Cybercrime and Punishment: A Rational Victim Model*

Ye Hong and William Neilson

Abstract

The idea that severe penalties effectively deter crime is at the core of theoretical work on crime and punishment in economics but is not fully supported by the empirical evidence. This paper identifies conditions under which a penalty loses deterrence power and may even exacerbates social losses. The key assumption is that the criminal can only be detected and stopped by the victim before completing the crime. It differs from the standard framework in which the apprehension is triggered after the completion of the crime. The victim in our model plays an active and critical role in deterring the criminal. In our setting we show that the public penalty imposed on apprehended criminals motivates the criminal's effort while reducing the victim's security investment. Furthermore, the criminal technology has a large influence on penalties' deterrence power.

JEL Classification: D90, K14, K24

Keywords: Cybercrime, Punishment, Deterrence, Contest

1 Introduction

Gary Becker's (1968) seminal work introduced to the economics literature the notion of a rational criminal, one who chooses whether to commit a crime based on a comparison of the expected benefits from committing it to the expected costs from possible detection and punishment. The idea proved enormously useful, and has become the standard framework for both theoretical and

*Many thanks to Dr. Gilpatric, Duc Cao, and Dr. Celik for valuable feedback. We also thank seminar participants from the Western Economic Association International and the Washington University at St. Louis.

empirical work on crime and punishment in economics. In a standard model the social planner sets both the probability and the severity of punishment to maximize social welfare, and social welfare depends on the benefits of the crime to the offender, the damage from the crime to the victims or society at large, and the costs of catching and punishing the offender. Implicit in this formulation, though, are assumptions that if the offender chooses to commit a crime he or she does so successfully with no possibility of being stopped, the victim has no way to protect him- or herself against crime, and the government is the only entity with the means to deter crime.

There are many types of crime for which these assumptions do not hold, and shoplifting provides a straightforward example. Many, if not most, merchants employ countermeasures like security tag sensors at store exits to catch shoplifting as it occurs, because once the item leaves the store there is little chance of apprehending the thief. Shoplifters know this and so take their own measures to increase their chances of getting away with the theft. Not only is the success probability of crime uncertain, it is also endogenous with both the offender and the intended victim able to influence it. Government agencies, such as the police, are unlikely to catch the offender without the merchant's help, and in many instances the police only become aware of the offender if the merchant hands the offender over to them. In short, shoplifting provides an example where the intended victim can undertake countermeasures to prevent the crime, the offender can take measures to improve his own probability of success, and the offender is unlikely to be caught and punished if the crime is successful.

Shoplifting is a very old problem, but a newer one makes this analysis much more germane. The problem is cybercrime and it is characterized by these same features. A hacker with greater skills or more advanced technology has a better chance of breaching the target's security measures, but the intended victim's countermeasures make it less likely the hacker will succeed[1]. A successful

[1]Recent studies have formulated offenders' probability of success as a function of factors controlled by both offenders and defenders. Studies about information security assume firms are self-reliant in cyber attacks (e.g. Gordon & Loeb, 2002; Huang, Hu, & Behara, 2008; Wu, Feng, Wang, & Liang, 2015). Those researchers constructed a probability of breach which can be influenced by the information system's vulnerability, the attack probability, and the information-security investment.

Another group of studies in network literature examines the optimal resources' allocation for a central planner to defend attackers in a network (e.g. Gueye, Walrand, & Anantharam, 2011; Goyal & Vigier, 2014).

Those studies examine the interaction between only two parties: the offender and the defender. They focus on the defender's optimal resource allocation, such as the security investment. This paper pays more attention to the optimal punishment and its deterrence effect. It points out in reality both the victim and the government are

hack means that the offender accesses the data without being caught, but when the security measures stop the hacker they can also lead to his identification and punishment. Far from being a passive participant in the crime, here the intended victim plays a major role in determining both the crime's success and the offender's chances of being caught and punished. To model cybercrime, one must adapt Becker's classic model to include the intended victim as a rational, active participant.

Furthermore, cybercrime can be viewed as an undesirable byproduct recent technologies developed and an evolution to traditional crimes. Although cyber crimes are comparable to some traditional crimes such as shoplifting, should we punish cyber criminals the same way as we do traditional criminals? Should we impose more severe sentences on cyber criminals because modern technologies are easy to access and offender-friendly? Without enough cybercrime convictions, judges have little to follow besides sentencing guidelines such as Computer Fraud and Abuse Act in which stiffer sentences are tied to greater social losses and deterrence power. Thus, to send strong messages to other cybercriminals, judges often impose draconian punishment. We aim to examine the common believes on cybercrime punishment by using the rational victim model adapted from Becker's economic crime model.

In this paper we construct and analyze a model with a rational hacker, a rational victim, and a social planner. The social planner moves first, setting the penalty a criminal faces when caught. The intended victim moves second, choosing the level of costly-self protection, and higher levels of self-protection make it more likely that the crime is stopped before completion. When the crime is stopped, there is some probability that the criminal is identified, but when the crime is carried through to completion, the criminal becomes impossible to punish. The hacker moves last, choosing whether to attempt the crime and, if so, the level of effort to exert toward successfully completing it[2].

defenders but they play very different roles. Moreover, we assume a successful breach implies the hacker is not detected by the security system, and therefore not being punished. By connecting the probability of breach with the probability of detection, the structure of our game differs substantially from the existing literature.

[2]According to the influential work, Staniford, Paxson, Weaver, et al. (2002), in computer security, hackers first scan the network in search for known vulnerabilities and detect what program or service is listening on that port. Once hackers gathered sufficient information regarding the network's weakness, they will send worms to exploit those vulnerabilities.

The results of the analysis differ greatly from the standard model. First, conditional on not being deterred, increases in the government-imposed penalty lead the offender to exert more effort. In other words, when the penalty for being caught rises, what criminal events that do occur tend to be executed more carefully. The intuition behind this result comes from thinking about the problem as a contest between the offender on the one hand and the intended victim and the public authority on the other. In a contest incentives are driven by the spread between the payoff upon success and the payoff upon failure, and the expected penalty increases this spread. Using our running examples, as penalties increase, data breach attempts use more sophisticated programming and violent property crimes involve more heavily-armed offenders. Because of this, increased fines can lead to reduced social welfare especially when the victim's loss is large.

Second, the penalty on apprehended criminals does not directly change the optimization problem of the victim, but it changes victim's behavior as he best-responds to hacker. An increased penalty that motivates greater hacker effort may induce the victim to put less effort into self protection if the victim is likely to lose the contest.

Third, there are circumstances under which the offender cannot be deterred, regardless of the size of the fine. This results when the size of the benefit to the offender relative to the size of the loss to the victim, together with the technology available to the offender, create a situation in which higher fines yield by the parties that ensures the offender wins. The model therefore offers a new explanation for the empirical findings of smaller deterrence effects of the expected punishment on property crimes than violent crimes (Levitt, 1995; McCrary, 2002; Evans & Owens, 2007; Lin, 2009; Chalfin & McCrary, n.d.). The model presented here fits property crimes well since victims can help with deterrence and offenders tend to be caught in the act or not caught at all. They do not fit violent crimes well where victims have less ability to prevent success and detection often occurs after the act.

When deterrence is impossible, a counterintuitive result obtains: the penalty should be as large as possible when the loss to the victim is relatively small, but the penalty should be zero when the loss to the victim is above some threshold. The reason is that when the loss to the victim is small the large penalty keeps the victim from investing too much in self-protection, but when the

loss is larger the zero penalty keeps the offender from trying so hard to succeed.

This paper proceeds as follows. Section 2 explains the game between the offender and the victim. It identifies the condition under which the hacker is not deterred regardless of the size of the fine. Section 3 investigates the optimal punishment to a domestic hacker from a social planner's view and how technology influences the punishment. Section 4 discusses the optimal punishment to a foreign hacker. Section 5 concludes the paper.

2 The game between the offender and the victim

We model the problem as a three-player sequential game between the social planner, the intended victim, and the potential hacker. The social planner moves first, setting the fine F the hacker must pay if caught. The intended victim moves second, observing F and then choosing the amount of costly security effort s to exert. This effort both reduces the probability that the crime is successful and increases the probability that the hacker is caught in the act. The potential hacker moves last, observing both F and s before deciding whether to commit a crime and, if so, how much costly effort x to exert to improve the chances of success. This section focuses on the subgame between the victim and the hacker, taking the fine as exogenous.

The probability that the crime is successful is

$$p(x,s) = \begin{cases} \frac{x}{x+s}, & \text{if } (x,s) \neq (0,0) \\ \frac{1}{2}, & \text{if } (x,s) = (0,0) \end{cases} \tag{1}$$

This is the standard contest success function introduced by Tullock (1980). The probability of a win is a funciton of the hacker and the victim's effort. Increases in the hacker's effort make success more likely while increases in the victim's security effort s make it less likely. Also, the success function is concave in x and convex in s, with $p_{xx} < 0$ and $p_{ss} > 0$. Results of our model relies on the nature of this type of contest rather than a specific contest success functional form. Skaperdas (1996) illustrates axiomatic foundations for the Tullock contest function.

The hacker is risk neutral and chooses both whether to commit a crime and how much effort

to provide if he does. His expected payoff from attempting a crime is given by

$$H(x) \equiv p(x,s)B - \frac{1}{\beta}x - (1 - p(x,s))F, \tag{2}$$

where B is the benefit he receives if the crime is successful, the cost of effort is x/β, and F is the *expected* fine he pays if he is unsuccessful. An expected fine captures the idea that when the victim stops the crime, doing so may or may not lead to a case the authorities want to prosecute. The expected fine combines both the probability of successful prosecution and the nominal fine if convicted. The parameter β captures the impact of the hacker's technology, and with better technology the hacker can achieve the same success probability at lower cost.

The hacker maximizes $H(x)$ subject to the constraint $x \geq 0$, reflecting the fact that effort cannot be negative.[3]

Conditional on choosing to commit a crime, the hacker's best-response function is

$$x^*(s,F) = \begin{cases} \sqrt{s(B+F)\beta} - s & \text{for} \quad F > \frac{s}{\beta} - B \\ 0 & \text{for} \quad F \leq \frac{s}{\beta} - B \end{cases} \tag{3}$$

When s is sufficiently small, the hacker's maximization problem has an interior solution, but when s is large the hacker goes to the corner solution of $x^* = 0$. Without discussing whether the hacker is deterred by the victim's effort and the fine, for now, we simply assume this corner solution is still conditional on the hacker attempting the crime; he just attempts it without exerting any effort toward being successful[4].

The expression yields some counterintuitive behavior. Rearranging the conditions governing which piece of the function $x^*(s)$ pertains, one finds that the hacker exerts positive effort when the fine is large ($F > \frac{s}{\beta} - B$) but zero effort when the fine is small ($F \leq \frac{s}{\beta} - B$). Additionally, the hacker's benefit B and the expected fine F appear only together. These two outcomes are related. Committing the crime successfully leads to gaining B, but it also means avoiding detection and

[3] $H''(x) = p_{xx}(x^*, s)(B + F) < 0$, with the inequality holding because the Tullock success function has $p_{xx} < 0$. This guarantees that an interior solution is a maximum.

[4] Since the optimal s is strictly positive as being proved in proposition 1, the hacker is deterred when the optimal effort is 0.

escaping the penalty F. Because of this, the total value of success is $B + F$, and this result comes entirely from the fact that to be prosecuted the hacker must be caught in the act. Overall, the fine affects the hacker's decision in two ways: (i) the fine increases the expected cost and therefore reduces the hacker's payoff from engaging the crime. (ii) the fine reduces the probability of detection because it motives the hacker to work harder to avoid being punished.

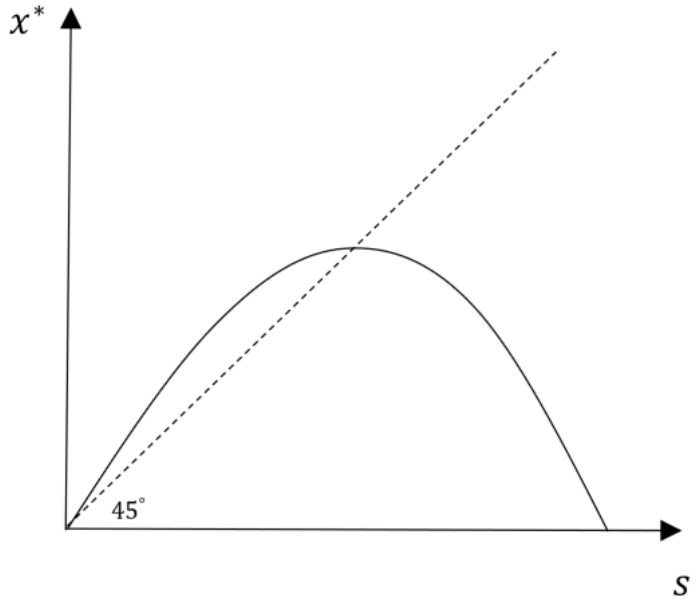


Figure 1: The relationship between the hacker's optimal effort and the victim's security investment

From expression (3) it also becomes clear that increases in the expected fine make the hacker exert more effort, irrespective of the security level chosen by the victim. He may or may not exert more effort when the victim's security level rises, since $dx^*/ds = (x^* - s)/2s$, hacker effort increases when the victim employs stronger security measures if and only if $s \leq (B + F)\beta/4$. Noting that $x^*((B + F)\beta/4, F) = (B + F)\beta/4$, when viewed in Figure 1 with hacker effort x on the vertical axis and victim effort s on the horizontal one, the hacker's best-response function is hump-shaped and reaches a maximum where it crosses the 45-degree line.

The hacker's reservation payoff is zero, and thus he chooses to attempt the crime if and only if $H(x^*(s, F)) > 0$. Thus, the hacker is deterred when the participation constraint is violated.

The victim suffers a loss L when the hacker succeeds, but she can reduce the probability of a

loss by investing more in security. The victim's expected loss is given by

$$V(x, s) \equiv p(x, s)L + s. \tag{4}$$

The victim must pay the cost of increasing s, but doing so reduces the probability of suffering the loss, L. The timing of the game prescribes that the victim moves before the hacker, and in a subgame perfect equilibrium the hacker best-responds to the victim's choice and the expected fine set by the authorities. Consequently, the victim chooses s to minimize $V(x^*(s, F), s)$, and let $s^*(F)$ denote the solution to this problem.[5] One can compute

$$s^*(F) = \begin{cases} \frac{L^2}{4(B+F)\beta} & \text{for} \quad F > \frac{L}{2\beta} - B \\ (B + F)\beta & \text{for} \quad F \leq \frac{L}{2\beta} - B \end{cases} \tag{5}$$

As before, this expression assumes implicitly that the hacker attempts a crime, although the hacker might not exert any effort to make it successful.[6] The top line of expression (5) reflects values of the parameters for which s^* remains low enough for the hacker to exert positive effort, and the bottom line reflects parameter values for which the hacker goes to the corner solution $x^* = 0$. The first result follows immediately from expression (5).

Proposition 1. *The victim always invests a strictly positive amount in security (that is, $s^*(F) > 0$ for all F).*

Proof. Suppose to the contrary that the victim chooses $s = 0$. The hacker observes this before making any decisions, and by choosing any $x > 0$ commits a successful crime with probability $p = 1$. Thus, by setting $s = 0$ the victim's payoff is $V(\cdot, 0) = -L$. On the other hand, if the victim makes the security investment according to $s^*(F)$ in expression (5), the hacker's success probability is always smaller than 1. Furthermore, $s^*(F) \leq L/2$ for all F, and attains that value

[5]The second-order condition is

$$\frac{d^2V(x^*(s), s)}{ds^2} = \frac{L}{4\beta^{\frac{1}{2}} s^{\frac{3}{2}} (B + F)^{\frac{1}{2}}} > 0.$$

[6]The conditions for the two parts of expression (5) match the conditions for the two parts of (3) but rearranged so that they relate to the fine, not the level of security chosen by the victim.

when $B + F = L/2\beta$. Consequently, by setting the security level according to (5) the victim's expected payoff is always greater than $-L/2$, and the victim prefers positive effort to zero effort no matter what fine is set. □

A rational victim always engages in some self-protection. When the fine is zero the victim invests $B\beta$ in security, and as F increases that investment rises linearly. It peaks at $s^*(L/2\beta - B) = L/2$, and then decreases tangentially to zero beyond that. Importantly, the most the victim ever pays for security is half of the potential loss from a successful crime. Because the security investment is strictly positive the hacker's probability of success is 0 when he exerts 0 effort. Since 0 effort brings $-F$ payoff to the hacker, he will not attempt the crime. Therefore, the bottom line of expression (3) indicates the hacker is deterred by the victim's effort. As (5) shows security investments and fines are strategic complements under the condition that the hacker is deterred by the security system; otherwise, they are strategic substitutes with increases in the government-set penalty partially crowding out the victim's investment in self-protection. The intuition behind stems from the nature of the contest. The fine motivates the hacker's effort in this asymmetric contest, and when the fine is small, the hacker is not sufficiently motivated, therefore the victim is willing to devote more effort to deter the hacker. However, the victim behaves this way until the fine reaches a certain level in which the hacker is sufficiently motivated. The victim will respond passively because the costly security effort outweighs the loss caused by the cyber attack that could be reduced.

The victim's effort, combined with potential fines from successful prosecution, may or may not deter the hacker from attempting the crime in the first place. To see when the hacker is deterred, that is, when $H(x^*(s^*(F), F)) \leq 0$, begin by substituting (5) into (3):

$$x^*(s^*(F), F) = \begin{cases} \frac{L}{4(B+F)}(2(B+F) - \frac{L}{\beta}) & \text{for} \quad F > \frac{L}{2\beta} - B \\ 0 & \text{for} \quad F \leq \frac{L}{2\beta} - B \end{cases} \tag{6}$$

In equilibrium the hacker exerts effort only when the benefit and fine combine to be sufficiently large, consistent with the finding that the benefit and fine together represent the payoff difference between a successful and an unsuccessful crime.

Substituting both $s^*(F)$ and $x^*(s^*(F), F)$ into the success function $p(x, s)$ yields the hacker's equilibrium probability of success:

$$p(x^*(s^*(F), F), s^*(F)) = \begin{cases} 1 - \frac{L}{2(B+F)\beta} & \text{for} \quad F > \frac{L}{2\beta} - B \\ 0 & \text{for} \quad F \leq \frac{L}{2\beta} - B \end{cases} \tag{7}$$

This expression shows two things. First, in equilibrium and conditional on him attempting a crime, the hacker's success probability increases with both the fine and the benefit from the crime, and it decreases with the severity of the victim's loss. Second, when the loss to the victim is large enough that the hacker exerts no effort, the hacker's success probability is zero. Third, the hacker's technology increases the probability of crime completion and makes the deterrence unlikely.

Substituting this into $H(x)$ from (2) yields

$$H(x^*(s^*(F))) = \begin{cases} \frac{(2B - L/\beta)^2 + 4F(B - L/\beta)}{4(B+F)} & \text{for} \quad F > \frac{L}{2\beta} - B \\ -F & \text{for} \quad F \leq \frac{L}{2\beta} - B \end{cases} \tag{8}$$

This allows us to identify the equilibrium participation condition.

Proposition 2. *In equilibrium, if $B > L/\beta$ the hacker attempts a crime for any value of F. If $L/2\beta \leq B \leq L/\beta$ the hacker attempts a crime if*

$$F < \frac{\left(\frac{L}{\beta} - 2B\right)^2}{4\left(\frac{L}{\beta} - B\right)} \tag{9}$$

and does not attempt a crime otherwise. If $B < L/2\beta$ the hacker does not attempt a crime.

Proof. Before beginning the three different cases, we offer the following preliminaries. First, if the hacker attempts a crime he also chooses $x > 0$, because if not his probability of success is $p = 0$ and his expected payoff is $H = -F < 0$. This means that the condition $F > L/2\beta - B$ must hold so that the top line of expression (8) describes utility. Second, differentiating the top line of

expression (8) with respect to F yields

$$\frac{\partial H}{\partial F} = -\frac{L^2}{4\beta^2(B+F)^2} < 0,$$

and so $H(x^*(s^*(F)))$ is decreasing in F.

If $B > L/\beta$ then from (8) it follows directly that $H(x^*(s^*(F))) > 0$ for all $F \geq 0$. Further, $L/2\beta - B < 0$ holds, so any nonnegative fine is larger than $L/2\beta - B$, as required.

If $L/2\beta \leq B < L/\beta$, then again any nonnegative fine is larger than $L/2\beta - B$. Also,

$$H(x^*(s^*(0))) = \frac{(2B - L/\beta)^2}{4B} > 0.$$

Solving $H(x^*(s^*(F_0))) = 0$ for F_0, and calling the result yields

$$F_0 = \frac{\left(\frac{L}{\beta} - 2B\right)^2}{4\left(\frac{L}{\beta} - B\right)}$$

and $F_0 > 0$ since $B < L/\beta$. Since H is decreasing in F, it follows that $H(x^*(s^*(F))) \geq 0$ for all $F \in [0, F_0]$.

Finally, let $B < L/2\beta$ and suppose, to the contrary, that the hacker attempts a crime. He must exert positive effort, otherwise his payoff is $-F < 0$, and so it must be the case that $F > L/2\beta - B$. As before, H decreases in F and $H = 0$ when the fine is set to F_0. Thus, for the hacker to have $H > 0$ so he attempts a crime and $x > 0$ so that he exerts effort for it to succeed, the fine must satisfy

$$\frac{L}{2\beta} - B < F < \frac{\left(\frac{L}{\beta} - 2B\right)^2}{4\left(\frac{L}{\beta} - B\right)}.$$

However, dividing both the left and right sides of the above expression by the left side yields

$$1 < \frac{\frac{L}{\beta} - 2B}{2\left(\frac{L}{\beta} - B\right)}.$$

But since $L/\beta - B > 0$, this becomes

$$2\frac{L}{\beta} - 2B < \frac{L}{\beta} - 2B,$$

which implies that $L/\beta < 0$, a contradiction. Consequently, the hacker does not attempt a crime when $B < L/2\beta$. □

Propositon 2 shows clearly the differences between the standard, rational hacker model and the rational victim model of this paper. In the standard model the hacker commits a crime if the expected benefit outweighs the expected cost. Increasing the expected punishment raises the expected cost of committing a crime, and if the fine becomes sufficiently large the hacker is deterred. Put more starkly, in the standard model the hacker can always be deterred by a large-enough fine.

In the rational victim model, though, this is no longer true. When the hacker's benefit from crime B is sufficiently large (greater than L/β), it is impossible to deter him. When the benefit is sufficiently small (less than $L/2\beta$) no fine is needed to deter the hacker, because sufficient deterrence is provided by the hacker's effort cost coupled with the victim's impact on the chances the crime succeeds. Only when B lies in an intermediate range does the expected punishment play a role in deterrence, and here it has the usual result that a sufficiently large fine deters crime.

The equilibrium outcomes of the subgame are characterized by the victim's participation decision in Proposition 2, his effort choice described by expression (6), and the victim's effort choice described by expression (5). With these it is possible to see how changing some of the parameters impacts the outcome of the subgame.

Suppose that the hacker's technology improves. This could occur, for example, if a hacker acquires better and faster hardware. The improved technology increases β, and it has the following effects. First, not surprisingly, it expands the range of L for which the hacker attempts a crime. It also expands the range over which the hacker cannot be deterred. Second, conditional on attempting a crime, the hacker exerts more effort as seen in expression (6). Third, from expression (5), the victim invests less in security conditional on the hacker participating. Finally, the improved

technology makes it more likely that the attempted crime succeeds in equilibrium, as shown in expression (7).

Similar results can be found from a change in the size of the victim's potential loss L or the size of the hacker's potential benefit B. As the crime becomes more costly for the victim, the victim invests more in security, the hacker is less likely to attempt a crime, and an attempted crime is more likely to fail. As the crime becomes more beneficial to the hacker, though, the set of circumstances under which he attempts a crime expands, he exerts more effort when he attempts one, the victim invests less in security when the size of the potential loss is sufficiently low, and the crime is more likely to succeed.

Proposition 2 can also be used to explore the effect of a change in the expected fine F, but that variable is set by the authority and therefore endogenous in the game as a whole. How to punish crimes when the hacker must be caught in the act and must be caught by the victim is the subject of the next section.

3 Deterrence and Punishment

At the beginning of the game, before the victim sets the security level and the hacker decides whether to attempt a crime and how much effort to devote to it, the social planner sets the level of the expected fine. Before discussing the optimal penalty structure, though, it is useful to compare the setting briefly with the standard rational criminal model.

In that model the social planner moves first, setting the probability and severity of punishment. In our setting those two parameters are collapsed into a single entity, the expected fine F. The hacker observes F and chooses whether to commit a crime. Doing so results in a benefit to him of B and a loss to society of L. The victim's role in the problem is passive, and the hacker's effort decision is binary, making it simply a participation decision.[7] He chooses to commit the offense if $B - c - F > 0$, where c is the effort cost associated with commiting the crime and 0 is his reservation payoff. It is straightforward from this setup that a sufficiently large expected fine

[7]It is possible to obtain the standard model from the framework in the preceding section by constraining the victim's effort to $s = 0$ and setting a minimum effort level $x_0 > 0$ that the hacker must meet or exceed if he exerts positive effort. Then the hacker's objective function is simply $H(x) = B - x_0/\beta - F$, where F is the *expected* fine.

deters crime, so that when $F \geq B - c$ the hacker chooses not to commit the crime.

The rational victim model we explore here does not share the result that a sufficiently large fine deters crime. In fact, large fines can encourage, not discourage crime, when the hacker cannot be deterred, and the simplest way to see this is by exploring the limit as $F \to \infty$. Suppose that $B > L/\beta$ so the hacker always attempts a crime. From expression (5), $lim_{F\to\infty} s^*(F) = 0$. From expression (7) the hacker's equilibrium probability of success has $lim_{F\to\infty} p = 1$. Consequently, as the fine increases without bound, the victim's security investment approaches zero and the hacker's chance to succeed approaches one.

There are two factors that drive these results. One is that the hacker avoids punishment by committing the crime successfully and only pays the fine if the crime is unsuccessful. This makes the criminal's total benefit from a successful crime $B + F$, the direct benefit B and the avoided penalty F. As the fine grows, so does the incentive for the hacker to succeed. The second factor comes from the fact that penalties crowd out the victim's own efforts at self-protection. As the expected penalty grows, the victim's effort approaches to zero, and that increases the hacker's success probability close to one. Since crimes are always successful, the hacker always commits them, and the large penalty has no deterrent effect.

In general, the social planner chooses F to minimize social loss, given by

$$W(F) = \begin{cases} W^C(F) \equiv p(x,s)(\alpha L - B) + \frac{1}{\beta}x + s & \text{when crime attempted,} \\ W^D(F) \equiv s & \text{when no crime attempted.} \end{cases} \tag{10}$$

The first line identifies the social loss function $W^C(F)$ that pertains when the hacker attempts the crime, and the second line identifies the social loss function $W^D(F)$ which pertains when the hacker is deterred. Whether a crime is attempted is endogenous and determined by the hacker, who moves last in the game. The expression αL captures both the direct loss to the victim, L, combined with any externalities stemming from the crime, and $\alpha \geq 1$. The first term in expression (10) is the probability that the crime succeeds times the net loss it generates, and it recognizes that the benefit to the hacker offsets losses to the victim. The last two terms are effort costs, with x/β the effort cost borne by the hacker and s the security investment made by the victim. The

penalty is a transfer from the hacker to others in society (but not just to the victim) so it has no impact on social welfare, and expression (10) implicitly assumes that fines can be administered costlessly. When the hacker elects not to attempt a crime, there are no losses from the crime and no effort costs by the hacker, but the victim must still pay for the security investment.

Proposition 3. *The optimal penalty is given by*

$$F^*(B,L,\beta) = \begin{cases} \bar{F} & \text{for } 2\beta B \geq L > \beta B \text{ or } L < \frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}} \\ 0 & \text{otherwise.} \end{cases}$$

In a subgame perfect equilibrium the social planner correctly predicts how the victim and hacker respond to the expected fine and each other, and so (10) should incorporate their behavior from the ensuing subgame. The social planner must decide whether or not to deter the crime, and so the two cases must be analyzed separately.

When crime is deterred, expression (10) shows that social loss is simply the security expenditure by the victim. From expression (5), when the hacker exerts zero effort the optimal security level is $(B+F)\beta$, which increases in the fine. Thus, conditional on a desire to deter crime, the social planner should set the fine as low as possible when $B < L/2\beta$.

Proposition 2 identifies two sets of circumstances under which the hacker can be deterred. When $B < L/2\beta$ the hacker can be deterred with a zero fine, but when $L/2\beta \leq B < L/\beta$ a positive fine is needed and it should be as large as possible so that the security investment can be reduced. Proposition 1 states that there is no equilibrium in which the victim invests nothing in security, and therefore we exclude the case that the victim's security approaches to 0 as the expected fine goes to infinity. To guarantee the existence of an equilibrium, assume that there is a maximal fine $\bar{F}$ and the social planner minimizes $W(F)$ subject to the constraint that $0 \leq F \leq \bar{F}$[8]. This leads to the conditional fine function $F^D(B,L,\beta)$ that applies when the social planner chooses to deter the crime:

$$F^D(B,L,\beta) = \begin{cases} 0 & \text{for} \quad B < \frac{L}{2\beta} \\ \bar{F} & \text{for} \quad \frac{L}{2\beta} \leq B < \frac{L}{\beta} \end{cases}$$

[8]Assume $\bar{F} \geq \frac{(\frac{L}{\beta}-2B)^2}{4(\frac{L}{\beta}-B)}$. This threshold is denoted as F_0 in proposition 2.

Note that it only applies when $B < L/\beta$ because otherwise deterrence is impossible.

When the social planner elects not to deter the crime, or when deterrence is impossible, the fine is set to minimize the first term in expression (10). Substituting from expressions (6), (5), and (7), differentiating with respect to F, and simplifying yields

$$\frac{\partial W^C(F)}{\partial F} = \frac{L}{2\beta(B+F)^2}[L(\alpha + \frac{1}{2\beta} - \frac{1}{2}) - B]. \tag{11}$$

The above expression has two noteworthy features. First, the denominator is always positive, and so the sign of the slope of $W^C(F)$ is determined by the term in parentheses on the right. Second, F appears nowhere in that term, and so the social loss function either increases everywhere or decreases everywhere. This means that the fine is either maximal or minimal. It should be maximal if $W^C(F)$ slopes downward and minimal if it slopes upward. Conditional on the social planner electing not to deter the crime, the optimal fine is

$$F^C(B, L, \beta, \alpha) = \begin{cases} 0 & \text{for} \quad L \geq \frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}} \\ \bar{F} & \text{for} \quad L < \frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}} \end{cases}$$

This leads to the following results.

Proposition 4. *In the range of parameters that the hacker is not deterred, F is nonincreasing in L. When criminal technology is sufficiently advance and the victim's loss is large, F is more likely to increase the social loss.*

Proof. Comparing the conditions for the optimal fine with the condition for not being deterred, the magnitude of each condition depends on the externality parameter α and the technology parameter β.

Suppose

$$\frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}} \leq \beta B$$

then,

$$\alpha + \frac{1}{2\beta} - \frac{1}{2} \geq \frac{1}{\beta}$$

$$\beta \geq \frac{1}{2\alpha - 1}$$

When it holds,

$$F^C(B, L, \beta, \alpha) = \begin{cases} 0 & \text{for} \quad L \geq \frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}} \\ \bar{F} & \text{for} \quad L < \frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}} \end{cases}$$

The result holds because the cutoff $L = \frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}}$ is within the set of not being deterred, $\{L|L < \beta B\}$. The piecewise function above shows the optimal fine should be 0 when the loss to the victim is larger than the cutoff conditional on the hacker is not deterred, therefore F^C is nonincreasing in L. Likewise, the optimal fine is nondecreasing in B and β and is nonincreasing in α.

Mathematically, let $L_n = \frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}}$ and $L_{n+1} = L_n - \epsilon$ where $\epsilon > 0$, so the sequence $\{L_n\}$ is decreasing. Plug L_n and L_{n+1} into the piecewise function $F^C(B, L, \beta, \alpha)$, we find

$$F^C(B, L_n, \beta, \alpha) = 0 < F^C(B, L_{n+1}, \beta, \alpha)$$

Let $k > 1$, we find

$$F^C(B, L_n, \beta, \alpha) = F^C(B, L_{n-k}, \beta, \alpha) = 0$$

$$F^C(B, L_{n+1}, \beta, \alpha) = F^C(B, L_{n+k}, \beta, \alpha) = \bar{F}$$

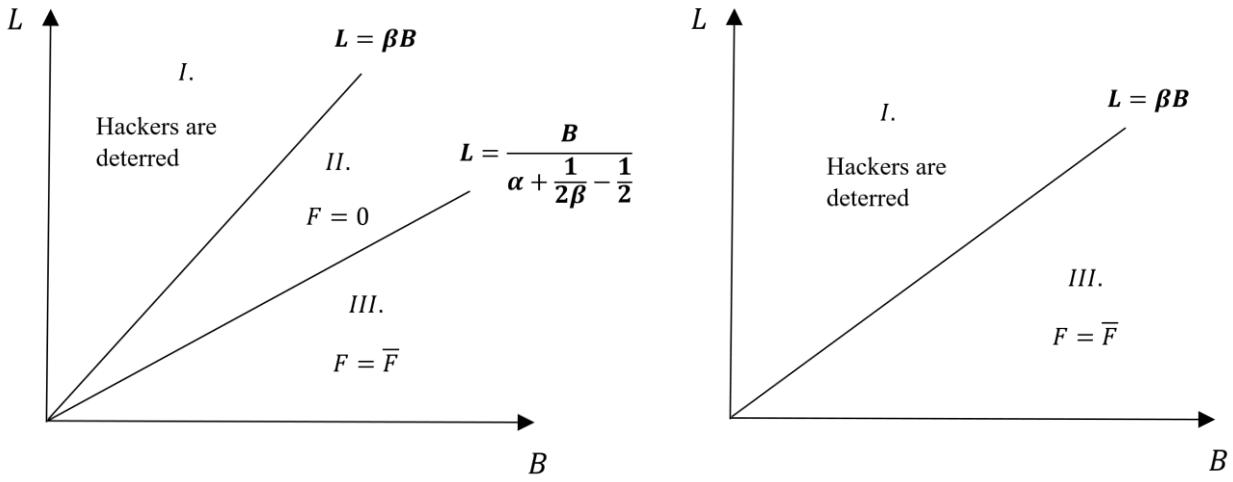
Thus, we conclude $F^C(B, L, \beta, \alpha)$ is nonincreasing in L.[9]

Otherwise, when $\beta < \frac{1}{2\alpha - 1}$

$$F^C(B, L, \beta, \alpha) = \bar{F}$$

The cutoff $L = \frac{B}{\alpha + \frac{1}{2\beta} - \frac{1}{2}}$ is beyond the set of not being deterred, $\{L|L < \beta B\}$. In this case, the optimal fine conditional on the hacker cannot be deterred is independent to L. □

[9]Mathematical proof for $F^C(B, L, \beta, \alpha)$ is nondecreasing in B and nonincreasing in α can be found in appendix.



(a) $\beta \geq \frac{1}{2\alpha-1}$ (b) $\beta < \frac{1}{2\alpha-1}$

Figure 2: Optimal Fine when Hackers are not Deterred

Most of these results are counterintuitive. Crimes involve advanced criminal technology and create large loss externality are included in Figure (2a). As it shows, holding everything else constant, when the loss L from the crime is sufficiently small the optimal fine is the maximal one, but as L grows the optimal fine eventually switches to zero. A more intuitive result would associate more damaging offenses with higher penalties, but the opposite holds here. The reason is that the fine crowds out the victim's security investment, but only the victim can stop the crime and lead to the apprehension of the criminal. As the damages grow, the socially-optimal policy is abstain from punishing hackers in order to incentivize victims to protect themselves.

When the benefit B to the hacker is sufficiently small, the optimal fine is zero. As B grows,the optimal fine eventually becomes maximal. While this seems intuitive that a larger penalty should associate with a crime that benefits the hacker more, the reason is counterintuitive. The intuitive reasoning relies on deterrence as a channel, but this result pertains only when the penalty losses the deterrence power. Instead, social welfare gains from the large fine exist because it crowds out some of the victim's security investment. An extreme case arises when $B > \alpha L$ so that a successful crime benefits the hacker more than it hurts the victim and the rest of society. The success probability p^* in expression (7) increases in F, so the maximal fine also maximizes the chance that the crime succeeds.

Figure (2b) includes crimes without advanced criminal technology and large loss externality. It

shows the fine is always maximal if the criminal is not deterred. Using our running examples, when the shoplifter's benefit is greater than the stolen store's loss, the shoplifter will attempt the crime although facing a severe punishment. And the maximal penalty is still optimal even though the shoplifter is not deterred by any penalty. However, the severe punishment is not always optimal for cybercrime. As the criminal's technology evolves, accessing other people's properties is much easier through the internet, the vulnerability of one port can put all the neighbor ports in danger and therefore generate a huge negative externality. Penalties are more likely losing the deterrence power. When the criminal cannot be deterred, he should also not be punished if the loss to the victim is large.

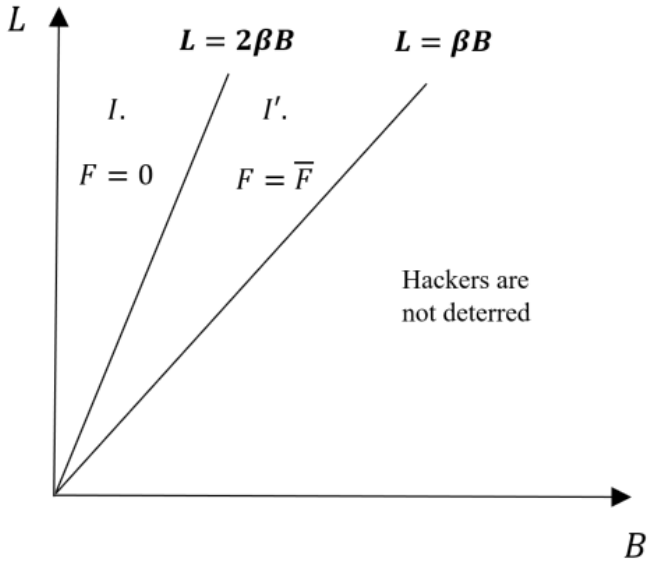


Figure 3: Optimal Penalty when Hackers are deterred

When the social planner elects to deter the crime, the likelihood that the hacker can be deterred relies on the technology he obtained. As Figure 3 shows the likelihood of deterrence decreases as the hacker obtains a better criminal technology (large β). The intuition for that result is straightforward. Better technology reduces the hacker's cost so he is more likely to attempt the crime. The optimal fine again increases with the criminal benefit and decreases with the victim's loss. Because when the criminal benefit is not too large or too small, the penalty regains the deterrence power and the hacker is deterred by a combination of the fine and the victim's effort. If crimes in region I' cannot be deterred by the maximal fine, that part of the region will merge

with the region in which hackers are not deterred (see appendix).

4 A foreign hacker

The preceding section analyzed optimal policy under the assumption that the offender is part of society and so his benefits and costs matter to social welfare. For some crimes, especially cybercrimes, it is possible for the hacker to live in a foreign country, in which case his benefits and costs would not enter social welfare. We analyze that situation in this section.

The social loss function becomes

$$W(F) = \begin{cases} W^C(F) \equiv p(x,s)\alpha L + s - (1 - p(x,s))F & \text{when crime attempted,} \\ W^D(F) \equiv s & \text{when no crime attempted.} \end{cases} \tag{12}$$

The equation is exactly the same when the social planner opts for deterrence, but it is different from before when the social planner elects not to deter. The foreign hacker's criminal benefit is not relevent to the social loss. But the fine is a monetary transfer from a foreign country so it reduces the social loss.

Following arguments like those above, compute

$$\frac{\partial W^C(F)}{\partial F} = \frac{L^2(2\alpha - 1) + 2L}{4(B+F)^2\beta} > 0, \tag{13}$$

where the inequality holds because $\alpha \geq 1$. This means that the social loss is always increasing with the size of the fine, and so when the penalty has no deterrence power, the optimal fine is zero. This leads to the following result.

Proposition 5. *When the social planner is indifferent to the hacker's welfare, the optimal fine is given by*

$$F^*(B, L, \beta) = \begin{cases} \bar{F} & \textit{for } L/2\beta \leq B < L/\beta \\ 0 & \textit{otherwise.} \end{cases}$$

When the hacker is foreign the social planner wants to deter the crime whenever possible. When deterrence is possible the social planner sets the fine at the lowest level possible that will

still deter the hacker. When deterrence is impossible the social planner sets the fine at zero in order not to motivate the hacker to work harder.

5 Conclusion

The paper considers a situation with a rational hacker and a rational victim. The victim can invest in security that not only increases the chance that the hacker's attempt at crime fails, but also leads to punishment of the hacker by an authority. However, the severe punishment provides incentives to the wrong player at the game, the hacker. The primary result is that unless the crime is very beneficial to the criminal, and assuming that the social planner cares about that benefit, optimal fines are as small as possible. Another major result is that there are circumstances under which deterrence is impossible even when fines are sufficiently large.

When constructing the optimal public punishment, for crimes discussed in this paper, the law and enforcement must consider the loss to the victim, the criminal benefit as well as the technology available to the criminal and the scale of the crime. Because under certain conditions, severe punishment cannot deter criminals but exacerbates the social loss. Nowadays, the modus operandi of criminals has changed substantially as a result of the development of internet. Traditional crimes, such as robbery, appear in a new electronic version (e.g., online banking fraud) and are facilitated by the Internet. According to the yearly Internet Crime Report, the reported loss in the U.S. rose dramatically from less than 18 million dollars in 2001 to over 1.4 billion in 2016. The indirect and defense costs for cyber crimes are much higher than that. Although cybercrime has become a threat, legislation is relatively vague about this type of crime compared to traditional crimes. Sometimes the punishment can be shockingly severe. For example, although downloading millions of articles from JSTOR without permission is a non-violent crime, an individual faces the possibility of decades in jail and backbreaking penalties; in contrast, violent crimes, such as rape carry much lighter sentences. The results of this paper suggest hackers with advanced knowledge or computing power are unlikely being deterred regardless of the severity of the penalty. Compare to hacking the information system of a company, a hacker steals information from a personal computer should be punished more severely. Not only the former crime has a large scale, but the

loss to the victim tends to be large. The reason stems from incentives a fine provides. When the victim's loss is small the central planner should set a large fine so the victim will reduce the costly security investment. As the victim's loss rises and eventually outweighs the cost on security investment, no fine should be imposed on the hacker. So the hacker will not work harder to avoid being punished and the victim will not be passive in protecting herself. Regard to the deterrence power of the public punishment, a government can develop technologies to reduce security's cost and on changing the structure of network connections.

In general, problems focus more on the behavior of the prospective victim than the prospective offender are within the scope of this rational victim model. The practice of citizens owning and carrying guns is becoming more and more prevalent in the United States as Americans realize "the police do not owe a specific duty to provide police services to citizens based on the public duty doctrine". After Warren v. District of Columbia; 444 A.2d. 1, D.C. Ct. of Ap. (1981) and Castle Rock v. Gonzales, 545 U.S. 748 (2005), thirty three states have enacted some form of stand-your-ground law. The common rationale for allowing citizens to carry gun is to help deter crime against them and others nearby. Our model suggests when the expected punishment from law and enforcement is low, the private security investment inevitably rises; the stand-your-ground law shifts the right of punishment from law and enforcement to citizens' hands , which restores the deterrence power to the punishment.

In conclusion, we should note several issues that were not addressed here. For one, we assume hackers only commit one crime, so incapacitation is not an issue. One may convert our model into a dynamic search model and incorporate the cost of recidivism in the social loss. For another, further crimes would need new analysis. Once new methods for law and enforcement to identify cyber criminals are invented, police may become less dependent on the victims' effort. The latest technologies of quantum communication and block chain can help build a more secured network, and therefore, eliminating many cyber crimes such as identity theft and data breach. As might be expected, crimes may evolve toward some types that are strengthened by the new technology, for example, human trafficking, drug selling, and so on, for the reason that online transactions will be more secure than before. After all, new crimes will grow from other platforms that disadvantages

the defender, and if the gaming structure of the new crimes changes we probably need new models to describe them.

6 Appendix

Properties of the objective functions:

$$H(x,s) \equiv p(x,s)B - \frac{x}{\beta} - (1-p(x,s))F \tag{14}$$

The FOC is

$$p_x(x^*,s)(B+F) - \frac{1}{\beta} = 0 \tag{15}$$

Notice the fine increases linearly, the increasing rate p_x decreases and converges to 0.

$$x^*(s) = \sqrt{s(B+F)\beta} - s \tag{16}$$

The SOC is

$$p_{xx}(x^*,s)(B+F) < 0 \tag{17}$$

The slope for offender's best response (best response to security level and central planner's penalty) function is found through

$$(p_{xx}\frac{dx^*}{ds} + p_{xs})(B+F) = 0 \tag{18}$$

$$\frac{dx^*}{ds} = -\frac{p_{xs}}{p_{xx}} = \frac{x-s}{2s} \tag{19}$$

$$p_{xx}\frac{dx^*}{dF}(B+F) + p_x = 0 \tag{20}$$

$$\frac{dx^*}{dF} = -\frac{p_x}{p_{xx}(B+F)} = \frac{x+s}{2(B+F)} > 0 \tag{21}$$

The firm will take offender's decision x^* into consideration. And firm chooses s to minimize

$$S(x^*, s) \equiv p(x^*, s)L + s \tag{22}$$

The FOC is

$$[p_x(x^*, s^*)\frac{dx^*}{ds} + p_s(x^*, s^*)]L + 1 = 0 \tag{23}$$

$$s^* = \frac{L^2}{4(B+F)\beta} \tag{24}$$

Plug s^*

$$x^* = \frac{L}{2} - \frac{L^2}{4(B+F)\beta} \tag{25}$$

The SOC is

$$p_{xx}(\frac{dx^*}{ds})^2 + 2p_{xs}\frac{dx^*}{ds} + p_x\frac{d^2x^*}{ds^2} + p_{ss} = \frac{L}{4s^{\frac{3}{2}}(B+F)^{\frac{1}{2}}\beta^{\frac{1}{2}}} > 0 \tag{26}$$

The slope for firm's best response (best response to the penalty) function is

$$\frac{ds^*}{dF} = -\frac{L^2}{4(B+F)^2\beta} < 0 \tag{27}$$

Proof for proposition 3: The central planner chooses an optimal fine that minimizes the social loss.

$$W^c(F) = p(x, s)(\alpha L - B) + \frac{x}{\beta} + s \tag{28}$$

The FOC is

$$\frac{L}{2\beta(B+F)^2}[L(\alpha + \frac{1}{2\beta} - \frac{1}{2}) - B] \tag{29}$$

The SOC is

$$-\frac{L}{\beta(B+F)^3}[L(\alpha + \frac{1}{2\beta} - \frac{1}{2}) - B] \tag{30}$$

Unless $B = L(\alpha + \frac{1}{2\beta} - \frac{1}{2})$, the FOC and SOC hold the opposite sign. The social loss either increasing at a decreasing rate or decreasing at an decreasing rate.

A side proof for proposition 3: Consider the case that the penalty is costly (marginal cost

of F is γ)

$$W^c(F) = p(x,s)(\alpha L - B) + \frac{x}{\beta} + s + rF \tag{31}$$

The FOC is

$$r + \frac{L}{2\beta(B+F)^2}[L(\alpha + \frac{1}{2\beta} - \frac{1}{2}) - B] \tag{32}$$

The SOC is

$$-\frac{L}{\beta(B+F)^3}[L(\alpha + \frac{1}{2\beta} - \frac{1}{2}) - B] \tag{33}$$

When $B\beta > L \geq \frac{B}{\alpha+\frac{1}{2\beta}-\frac{1}{2}}$, the optimal penalty would be 0, $F^* = 0$; when the penalty is social costless such as a monetary fine ($\gamma = 0$) and $L < \frac{B}{\alpha+\frac{1}{2\beta}-\frac{1}{2}}$, the optimal penalty would be at the maximum, $F^* = \bar{F}$. When enforcing the penalty generates a cost to the society($\gamma > 0$), the optimal penalty varies in accordance with the offender's technology endowment, externality of the illegal activity, the expected gain and loss, and the cost of enforcing the penalty, $F^* = \sqrt{\frac{L[B+(\frac{1}{2}-\frac{1}{2\beta}-\alpha)L]}{2\gamma\beta}} - B$. The optimal penalty decreases with the cost of the penalty.

Proof for proposition 4: F is nondecreasing in B. Let $B_n = L(\alpha+\frac{1}{2\beta}-\frac{1}{2})$ and $B_{n+1} = B_n+\epsilon$ where $\epsilon > 0$, so the sequence $\{B_n\}$ is increasing. Plug B_n and B_{n+1} into the piecewise function $F^C(B, L, \alpha)$, we find

$$F^C(B_n, L, \alpha) = 0 < F^C(B_{n+1}, L, \alpha)$$

Let $k > 1$, we find

$$F^C(B_n, L, \alpha) = F^C(B_{n-k}, L, \alpha) = 0$$

$$F^C(B_{n+1}, L, \alpha) = F^C(B_{n+k}, L, \alpha) = \infty$$

Thus, we conclude $F^C(B, L, \alpha)$ is nondecreasing in B.

Similar proof for F is nonincreasing in α. Let $\alpha_n = \frac{B}{L} + \frac{1}{2} - \frac{1}{2\beta}$.

A brief explanation for Figure 3: (9) depicts the condition that the hacker attempts a crime. If the maximal fine is less than $\frac{(\frac{L}{\beta}-2B)^2}{4(\frac{L}{\beta}-B)}$ the hacker is not deterred. The optimal fine is then determined by the social planner's objective function.

References

Alesina, A., & La Ferrara, E. (2014). A test of racial bias in capital sentencing. *The American Economic Review*, *104*(11), 3397–3433.

Allingham, M. G., & Sandmo, A. (1972). Income tax evasion: A theoretical analysis. *Journal of public economics*, *1*(3-4), 323–338.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Springer.

Arce, D. G., Kovenock, D., & Roberson, B. (2012). Weakest-link attacker-defender games with multiple attack technologies. *Naval Research Logistics (NRL)*, *59*(6), 457–469.

Becker, G. S. (1968). Crime and punishment: An economic approach. In *The economic dimensions of crime* (pp. 13–68). Springer.

Böhme, R. (2013). *The economics of information security and privacy*. Springer.

Brenner, S. W., & Jewkes, Y. (2007). Cybercrime: Re-thinking crime control strategies. *Crime online*, 12–28.

Card, D., & Dahl, G. B. (2011). Family violence and football: The effect of unexpected emotional cues on violent behavior. *The Quarterly Journal of Economics*, qjr001.

Chalfin, A., & McCrary, J. (n.d.). Forthcoming."are us cities underpoliced? theory and evidence.". *Review of Economics and Statistics*.

Chalfin, A., & McCrary, J. (2017). Criminal deterrence: A review of the literature. *Journal of Economic Literature*, *55*(1), 5–48.

Cook, P. J. (1980). Research in criminal deterrence: Laying the groundwork for the second decade. *Crime and justice*, *2*, 211–268.

Corman, H., & Mocan, N. (2005). Carrots, sticks, and broken windows. *The Journal of Law and Economics*, *48*(1), 235–266.

DeAngelo, G., & Hansen, B. (2014). Life and death in the fast lane: Police enforcement and traffic fatalities. *American Economic Journal: Economic Policy*, *6*(2), 231–257.

Dills, A. K., Miron, J. A., & Summers, G. (2008). *What do economists know about crime?* (Tech.

Rep.). National Bureau of Economic Research.

Di Tella, R., & Schargrodsky, E. (2004). Do police reduce crime? estimates using the allocation of police forces after a terrorist attack. *The American Economic Review*, *94*(1), 115–133.

Doleac, J. L. (2017). The effects of dna databases on crime. *American Economic Journal: Applied Economics*, *9*(1), 165–201.

Doleac, J. L., & Sanders, N. J. (2015). Under the cover of darkness: How ambient light influences criminal activity. *Review of Economics and Statistics*, *97*(5), 1093–1103.

Drago, F., Galbiati, R., & Vertova, P. (2009). The deterrent effects of prison: Evidence from a natural experiment. *Journal of political Economy*, *117*(2), 257–280.

Ehrlich, I. (1996). Crime, punishment, and the market for offenses. *The Journal of Economic Perspectives*, *10*(1), 43–67.

Evans, W. N., & Owens, E. G. (2007). Cops and crime. *Journal of Public Economics*, *91*(1), 181–201.

Freeman, R. B. (1996). *Why do so many young american men commit crimes and what might we do about it?* (Tech. Rep.). National Bureau of Economic Research.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438–457.

Goyal, S., & Vigier, A. (2014). Attack, defence, and contagion in networks. *The Review of Economic Studies*, *81*(4), 1518–1542.

Grasmick, H. G., & Bryjak, G. J. (1980). The deterrent effect of perceived severity of punishment. *Social forces*, 471–491.

Gueye, A., Walrand, J. C., & Anantharam, V. (2011). A network topology design game: How to choose communication links in an adversarial environment. In *Proc. of the 2nd international icst conference on game theory for networks, gamenets* (Vol. 11).

Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, *114*(2), 793–804.

Kessler, D., & Levitt, S. D. (1999). Using sentence enhancements to distinguish between deterrence

and incapacitation. *The Journal of Law and Economics*, *42*(S1), 343–364.

Kim, S. H., Wang, Q.-H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM*, *55*(3), 66–73.

Levitt, S. D. (1995). *Using electoral cycles in police hiring to estimate the effect of policeon crime* (Tech. Rep.). National Bureau of Economic Research.

Levitt, S. D. (2004). Understanding why crime fell in the 1990s: Four factors that explain the decline and six that do not. *The Journal of Economic Perspectives*, *18*(1), 163–190.

Lin, M.-J. (2009). More police, less crime: Evidence from us state data. *International Review of Law and Economics*, *29*(2), 73–80.

Lochner, L. (2007). Individual perceptions of the criminal justice system. *The American Economic Review*, *97*(1), 444–460.

Makowsky, M. D., & Stratmann, T. (2009). Political economy at any speed: what determines traffic citations? *The American Economic Review*, *99*(1), 509–527.

McCrary, J. (2002). Using electoral cycles in police hiring to estimate the effect of police on crime: Comment. *The American Economic Review*, *92*(4), 1236–1243.

McCrary, J., & Lee, D. S. (2009). The deterrence effect of prison: Dynamic theory and evidence. *Berkeley Program in Law & Economics, Working Paper Series*.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives*, *23*(3), 3–20.

Nagin, D. S. (2013). Deterrence: A review of the evidence by a criminologist for economists. *Annu. Rev. Econ.*, *5*(1), 83–105.

Paternoster, R. (2010). How much do we really know about criminal deterrence? *The Journal of Criminal Law and Criminology*, 765–824.

Posner, R. A. (1972). The behavior of administrative agencies. *The Journal of Legal Studies*, *1*(2), 305–347.

Rao, J. M., & Reiley, D. H. (2012). The economics of spam. *The Journal of Economic Perspectives*, *26*(3), 87–110.

Skaperdas, S. (1996). Contest success functions. *Economic theory*, *7*(2), 283–290.

Staniford, S., Paxson, V., Weaver, N., et al. (2002). How to own the internet in your spare time. In *Usenix security symposium* (Vol. 2, pp. 14–15).

Stigler, G. J. (1970). The optimum enforcement of laws. *Journal of Political Economy*, *78*(3), 526–536.

Tonry, M. (2008). Learning from the limitations of deterrence research. *Crime and Justice*, *37*(1), 279–311.

Tullock, G. (1980). Efficient rent seeking. *Towards a Theory of the Rent-Seeking Society*, *James Buchanan, Roger Tollison, and Gordon Tullock (eds.)*, Texas A&M University Press.

Winkler, M. (2016). Is the world ready for quantum computers. *Bloomberg Businessweek*, 12.

Wu, Y., Feng, G., Wang, N., & Liang, H. (2015). Game of information security investment: Impact of attack types and network vulnerability. *Expert Systems with Applications*, *42*(15), 6132–6146.