Information Security Journal: A Global Perspective, 00:1–13, 2014

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2014.931488

Toward a Monopoly Botnet Market

Zhen Li[1] and Qi Liao[2]
[1]Department of Economics and Management, Albion College, Albion, Michigan, USA
[2]Department of Computer Science, Central Michigan University, Mount Pleasant, Michigan, USA

ABSTRACT Economics play an increasingly important role in fighting cyber crimes. While the arms race against botnet problems has achieved limited success, we propose an approach attacking botnets through affecting a botnet market structure. The characteristics of the present underground botnet market suggest that it functions effectively as perfectly competitive. Competitive markets are usually efficient. We argue that less competition in the botnet market is actually preferred. Our economic analysis suggests that monopoly reduces the overall market output of botnets. Using a model of market structure evolution, we identify key forces that affect the botnet market structure and propose possible ways such as defaming botnet entrants to reduce competition, which ultimately reduce the size and output of the botnet market. The analysis provides useful insight to botnet defenders as a guidance on an efficient allocation of defending resources by attacking more on new entrants to the botnet market relative to the existing botmasters.

KEYWORDS botnet defamation, botnet defense, economics, market structure, monopoly

1. INTRODUCTION

Network security problems, such as hacking, attacking, malware, and spam, plague today's Internet. Most of these problems are related to one single source—botnets. Botnets are networks consisting of compromised computers known as "zombies," "robots," or simply "bots." Computers could be hacked and controlled through malware, ranging from running binaries from email attachments to installing application software from untrusted sources, to viewing flash on Websites. Since their appearance, botnets have evolved rapidly and have increasingly become a security concern.

Nowadays, botnets are commonly used for an array of malicious attacks including distributed denial-of-service attacks (DDoS), key-logging, ad clicks, SMTP mail relays for spam, and identity and financial information theft, all of which have the potential to generate revenue for botmasters, that is, cybercriminals who acquire, control, and manage (aka "herd") botnets (Franklin, Paxson, Perrig, & Savage, 2007; Ford & Gordon, 2006; Z. Li, Liao, & Striegel, 2008). Botmasters' profit-driven activities impose disproportionate costs on society: the monetary cost of cyber crime to society may be roughly compared with what the cyber criminals earn, but the indirect and defense costs to society are much higher (Anderson et al., 2013). While technical approaches alone have achieved limited success, economic approaches can

Address correspondence to Qi Liao, Department of Computer Science, College of Science and Technologies, Central Michigan University, Pearce 417, Mount Pleasant, MI 48859, USA. E-mail: liao1q@cmich.edu

be useful for understanding and mitigating network security problems and, thus, should be integrated into technical designs (Anderson, 2001, 2006).

Recently, there has been extensive diversification of the underground cyber crime economy. The online crime ecosystem has evolved into a supply chain. Malware authors sell toolkits to botmasters; botmasters sell or rent botnet services to cyber criminals such as carders and spammers to launch malicious attacks, steal credentials, etc.; and the stolen credentials and other virtual assets can be sold to end users to make unauthorized transactions. While cyber criminals may build their own botnets to launch attacks, it is much more common to hire such botnet services. Botnets can even be created on demand (Caballero, Grier, Kreibich, & Paxson, 2011). A high specialization of activities in the underground markets has been found (Segura & Lahuerta, 2010). Virtually every component of this underground economy ultimately hinges on access to compromised systems. As botnets are important links of the supply chain of the cyber criminal infrastructure, disrupting the botnet market in which botnet services are traded will interfere with the effective functioning of the underground ecosystem, and hence help alleviate the Internet security threat.

To that end, we study the market structure of the underground botnet economy by applying the economic analysis of market structures to categorize the botnet market and explore key determining factors that may shape the botnet market structure. Various market structures will have very different welfare and efficiency implications. We observe that the current underground botnet market has largely the characteristics of a perfectly *competitive* market because cyber criminals of today no longer require specialized knowledge or technical skill to herd botnets. Also, malicious software, ready-to-use zombie networks, and anonymous hosting services are all readily available on the Internet at low prices.

One major contribution of this article is to explore a monopolistic botnet market structure, which is preferable to botnet defenders. We argue that *monopoly*, though not an efficient type of market structure for most legitimate commodities, can be a desirable market structure for malicious botnets from the perspective of defenders. According to economic theories of market structure analysis, reducing the level of competition in the botnet market will result in higher prices as botmasters seek for monopolistic profit by restraining their supply of botnets, thus hurting the botnet consumers, who are primarily cyber criminals engaging in illegal activities. Ultimately, less competition in the botnet market will lead to reduced transactions in botnet services, that is, reduced market output of botnets.

In particular, we derive a model that describes the evolution of the botnet market and identify some key forces governing its evolution. A distinctive feature of the model is that the factors determining the early evolution of the botnet market will shape its structure in long-run equilibrium. The model emphasizes how factors and events that influence the number of potential botmasters, the survival of new entrants, and the growth of incumbent botmasters will affect the ultimate number of botmasters and the size distribution of them in the market.

This article applies economic theories and analysis of market structure to categorize the botnet market based on its main characteristics, explores key determining factors that may shape its market structure, and suggests possible ways to shift the botnet market away from competition. Contrary to the traditional thinking that we should mainly focus on large botnets, we propose biased defaming attack targeting new entrants to the botnet market, forcing them to drop out shortly. The low survival rate of new entrants will further discourage market entry through the contagion effect.

By emphasizing the effects of market structure on market price and market output, the article aims at providing botnet defenders and policy makers with relevant information of the effective allocation of defense resources. Though the article focuses on the botnet market, the insights learned can also be applied to other underground markets in the supply chain.

The rest of the paper is organized as follows. Section 2 provides a brief introduction to the economics of market structure, characterizes the underground botnet market as competitive, and compares the efficiency implications of competition and monopoly in a market. Section 3 derives a model of botnet market evolution and identifies key forces that determine its market structure in equilibrium. Based on the modeling analysis, we propose possible ways to reduce competition in the botnet market in Section 4. Section 5 discusses related work. Section 6 concludes the paper.

2. BOTNET MARKET STRUCTURE

In this section, we begin with a brief introduction of various market structures. We then define the current botnet market as being nearly perfectly competitive, followed by a comparison of competitive and monopolistic botnet markets to show that a monopolistic market structure will be

less efficient than a competitive market structure for botnet underground economy.

2.1. Introduction to Market Structure

In economics, market structure refers to the organizational and other characteristics of the industry serving the market. The most important characteristics defining market structure include the number of buyers and sellers, the nature of costs (including the potential for producers to exploit economies of scale and the presence of sunk costs), and the extent of product differentiation, and ease of entry and exit (Baumol, 1982; Colton, 1993). The four major types of market structure are

- Perfect competition, where there are no barriers to entry, many sellers offer a standardized product, and many consumers shop on price differences alone.
- Monopolistic competition, where many sellers offer a differentiated product. It is similar to competition, with the exception that the products themselves are a bit different from one another, so consumers look for those differences rather than price differences.
- Oligopoly, a market dominated by a small number of firms.
- Monopoly, where there is only one seller dominating the entire market.

Figure 1 illustrates the market structure continuum in terms of market power, product differentiation, number of competitors, and ease of entry and exit. In particular, "Market Power" refers to the ability of a seller to profitably raise its price. "Product Differentiation" is the easiness and likelihood to differentiate a seller's product from its competitors' products to attract customers. "Number of Competitors" measures the level of competition in a market, and "Ease of Entry and Exit" is the ease with which new sellers can enter a market and existing sellers can leave a market.

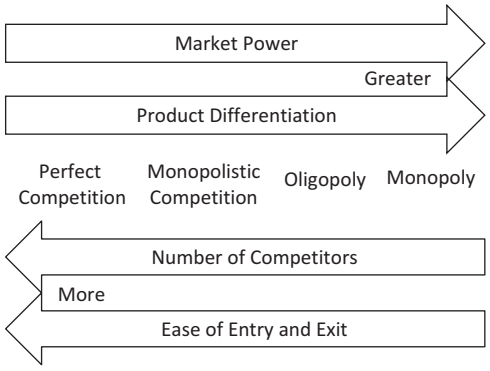


FIGURE 1 **Market structure continuum.**

Market structure is important in that it affects market outcomes through its impact on the motivations, opportunities, and decisions of buyers and sellers in the market. For most legitimate goods and services, competition is preferred as perfect competition can be both productively and allocatively efficient (V. L. Smith, 1987).

2.2. Competitive Botnet Market

The botnet underground market shares many features of a competitive market. It has been shown that compared with conventional markets, markets on the Internet are more competitive, and retailing on the Internet is almost perfectly competitive (M. D. Smith, Bailey, & Brynjolfsson, 2000).

Large participation has been found in the botnet market (Franklin et al., 2007). On the supply side of the botnet market, it is no longer necessary to acquire specialized knowledge or expertise to herd bots. The term "herding" refers to botmasters' acquisition and maintenance of botnets. While trivial, there is cost to herd botnets. For example, one needs to scan and discover vulnerabilities of machines, write malware to explore the specific vulnerabilities and gain control of such systems. On today's Internet, ready-to-use generic malware and hosting services can be easily acquired at relatively low prices (Symantec, 2012). The easy and cheap acquisition of malware allows even nonexperts to generate their own customized botnets. Meanwhile, it is also easy to join the demand side of the botnet market. Practically anyone with the knowledge of the Internet search engines can probably locate botnet sellers on the hacking message boards.

Besides large market participation, another key feature of a competitive market is the relatively low price. For botnet pricing in particular, different factors are in effect: size of botnet, type of usage, intended targets, location, duration of attack, and so forth. Economic theories of supply-and-demand analysis suggest that changes in supply and demand lead to price changes. Unpicking the extent to which price variation is due to supply or demand is challenging for an underground market like the botnet market, where we have only limited information. Nevertheless, it has been found that though actual botnet prices vary, the value of each machine stays quite low (Segura & Lahuerta, 2010). The low botnet price suggests the possibly intense competition in the botnet market.

Normally competition is preferred in a market as it increases efficiency. Nevertheless, to fight against botnets, promoting a *monopoly* botnet market structure can be an effective economic approach to reduce the size of the botnet market.

2.3. Competition versus Monopoly in Botnet Market

In this section, we illustrate how price and output of botnets change when the botnet market shifts from competition to monopoly. Botmasters are assumed profit-driven who determine the price and output levels that return the greatest profit. Regardless of market structure, total profit reaches its maximum point where marginal revenue equals market cost ($MR = MC$). Marginal cost (MC) is additional cost of producing one more unit of product. It depends on the cost structure of the producer, not on the structure of the product market.

Marginal revenue nevertheless, depends on market structure. Marginal revenue is the additional revenue that will be generated by increasing product sales by one unit. Under perfect competition, botmasters are price takers so that MR is fixed at the given market price level; that is, $P = MR$ where P is the market price of botnets. Under monopoly, the monopolist is a price setter. The monopolistic MR can be derived from total revenue $TR(Q) = P(Q) \times Q$. By product rule, $MR(Q) = \frac{d(TR)}{dQ} = P(Q) + P'(Q) \times Q$, where $P(Q)$ is the standard price, just as in competitive market, and $P'(Q) \times Q$ is Cournot distortion due to sellers' incentive to reduce quantity to raise price. MR depends on the price elasticity of demand (denoted by ϵ) that measures the responsiveness of botnet consumers to a change in market price: $\varepsilon = -\frac{dQ}{dP} \times \frac{P}{Q}$, from which we derive $-\frac{P}{\varepsilon} = \frac{dP}{dQ} \times Q = P'(Q) \times Q$, thus $MR = P(1 - \frac{1}{\varepsilon})$. If $\varepsilon < 1, MR < 0$, thus monopoly botmaster will not rent botnets where demand is inelastic ($\varepsilon < 1$). Therefore, in the range of demand where monopolistic botnet revenue falls with output, monopoly botmaster always reduces output to increase revenue.

Rearranging $MR = P(1 - \frac{1}{\varepsilon}) = MC$, the monopolistic elasticity pricing rule is $\frac{P-MC}{P} = \frac{1}{\varepsilon}$, measuring the percentage markup of price over marginal cost. The markup is equal to the inverse of the price elasticity of demand. It can be viewed as a measure of monopoly power. As elasticity increases (or decreases), a monopolist has less (or more) power to increase price above marginal cost.

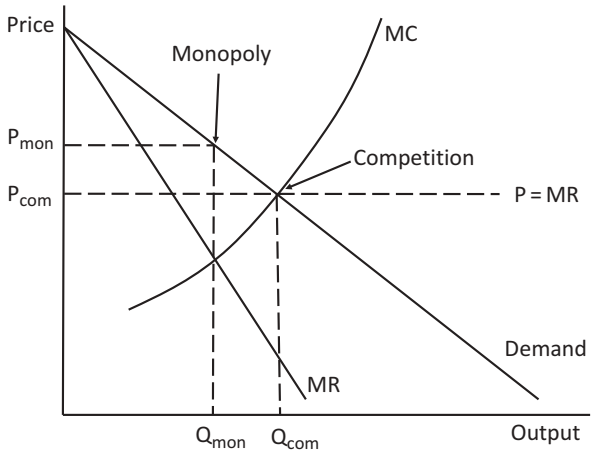


FIGURE 2 **Competitive vs. monopolistic botnet market.**

Figure 2 illustrates the marginal cost (MC) curve, and the marginal revenue (MR) curve under both competition (horizontal) and monopoly (downward-sloping). When profit is maximized at $MR = MC$, the size of the market is at Q_{com} under competition, and Q_{mon} under monopoly.

As in Figure 2, monopolistic output is less than and monopolistic price is higher than the counterpart in a competitive market ($Q_{mon} < Q_{com}, P_{mon} > P_{com}$). That is, a monopolist produces a lower output which it sells at a higher price. Competitive pressures in perfect competition serve to eliminate supernormal profit, which is in absence in monopoly. Due to organizational slack resulting from the absence of competitive pressures, monopolies are always likely to be technically and productively inefficient (Leibenstein, 1966), which happens at all levels of output.

In practice, it is difficult for botmasters to gain monopolistic power as the technical obstacles for entering the botnet market have been falling. Botmasters themselves may also lack the incentive to get big. On one hand, botmasters do not have to be big, which depends on the business model they intend to adopt. On the other hand, big botnets are more likely to be noticed and dismantled, which is bad from the perspective of botmasters. The recent trend is toward smaller botnets (Cooke, Jahanian, & Mcpherson, 2005; Vogt, Aycock, & Jacobson, 2007). Therefore, the transition from competition to monopoly is unlikely to occur automatically. Is there anything defenders can do to make the botnet market less competitive? In the following, we use a botnet market evolution model to identify a number of key forces that influence the level of competition in the botnet market, and explore some

possible ways to make the botnet market shift away from competition.

3. MODELING BOTNET MARKET EVOLUTION

In this section, we modify the general industry evolution model (Klepper & Graddy, 1990) to illustrate the evolution of the botnet market and identify key determining forces of the botnet market structure.

The botnet market is assumed initiated in period 0. At the beginning of period t, the number of botmasters in the market is denoted by N_t, and their total output is denoted by Q_t. In every period, there may be entry and exit. The dynamics of competition is captured by $N_t = N_{t-1} + E_{t-1} - X_{t-1}$, where E_{t-1} is the number of entrants during period $t-1$ that are still in the market at the end of the period, and X_{t-1} is the number of incumbent botmasters that exit during period $t-1$. Such botnet market evolution is essentially a stochastic process, but we impose no structure on the probability distribution of entry and exit, which largely depends on the cost structure of individual botmasters. The random distribution of cost structure is not essential for our analysis. What is of interest is the final direction in which the process will evolve and defenders' strategies that may change the final equilibrium status. The process over which the long-run equilibrium is reached does not matter much.

Consider entry to the botnet market. In each period t, there are K_t potential botmasters that could conceivably enter the market, of which E_t choose to enter. We assume that entry causes the pool of potential botmasters to shrink, that is, $K_t \geq K_{t+1}$. There is a lump-sum cost associated with entry, including the cost of acquiring botnet toolkits and command and control (*C&C*) channels. Since botmasters are endowed with various levels of expertise (e.g., experts vs. rookies) and malware costs can also be different, so that the startup cost varies among potential botmasters, that is, $F_i > 0$ where F_i is the fixed startup cost for potential botmaster *i*. Different from (Klepper & Graddy, 1990) where constant returns to scale is assumed, the expansion of botnets is subject to increasing returns to scale whereby the per-bot cost decreases as the size of botnets increases. Herding botnets is a scalable attack as the cost of the attack has very little dependence of the total number of machines hacked (Herley, 2013). In many cases in the botnet market, bulk discounts are granted (Caballero et al., 2011), reflecting scale economies in botnet production. Therefore, for a representative botmaster *i,* the total cost function takes the form of $C(Q_i) = F_i + c \times Q_i$, where c is the marginal cost of herding botnets. Marginal cost is assumed constant and homogeneous to botmasters at $MC = c$, but botmasters differ in their scale of production of Q_i. We can derive average cost as $AC(Q_i) = \frac{C(Q_i)}{Q_i} = \frac{F_i}{Q_i} + c$ from total cost. Average cost is assumed lower bounded at $AC(Q_i) \geq L$ where L is the lowest attainable average cost possible, homogenous to all botmasters. As $Q \to \infty, F/Q \to 0$; that is, when the size of botnets is infinitely large, average cost converges to marginal cost. Average cost is heterogeneous to botmasters for various reasons. In the context of the model setup, the key difference lies in level of expertise (measured by F_i) and experience (measured by Q_i). Average cost tends to be higher for rookie botmasters than seasoned botmasters as the latter are more experienced and normally operate at a larger scale, that is, a higher Q_i for seasoned botmasters. Potential botmasters with more expertise tend to have a lower average cost than nonexperts, that is, a lower F_i for skillful experts.

Entrants can lower average cost upon entry. The cost reduction could be realized through the imitation of successful botmasters or from the accumulation of experience. For simplicity, we assume all the cost reduction occurs upon entry thus botmasters entering during period t with an average cost $AC > L(1+\gamma)$ can reduce their cost to $AC/(1+\gamma)$ by the end of period *t,* where γ quantifies the ease of survival of entrants. After the period of entry, surviving botmasters can further lower average cost when they expand botnets.

We assume that all botmasters are profit maximizing, thus a potential botmaster will enter the market only if the expected profit from entry is nonnegative. Profit depends on market price and average cost as $\Pi_{i,t} = (P_t - \frac{F_i}{Q_{i,t}} - c) \times Q_{i,t}$, where $\Pi_{i,t}$ is the profit received by botmaster i in period *t,* and P_t is the botnet price at the beginning of period *t,* homogeneous to all botmasters selling in the market. Botmasters entering the market in period t are assumed to enter with a botnet size of one unit. If they are still in the market by the end of period *t,* they change their botnet size in period $t+1$ at a rate that is determined by their cost, relative to market price: Botmasters with $P_{t+1} < \frac{F_i}{Q_{i,t+1}} + c$ exit the market; botmasters with $P_{t+1} = \frac{F_i}{Q_{i,t+1}} + c$ maintain their botnet size; botmasters with $P_{t+1} > \frac{F_i}{Q_{i,t+1}} + c$ expand botnets. In period $t+1$, the size of the botnet market is the sum of all botmasters' output, i.e., $Q_{t+1} = \sum_i (Q_{i,t+1})$. The greater the market price is, the faster will be the expansion of the botnet market.

Proposition 1. There exists a period T such that: (i) for all periods $t < T, P_t > P_{t+1}$ and $Q_t < Q_{t+1}$; (ii) for all periods $t \geq T, P_t = P_{t+1}$ and $Q_t = Q_{t+1}$.

Proof. The supply-and-demand model of economics states that all else being equal, the market price falls when supply increases. Recall average cost of botmaster i in period t is $AC_{i,t} = \frac{F_i}{Q_{i,t}} + c \geq L$. Suppose $P_t < P_{t+1}$ for some period t, then $P_{t+1} > \frac{F_i}{Q_{i,t}} + c$ must hold true for all incumbent botmasters in period t as $P_t \geq \frac{F_i}{Q_{i,t}} + c$ applies to all incumbents in period t. This implies $Q_{t+1} \geq Q_t$, and hence $P_{t+1} \leq P_t$, which is inconsistent with the presumption of $P_t < P_{t+1}$. Therefore, for any period t, only $P_t \geq P_{t+1}$ is possible.

Initially at period 0, P_0 is at a high level due to limited supply. With existing botmasters expanding and potential botmasters entering the market, the botnet price keeps falling as more botnets are supplied to the market, i.e., $P_t > P_{t+1}$ and $Q_t > Q_{t+1}$ during the period of market expansion, and T marks the end of expansion.

During market expansion, surviving botmasters keep increasing output, hence average cost keeps falling until it reaches L, the lowest attainable level. Suppose $P_t > L$ for all t, then all botmasters that have reached L will expand botnet output in every period. Eventually, as all incumbent botmasters have reached the lowest attainable cost L, the total output by all the botmasters must be equal to the botnets demanded for at price L to make the botnet market clear in every period. But this is not possible when $P_t > L$. Therefore, eventually, the botnet price must stabilize at L, and the quantity of botnets supplied to the market stabilizes as well. That is, $P_t = L$ for all $t \geq T$. After period T, all existing botmasters maintain their botnet size as the market price of botnets and their average cost are equal. No new botmasters enter the market as the expected profits from entry will be negative when the price level is too low for newcomers in lack of cost advantage. Therefore, after period T, the botnet market is stabilized with constant number of botmasters, total botnets supplied to the market, and market botnet price. □

Proposition 2. There exists periods $t_1 \leq t_2 < T$ such that: (i) if $t \leq t_1$, then $N_{t+1} \geq N_t$; (ii) if $t_2 \leq t < T$, then $N_{t+1} \leq N_t$; and (iii) if $t \geq T$, then $N_{t+1} = N_t$.

Proof. In early periods of botnet market expansion ($t \leq t_1$), the botnet price must exceed the cost of all incumbent botmasters. As no existing botmasters exit the market, $N_{t+1} \geq N_t$.

Exit occurs in period t_2 when the falling botnet price starts to drive less cost effective botmasters out of business. Given that $P_t > L$ for all $t < T$ and $P_{t+1} < P_t$, all botmasters with a cost that is between P_{t+1} and P_t exit the market in period $t + 1$. Since the pool of potential botmasters shrinks over time, and potential botmasters are cost inferior to incumbent botmasters unless they have superior expertise, there will be no entry or less entry. Hence, for $t_2 \leq t < T, N_{t+1} \leq N_t$.

From Proposition 1, $P_t = L$ for all $t \geq T$. All existing botmasters keep their botnet capacity, and there will be no entry and exit. Therefore, in long-run botnet market equilibrium, the number of botmasters is stabilized; that is, $N_{t+1} = N_t$ for all $t \geq T$. □

Proposition 2 says that the dynamics of competition in the botnet market is composed of three stages. In the early stage of market expansion, the number of botmasters grows. At some later point of market evolution, the number of botmasters falls. Eventually, the number of botmasters stabilizes.

Combining Propositions 1 and 2, the botnet market will eventually be composed of the most cost-effective botmasters that have attained the lowest possible cost. The existing botmasters will be either early entrants producing at larger scales (the larger scale could be reflected by multiple smaller but linked botnets under the control of the same botmaster in the market) or later entrants with endowed expertise advantage. The largest botmasters are those that are among the first to attain the lowest attainable cost. If, after the first botmasters reach the most cost effective botnet scale, there is an unexpectedly long delay before others to catch up, then market shares of first botmasters will be high.

The smaller is the entry cost (F_i) and the slower is the fall in botnet price, the longer will be the initial stage of botnet market expansion before the number of botmasters starts to decline. Entry cost varies among potential botmasters. In each period, only the potential botmasters with competitively low cost choose to enter the market. In early days of market expansion, no prior entrants exit the market, and the number of botmasters rises. Nevertheless, the fall in botnet price will force less competitive botmasters to exit. Entry eventually ceases but exit continues, causing the number of botmasters to decrease. Stability is reached only when there is no longer any disparity in cost among existing botmasters, with the most cost effective botmasters remaining. Propositions 1 and 2 explain the fall in botnet

price, the rise in botnet supply, the change in the number of botmasters, and the eventual leveling off of them that characterize the evolution of the botnet market.

Proposition 3. Events and forces in any period that lead to a greater number of potential botmasters, greater ease of survival of entrants or lower expansion rates of incumbent botmasters will cause the number of botmasters to increase in the following period.

Proof. A rise in K_t (the number of potential botmasters), a rise in γ (measuring the ease of survival), and a rise in the expansion rates of incumbent botmasters during period t must cause P_{t+1} to fall relative to what it would have been. Consider the effect of the price change on N_{t+1}. If K_t rises, causing P_{t+1} to fall, then exit during period t will rise, causing the number of botmasters during period t to fall relative to what it would have been. Suppose this fall is balanced by an equal rise in the number of botmasters entering the botnet market during period t as K_t rises, then N_{t+1} would be unaffected. Since incumbent botmasters are always at least as big as entrants, this implies that Q_{t+1} would fall. But this cannot be if P_{t+1} falls. Consequently, the number of botmasters entering during period t must rise by more than the rise in the number of incumbent botmasters that exit during period t, implying that N_{t+1} must rise relative to what it would have been. Similar argument shows that a rise in γ in period t will lead to a rise in N_{t+1}. If the expansion of all existing botmasters increases, causing P_{t+1} to fall, then the exit rate of botmasters during period t will rise, and the number of entrants during period t will fall, implying that N_{t+1} will fall. □

4. MODEL IMPLICATION

It is interesting to note that the underground botnet market is different from markets for legitimate goods and services where competition is considered welfare-enhancing. In the botnet market, both sellers and buyers are detrimental. Moving from competition to monopoly has an efficiency loss to the botnet market, which is indeed a net gain for the society from the perspective of fighting botnets. In this section, we study and evaluate such impact on the botnet market.

4.1. Reduction in Botnet Market Output

We first use numerical examples to show how market output changes when market structure changes, as discussed in subsection 2.3, with four types of demand functions commonly used in economics: linear demand, concave demand, exponential demand, and constant elasticity demand. For the supply side, the constant marginal cost is held at $MC = 0.5$ for illustration purposes only.

Figure 3 and Table 1 summarize the change in market output as the market shifts from competition to monopoly.

The graphical and numerical illustrations illustrate how much market output decreases depends on both the supply and demand side of the market. Economists have found that the Internet has created real time experiments to address traditional economic questions about consumer behavior and market outcomes. For example, (Einav, Kuchler, Levin, & Sundaresany, 2011) documented experiments conducted by eBay sellers across a wide array of retail products to estimate nonparametric auction demand curves. They found that all demand curves have similar shape, and the marginal cost is constant.

Given the demand side, the level of competition depends on the cost structure of botmasters. In particular, fixed cost can significantly affect the number of botmasters in equilibrium.

Assume in the botnet market, a botmaster faces a linear demand curve

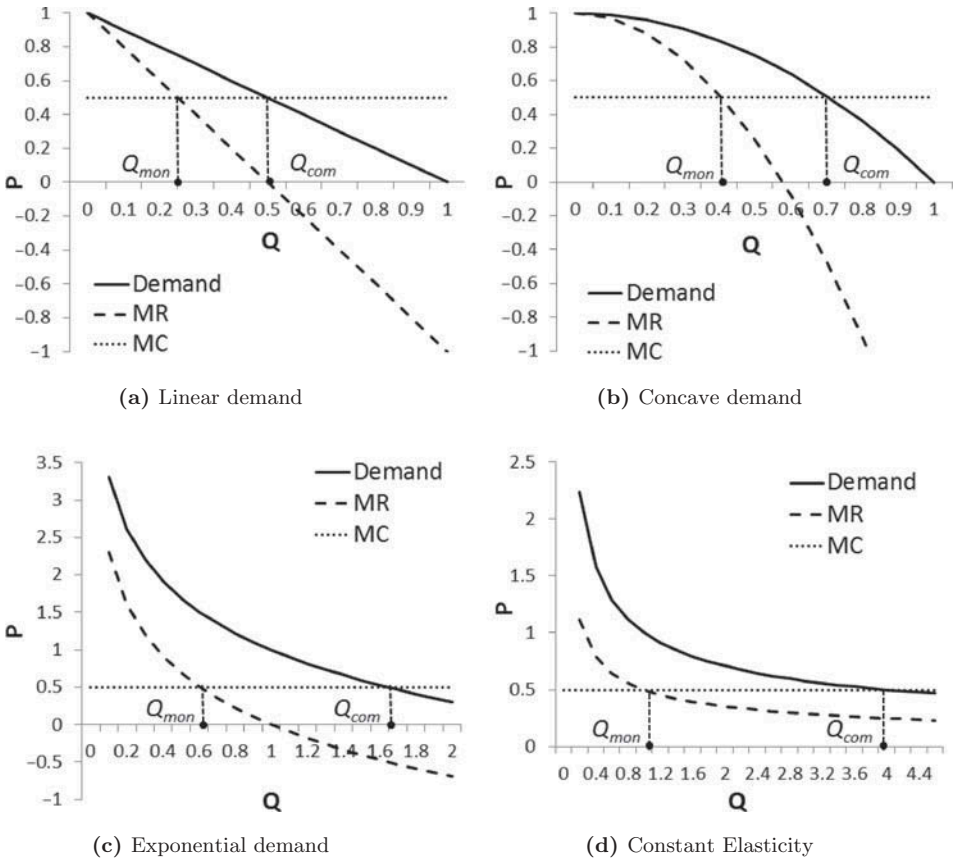
$$q = Q \times [\frac{1}{n} - b(p - \bar{p})] \tag{1}$$

where q is the output of the botmaster, Q is the total market output, n is the number of incumbent botmasters, p is the botmaster's price, and $\bar{p}$ is the average price of the botmaster's competitors (i.e., the other n–1 botmasters in the market). b is a constant term representing the responsiveness of the botmaster's sale to its price, positively related to the price elasticity of demand.

As in section 3, the average cost of the botmaster is $AC = F/q + c$. In market equilibrium, all incumbents charge the same price that equals to the lowest attainable cost, and each will sell an amount $q = Q/n$. Thus, the botmaster's average cost depends on the size of the market and the number of botmasters in the market:

$$AC = n \times \frac{F}{Q} + c \tag{2}$$

From the demand function, we derive the marginal revenue curve as $MR = p - q/(bQ)$. The profit-maximizing botmaster will set marginal revenue equal to marginal cost so that $p = c + q/(bQ)$. In market equilibrium, $q = Q/n$, therefore



(a) Linear demand (b) Concave demand

(c) Exponential demand (d) Constant Elasticity

FIGURE 3 **Comparison of market output under competition and monopoly with various demand.**

TABLE 1 **Decrease in Market Output from Competition to Monopoly**

Demand function	Q_{com}	Q_{mon}	Change
$P(Q) = 1–Q$	0.50	0.25	−0.25
$P(Q) = 1–Q^2$	0.70	0.40	−0.30
$P(Q) = 1–Ln(Q)$	1.65	0.61	−1.04
$P(Q) = \frac{1}{\sqrt{Q}}$	4.00	1.00	−3.00

$$p = c + \frac{1}{bn} \tag{3}$$

Because of entry and exit, all incumbents earn zero economic profit in long-run equilibrium; that is, $p = AC$, from which, we derive

$$n = \sqrt{\frac{Q}{bF}} \tag{4}$$

The size of fixed cost is a key determinant of the equilibrium number of botmasters. Figure 4 illustrates how the market equilibrium number of competitors is decreasing in fixed cost. In the figure, $Q = 500$ and $b = 1$ for illustration purposes only.

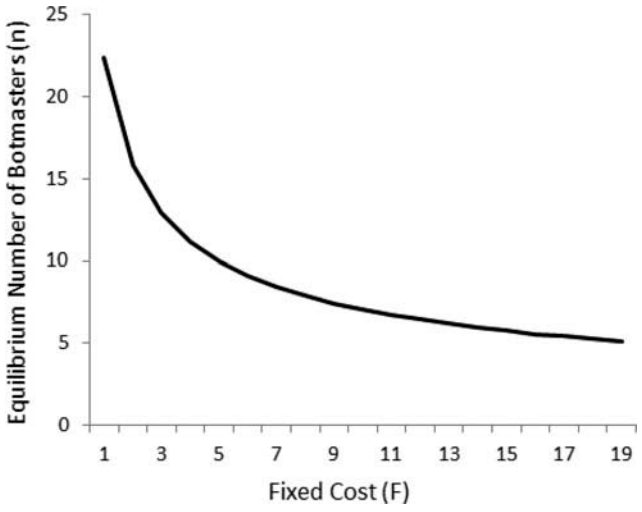


FIGURE 4 **Rising fixed cost reduces the equilibrium number of botmasters (thus defaming may reduce market competition by raising the entrants' costs).**

4.2. Reduction in Botnet Size

In the botnet market evolution model derived in Section 3, the specified cost function is a reasonable representation of botmasters' cost structure. Figure 5 plots the unit botnet price (per Megabit per hour of service) calculated using

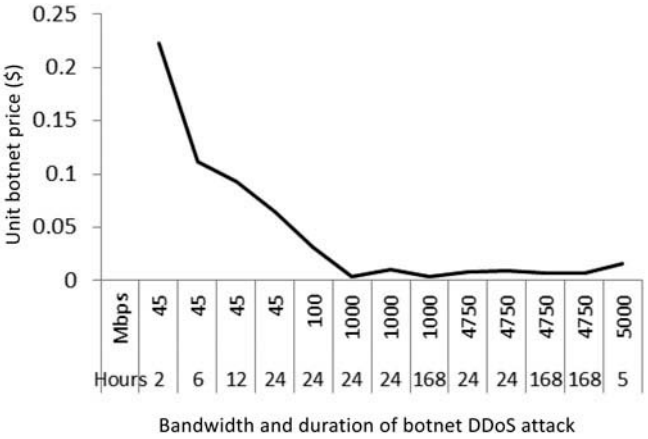


FIGURE 5 **The general trend of botnet unit rental prices (per Mbps per hour) in DDoS attacks: decreasing and stabilizing as the botnet size increases.**

data from published research findings (Segura & Lahuerta, 2010). As shown, initially the per-unit price decreases as the botnet size increases, eventually the price levels off. As price equals to average cost with entry and exit, the unit price curve approximates the average cost of botmasters at different production scales. The shape of the curve supports the assumptions of a relatively significant fixed cost, constant marginal cost, and falling average cost.

The economic analysis in section 2 suggests the supply-reduction guiding principle to reduce the size of the botnet market. From the modeling analysis in section 3, some major forces that affect botnet market competition include:

- the pool of potential botmasters,
- the entry cost for potential botmasters to enter the botnet market,
- the survival rate of new botmasters, and
- the expansion of incumbent botmasters.

The number of botmasters in the market (thus market competition) will fall if the number of potential entrants decreases, entry cost increases, the survival rate of entrants falls, or the growth rate of incumbent botmasters increases. All are essentially to widen the cost disparity between entrants and incumbents. Given expertise, incumbents are more cost effective than newcomers since average cost is decreasing in the level of botnet production, as in $AC = \frac{F}{Q} + c$ from section 3. The cost advantage of incumbents will be strengthened if the entry cost F is increased for newcomers. The larger the cost advantage enjoyed by incumbent botmasters, the smaller is the eventual stabilized number of botmasters. By making it harder for potential botmasters to enter or survive, the size of the botnet market will be reduced. Government policies, legal enforcements, or technical defense measures can affect these determining forces of market competition.

4.3. Transition from Competitive to Monopolistic Botnets

The economic analysis calls for reduced competition in the botnet market. In this section, we discuss possible ways to transform the botnet market from competition to monopoly. The level of competition in the botnet market depends on the number of botmasters participating in the market (associated with entry and exit), their production scale, and product differentiation. The existence of monopolies or market power is often from barriers to entry, high start-up costs or other obstacles (e.g., control of resources, government regulation, education requirements) that prevent new competitors from easily entering the market. For the underground botnet market, government regulations and law enforcements are not as effective as a legitimate market. The cost advantages created by proprietary expertise and know-how are no longer as dominant in today's Internet. It is challenging to develop effective barriers to entry for the botnet market. We observe that although botmasters may lack the incentive to grow (Cooke et al., 2005; Vogt et al., 2007), there is motivation for product differentiation; in particular, botmasters are motivated to build good online reputation among buyers to distinguish themselves from competitors. Based on the modeling analysis, we propose measures aimed at broadening the cost disparity between entrants and incumbents through biased defaming of botmasters.

Reputation and trust are essential for the Internet markets because of the spatial and temporal separation between buyers and sellers imposed by the medium. It has been found that reputation markets (information markets designed to assess content quality) (Yan & Roy, 2008) may offer a number of desirable features for users of online content. On the Internet, a seller's reputation is vetted online nearly in real-time by consumers leaving online reviews and sharing experiences on social media Websites. As an underground market, the botnet market operates in an environment of dishonesty and mutual distrust (Franklin et al., 2007). Trust plays a critically important role in the effective functioning of the market.

It has been shown that it is feasible to attack the verification system of underground markets. Franklin et al. (2007) proposed two approaches to disrupt the client

identification capabilities of open underground markets, a Sybil attack and a slander attack. In a Sybil attack, numerous identities (Sybils) are generated to undercut the participant verification system by advertising deceptive sales. In a slander attack, an attacker eliminates the verified status of buyers and sellers through false defamation. By creating pseudo identities and eliminating the status of honest identities, the number of successful transactions decreases. Caballero et al. (2011) built a program to mimic the network communication used by pay-per-install (PPI) services to obtain the client programs. They exploited the client programs that the PPI provider distributes without actually executing the client programs and accounting. Though the purpose of the researchers is to collect data to study the PPI market, infiltration technique can be used to disrupt the communication between PPI services and clients.

In the botnet market, seasoned sellers tend to have a cost advantage over new competitors. Biased defaming that targets entrants can further strengthen the cost advantage of incumbents. When implementing reputation attacks, instead of eliminating the verified status of sellers randomly, we recommend that the attacks on verification systems target new entrants to the market, forcing them to drop out shortly. Economics is all about the efficient and optimal use of limited resources. Given the limited resources available, botnet defenders should assign a high priority to prevent *new* competitors from surviving. Compared with defaming seasoned botmasters, discrediting new entrants can be much more cost effective. When entrants are kept away from the botnet market, incumbents' market power will increase, and they will be able to raise price to make monopolistic profit by restraining botnet output. As market competition decreases, the market output decreases as well. The effective credibility attack against new entrants in the botnet market can have contagion effects on potential entrants, discouraging them from entry. The lack of credibility of new entrants will also discourage buyers from choosing new entrants, further lowing the incentive of entry. In the framework of the economic model, effective defaming of entrants is equivalent to increasing the entry cost, thus reducing the level of competition in market equilibrium.

5. RELATED WORK

There is a large economic literature on market structure analysis. Much focuses on a specific industry, including the e-Commerce market and the underground markets like the drug market. For example, Smith et al. (2000) reviewed the academic research on the characteristics of electronic markets and discussed the implications of the research. Varian (2001) reviewed various economic phenomena that are important in high-technology industries and market structure. Wilson and Stevens (2007) provided a review of what is known about the economic structure of illicit drug markets. Our work on the underground botnet economy, to some extent, combines these studies as it is industry-specific, underground, and over the Internet. Our market evolution analysis is based on the industry evolution model in (Klepper & Graddy, 1990). The purpose is to modify the general model based on the observations of the botnet market. As we support a less competitive botnet market structure, the modeling analysis helps identify key factors that affect the level of competition in the botnet market, and hence provides valuable insight to effectively reduce botnet market competition.

There is also a large literature on botnets. Rodrguez-Gmez, Maci-Fernndez, and Garca-Teodoro (2013) proposed a taxonomy of botnet research based upon the botnet's life-cycle (the sequence of stages a botnet needs to pass through to reach its goal), including beginning conception, recruitment, interaction, marketing, attack execution, and end attack success, and presented a selection of botnet research organized according to the proposed taxonomy. They believed that new defense schemes against botnets should be specifically based on the marketing stage as botmasters nowadays are profit-driven. Our work is in line with recent research on mitigating cyber crime and botnets by economic approaches. Over years, there have been various efforts to understand, measure, and analyze botnets (McCarty, 2003; Karasaridis, Rexroad, & Hoeflin, 2007; Dagon, Zou, & Lee, 2006; Grizzard, Sharma, Nunnery, Kang, & Dagon, 2007; Cooke et al., 2005; Wang, Sparks, & Zou, 2007; Rajab, Zarfoss, Monrose, & Terzis, 2007; Liu, Gong, Yang, & Jakalan, 2011). For example, studies by Rajab et al. (2007) and Liu et al. (2011) focused on the nature of botnet size, botnet membership, and its measurement issues. Technical approaches for disrupting underground markets have focused on activities such as locating and disabling hosting infrastructure or tracking and identifying malicious attackers. These techniques face numerous social and technological obstacles which limit their success. Recently, economic approaches by Anderson (2001, 2006), Johnson and Pfleeger (2011), Camp and Johnson (2012), Garg, Husted, and Camp (2011), and other researchers have been attracting more attention. Economic measures can often be of low cost when they deal with the security threat indirectly through

changing the incentives of market participants. Using a seven-month trace of logs collected from an active underground market, researchers (Franklin et al., 2007) provided first-hand exploration into the underground economy which specializes in the commoditization of activities such as credit card fraud, identity theft, spamming, phishing, online credential theft, and the sale of compromised hosts. Based on market data gathered, they proposed potential low-cost approaches to disrupt the underground markets.

The underground botnet ecosystem provides the main sources of illegal income for cyber criminals. Researchers have studied the underground markets directly. Thomas and Martin (2006) documented online crime. Franklin et al. (2007) monitored the public chat channels used by online criminals to contact each other. Ford and Gordon (2006) proposed launching revenue-destabilization attacks on botnet generated revenue streams from online advertising fraud by constructing a distributed network of machines capable of controlling advertising impression numbers, click through rates and software package installs. Similar discrediting and attacking approaches may be used to reduce botnet market competition. Ormerod et al. (2010) proposed an approach of defeating a botnet toolkit through discouraging or prosecuting its end users. With data collected on web, Zhuge et al. (2009) studied the aspects of the underground market visible as part of the World Wide Web. Kanich et al. (2008) introduced a methodology for measuring the conversion rate of spam, the probability that an unsolicited email will ultimately elicit a sale. Caballero et al. (2011) performed a measurement study of the PPI market by infiltrating PPI services. The economic incentives for launching DDoS attacks were modeled in (Segura & Lahuerta, 2010). Despite the efforts, there is still a long way to go to understand the economics of online crime and quantify Internet security threat.

Uncertainty may play an important role in decision-making of cyber criminals. Chandrasekaran et al. (2006) detected phishing sites by submitting fake responses which mimic real users, reversing the role of the victim and the adversary. Herley and Florêncio (2009) studied the rippers who cheat other participants in the IRC markets. Li et al. (2008) used virtual bots to create *uncertainty* in the necessary rental size of botnets for an attack. Li and Schmitz (2009) built spam traps to submit credentials to phishing sites and used phoneybots to submit honeytokens to pharmers and phishing malware. To some extent, biased defaming of new entrants proposed in this paper works by increasing uncertainty of joining the underground market, hence discouraging market participation.

6. CONCLUSION AND FUTURE WORK

Botnets pose a serious threat to the overall health of today's Internet. While technical approaches have achieved limited success, this article addresses the botnet problem from a different angle by applying economic theories of market structure to the supply chain of cybercriminal infrastructure. Based on the observation that the current botnet market functions close to perfect competition, we encourage a monopoly structure of the botnet market. The economic analysis suggests that the profit-maximizing output level under monopoly is less than that of a competitive market. Contradictory to tradition wisdom that defenders should always attack big targets, we suggest the focus should be shifted to pose barriers to new entrants to the botnet market. One implementation is through biased defaming attack on less experienced entrants. The less efficient market structure will ultimately reduce the output of botnets.

Our findings provide insight for botnet defenders regarding the efficient allocation of limited defense resources and the importance of prioritizing targets of attack. Although our analysis focuses on the botnet market, similar logic may apply to other cybercrime markets consisting the underground ecosystem, such as the market for malware and the market for trading credentials stolen by botnets. The attacks on various markets of the system can be reinforced. For instance, attacking the malware market will make the price of botnet toolkits rise, increase the entry cost of botmasters, and reduce their financial incentives to enter the botnet market. The intervention counteracting the trend towards specialization and diversification in the cybercriminal economy will be our future study.

REFERENCES

Anderson, R. (2001, December 10–14). Why information security is hard—an economic perspective. Proceedings of the 17th Annual Computer Security Applications Conference, pp. 358–365.

Anderson, R. (2006, October 27). The economics of information security. Science, 314(5799), 610–613.

Anderson, R., Barton, C., Bhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy, pp. 265–300. Berlin, Germany: Springer.

Baumol, W. J. (1982, March). Contestable markets: An uprising in the theory of industry structure. American Economic Review, 72(1), 1–15.

Caballero, J., Grier, C., Kreibich, C., and Paxson, V. (2011, August 8–12). Measuring pay-per-install: The commoditization of malware distribution. Proceedings of the 20th USENIX Security Symposium, pp. 187–202.

Camp, L. J., and Johnson, M. E. (2012, March). The economics of financial and medical identity theft. Berlin, Germany: Springer.

Chandrasekaran, M., Chinchani, R., and Upadhyaya, S. J. (2006, June 26–29). Phoney: mimicking user response to detect phishing attacks. Proceedings of the 2006 International Symposium on the World of Wireless, Mobile and Multimedia Networks, pp. 668–672.
Colton, R. D. (1993, September). Consumer information and workable competition in telecommunications. Journal of Economic Issues, 27(3), 775–792.
Cooke, E., Jahanian, F., and Mcpherson, D. (2005, July 7). The zombie roundup: Understanding, detecting, and disrupting botnets. Proceedings of the Steps to Reducing Unwanted Traffic on the Internet Workshop, pp. 39–44.
Dagon, D., Zou, C., and Lee, W. (2006, February 3). Modeling botnet propagation using time zones. Proceedings of the 13th Network and Distributed System Security Symposium.
Einav, L., Kuchler, T., Levin, J., and Sundaresany, N. (2011, September). Learning from seller experiments in online markets. NBER Working Paper No. 17385.
Ford, R., and Gordon, S. (2006, September 19–22). Cent, five cent, ten cent, dollar: Hitting botnets where it really hurts. Proceedings of the 2006 Workshop on New Security Paradigms, pp. 3–10.
Franklin, J., Paxson, V., Perrig, A., and Savage, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 375–388.
Garg, V., Husted, N., and Camp, J. (2011, November 8–9). The smuggling theory approach to organized digital crime. Ecrime Researchers Summit, pp. 1–7.
Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B. B., and Dagon, D. (2007, April 10). Peer-to-peer botnets: Overview and case study. Proceedings of the First Workshop on Hot Topics in Understanding Botnets, pp. 1–1.
Herley, C. (2013, March-April). When does targeting make sense for an attacker? IEEE Security & Privacy, 11(2), 89–92.
Herley, C., and Florêncio, D. (2009, June 24–25). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. Proceedings of the Eighth Workshop on the Economics of Information Security, pp. 33–53.
Johnson, M. E., and Pfleeger, S. L. (2011). Addressing information risk in turbulent times. IEEE Security and Privacy, 9(1), 49–57.
Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., and Savage, S. (2008, October 27–31). Spamalytics: An empirical analysis of spam marketing conversion. Proceedings of ACM Conference on Computer and Communications Security, pp. 3–14.
Karasaridis, A., Rexroad, B., and Hoeflin, D. (2007, April 10). Wide-scale botnet detection and characterization. Proceedings of the First Conference on First Workshop on Hot topics in Understanding Botnets, pp. 7–7.
Klepper, S., and Graddy, E. (1990, Spring). The evolution of new industries and the determinants of market structure. The RAND Journal of Economics, 21(1), 27–44.
Leibenstein, H. (1966). Allocative efficiency vs. x-efficiency. American Economic Review, 56(3), 392–415.
Li, S., and Schmitz, R. (2009, September 20–October 21). A novel antiphishing framework based on honeypots. Proceedings of the 4th Annual Anti-phishing Working Groups Ecrime Researchers Summit, pp. 1–13.
Li, Z., Liao, Q., and Striegel, A. (2008, June 25–28). Botnet economics: Uncertainty matters. Proceedings of the Seventh Workshop on the Economics of Information Security, Hanover, NH.
Liu, S., Gong, J., Yang, W., and Jakalan, A. (2011, September). A survey of botnet size measurement. Proceedings of the 2011 Second International Conference on Networking and Distributed Computing, pp. 36–40.
McCarty, B. (2003, July–August). Botnets: Big and bigger. IEEE Security & Privacy, 1(4), 87–90.
Ormerod, T., Wang, L., Debbabi, M., Youssef, A., Binsalleeh, H., Boukhtouta, A., and Sinha, P. (2010, July 18–25). Defaming botnet toolkits: A bottom-up approach to mitigating the threat. Proceedings of the Fourth International Conference on Emerging Security Information Systems and Technologies, pp. 195–200.
Rajab, M. A., Zarfoss, J., Monrose, F., and Terzis, A. (2007). My botnet is bigger than yours (maybe, better than yours): Why size estimates remain challenging. Proceedings of the First Conference on First Workshop on hot topics in understanding botnets. Retrieved from http://dl.acm.org/citation.cfm?id=1323133&CFID=509421030&CFTOKEN=28790071
Rodrguez-Gmez, R. A., Maci-Fernndez, G., and Garca-Teodoro, P. (2013, August). Survey and taxonomy of botnet research through life-cycle. ACM Computing Surveys, 45(4), Article No. 45.
Segura, V., and Lahuerta, J. (2010). Modeling the economic incentives of DDoS attacks: Femtocell case study. Economics of Information Security and Privacy, 107–119.
Smith, M. D., Bailey, J., and Brynjolfsson, E. (2000). Understanding digital markets: Review and assessment. In E. Brynjolfsson & B. Kahin (Eds.), Understanding the digital economy, pp. 99–136. Cambridge, MA: MIT Press.
Smith, V. L. (1987). Experimental methods in economics. The New Palgrave: A Dictionary of Economics, 2, 241–249.
Symantec. (2012, April). Internet security threat report. Symantec Corporation, Volume 17.
Thomas, R., and Martin, J. (2006, December). The underground economy: priceless. The USENIX Magazine, 31(6), 7–16.
Varian, H. R. (2001). High-technology industries and market structure. Proceedings from Federal Reserve Bank of Kansas City, pp. 65–101.
Vogt, R., Aycock, J., and Jacobson, M. J. (2007, February 28–March 2). Army of botnets. Proceedings of the 2007 Network and Distributed System Security Symposium, pp. 111–123.
Wang, P., Sparks, S., and Zou, C. C. (2007, April 10). An advanced hybrid peer-to-peer botnet. Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets. Retrieved from http://dl.acm.org/citation.cfm?id=1323130&CFID=509421030&CFTOKEN=28790071
Wilson, L., and Stevens, A. (2007). Understanding drug markets and how to influence them. The Beckley Foundation Drug Policy Programme Report 14.
Yan, X., and Roy, B. V. (2008). Reputation markets. Proceedings of the 3rd International Workshop on Economics of Networked Systems, pp. 79–84.
Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., and Zou, W. (2009). Studying malicious websites and the underground economy on the Chinese web. Managing Information Risk and the Economics of Security, 225–244.

BIOGRAPHIES

Zhen Li is an associate professor of economics in the Department of Economics and Management at Albion College. She holds a Master's Degree and PhD in Economics from Princeton University. She graduated with her Bachelor's Degree in International Economics from Peking University. Dr. Li's recent research interests include inter-disciplinary research study in economics and game theory of computer networks and information security, and she has published a number of articles in the field.

Qi Liao is an assistant professor in the Department of Computer Science at Central Michigan University. He received his MSc and PhD in Computer Science and Engineering from the University of Notre Dame. He graduated with a BSc and Departmental Distinction

in Computer Science from Hartwick College with a minor concentration in mathematics. His research interests include computer and network security, anomaly detection, security data analysis and visualization, and economics and game theory of cybersecurity. Dr. Liao received USENIX best paper award and other awards from National Security Innovation Competition at Colorado Springs, University of Notre Dame Center for Research Computing, and IEEE Visual Analytics Science and Technology Challenge. Dr Liao has served as international conference co-chair, on technical program committees, on journal editorial boards, and numerous times as a peer reviewer. He is a member of Kappa Mu Epsilon, Upsilon Pi Epsilon, and Tau Beta Pi.