and OPtimization (NetGCoop)*, pages 232–238, 2014.

[20] Stu Sjouwerman. Q1 2020 coronavirus-related phishing email attacks are up 600 URL `https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600`.

[21] Onur Kemal Tosun. Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76:101795, 2021.

[22] Dong Quan Vu, Patrick Loiseau, and Alonso Silva. Efficient computation of approximate equilibria in discrete colonel blotto games. In Jérôme Lang, editor, *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI 2018, July 13-19, 2018, Stockholm, Sweden*, pages 519–526. ijcai.org, 2018. DOI: `10.24963/ijcai.2018/72`. URL `https://doi.org/10.24963/ijcai.2018/72`.