George Mason University School of Law
Working Paper Series

Year 2005 *Paper* 26

An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods

Bruce H. Kobayashi[*]

[*] George Mason University School of Law, bkobayas@gmu.edu

An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods

Bruce H. Kobayashi

Abstract

This paper examines the incentives of private actors to invest in cybersecurity. Prior analyses have examined investments in security goods, such as locks or safes that have the characteristics of private goods. The analysis in this paper extends this analysis to examine expenditures on security goods, such as information, that have the characteristics of public goods. In contrast to the private goods case, where individual uncoordinated security expenditures can lead to an overproduction of security, the public goods case can result in the underproduction of security expenditures, and incentives to free ride. Thus, the formation of collective organizations may be necessary to facilitate the production of public security goods, and the protection of information produced by the collective organization should be a central feature of such organizations.

An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods.

Bruce H. Kobayashi[*]

ABSTRACT

This paper examines the incentives of private actors to invest in cybersecurity. Prior analyses have examined investments in security goods, such as locks or safes that have the characteristics of private goods. The analysis in this paper extends this analysis to examine expenditures on security goods, such as information, that have the characteristics of public goods. In contrast to the private goods case, where individual uncoordinated security expenditures can lead to an overproduction of security, the public goods case can result in the underproduction of security expenditures, and incentives to free ride. Thus, the formation of collective organizations may be necessary to facilitate the production of public security goods, and the protection of information produced by the collective organization should be a central feature of such organizations.

I. INTRODUCTION

It is well documented that private citizens spend large amounts on private security measures. These security expenditures include everything from simple devices such as door locks and bars on windows to elaborate electronic security systems and private security guards. Unlike general law enforcement expenditures, these protection expenditures are often aimed at the direct prevention of loss, and do not

[*] Associate Dean for Academic Affairs & Professor of Law, George Mason University School of Law, 3301 Fairfax Drive, Arlington, VA 22201, United States, 703-993-8034 (Phone), 703-993-8088 (Fax) bkobayas@gmu.edu. The author would like to thank the Critical Infrastructure Protection Project at the George Mason University Law School for funding. The author received helpful comments from Amitai Aviram, and participants at the CIPP/GMU Law School Conference of the Law and Economics of Cyber Security.

necessarily rely upon ex-post sanctions to reduce the net gain from criminal activity.[1]

The use of private security measures is likely to be important in the cybersecurity context. Use of private resources, including resources aimed at gathering information about the nature and frequency of past and future cyber attacks may be efficient given the decentralized nature of the internet. Further, traditional deterrence through ex-post sanctions may be difficult to implement in this setting for several reasons. Private resources aimed at identifying and pursuing those responsible for cyber attacks often will inure to the benefit of others, and thus are likely to be under produced.[2] As a result, those responsible for cyber attacks may perceive that they face low probabilities of punishment.[3]

[1] For analyses of private law enforcement systems, see Gary Becker and George Stigler, *Law Enforcement, Malfeasance, and Compensation of Enforcers*, 3 J Legal Stud 1 (1974); William M. Landes and Richard A. Posner, *The Private Enforcement of Law,* 4 J Legal Stud 1 (1975); David Friedman, *Private Creation and Enforcement of Law: A Historical Case,* 8 J Leg Stud 399 (1979); David Friedman, *Efficient Institutions for the Private Enforcement of Law,* 13 J Legal Stud 379 (1984). See also Doug Lichtman and Eric Posner, *Holding Internet Service Providers Accountable,* _ Sup Ct Econ Rev _ (2005) (discussing use of vicarious liability as a way to increase security and law enforcement).

[2] The Microsoft Corporation recent announced the initial $5 million funding of the Anti-Virus Reward Program that would pay bounties for information that leads to the arrest and conviction of those responsible for launching malicious viruses and worms on the Internet. *See* Microsoft Press Release, November 5, 2003. For a discussion of bounties generally, see Becker and Stigler, 3 J Legal Stud 1 (cited in note 1). Microsoft, owing to its large market share, can internalize more of the benefits of private enforcement expenditures. However, its large market share and its de facto standard status also serves to lower the costs of conducting a widespread cyber attack, and has also resulted a many attacks directed at computers using Microsoft products. For an analysis of the tradeoffs involved with de facto standards in the cybersecurity context, see Randy Picker, *Raising Transactions Costs and Network Security: Of Heterogeneity and Autarky,* in The Law & Economics of Cybersecurity, M. Grady and F. Parisi, eds. (Cambridge forthcoming 2005).

[3] Indeed, this result in not exogenous. Rather, it is a result of the fact the benefits from efforts by private citizens to apprehend and identify such individuals produce external benefits that, absent adequate civil judgments of bounties, inure to the benefit of others.

This in turn requires that large magnitude punishment be used for optimal deterrence, a difficult task given the difficulty of obtaining meaningful civil judgments against many of the defendants. The large volume and inchoate nature of many of the attacks may also make the authorities reluctant to impose large criminal penalties on individuals for such behavior.[4]

Prior economic analyses on security expenditures have examined potential divergences in the private and social incentives to provide private security measures.[5] These studies have shown that the private and social incentives to provide investments in security diverge due to an inability to internalize positive and negative externalities generated by private security investments.[6] Specifically, positive spillovers include the effect of expenditures that reduce the ex-ante net benefit of crime, and thus serve as a general deterrent to such activity. These expenditures can include expenditures aimed at identifying those responsible for criminal acts, and resources that minimize the harm that occurs as a result of crimes. Negative spillovers include the effect of expenditures that serve to divert criminal activity from those who invest in private security to those

[4] The paper does not consider the use of public sanctions and enforcement resources. The level of public enforcement will generally affect the level of private expenditures. For example, public enforcement and sanctions may serve to "crowd out" private expenditures. For an analysis of punishment for attempts, see Steven Shavell, *Deterrence and the Punishment of Attempts,* 19 J Legal Stud 435 (1990), David D. Friedman, *Impossibility, Subjective Probability, and Punishment for Attempts,* 20 J Legal Stud 179 (1991).

[5] Steven Shavell, *Individual Precautions to Prevent Theft: Private versus Socially Optimal Behavior,* 11 Intl Rev L & Econ 123 (1991).

[6] Id. See also Charles T. Clotfelter, *Private Security and the Public Safety,* 5 J Urban Econ 388 (1978).

who have not. The inability to internalize these spillover effects will result in the underproduction of the security expenditures that serve to generally deter crime, and can result in a relative overproduction of resources that serve mainly to divert criminals less protected targets.[7]

This paper extends the current literature on the private security investments by explicitly examining the issue of the investment and production of intangible security goods. The intangible nature of security inputs distinguishes the cybersecurity setting from the standard setting examined that involves private goods such as door locks. Specifically, security expenditures in the cybersecurity setting often involve investments in information, including information on the nature and frequency of cyber attacks, information on future attacks, and information on existing vulnerabilities and potential defenses. These cybersecurity expenditures have the characteristics of classic informational public goods. The existence of public security goods requires an analysis that examines the rate at which such assets are produced in addition to the question of how such assets are deployed.

It is shown that security investments in public goods can increase the divergence between the private and social incentives to produce and deploy security assets relative to the private security goods case. Specifically, independent individual security expenditures on non appropriable public goods

[7] Koo Hui-Wen and I. P. L. Png, *Private Security: Deterrent or Diversion?* 14 Intl Rev L & Econ 87 (1994).

can lead to free riding and underproduction. The potential for free riding suggests that a legal or market response is required to insure the adequate production of public good security expenditures. This paper examines how alternative private institutions, such as intellectual property protection, secrecy, or the use of contractual security collectives might address the pubic good problem.[8]

The article is organized as follows. Section II reviews the existing literature on the private production of security by examining the deployment of an existing set of security measures. Section III alters the model to consider the production of intangible security assets. Section IV considers production and deployment with secrecy or intellectual property protection. Section V concludes.

II. THE PRIVATE PRODUCTION OF PRIVATE SECURITY GOODS

Prior studies of the private production of security have examined the consequence of two non-internalized spillover effects that result from such expenditures. The first spillover effect is the positive effect that these expenditures have on reducing crime and other socially costly acts. For example, consider investments in security that serve to decrease the net benefits of crime or other types of wealth transferring activity. If such investments are not observable ex-ante, such expenditures not only decrease the expected losses to the person that makes the investment, but it also has a general deterrent effect that reduces the overall level

[8] For a description of some of the institutions that have arisen to counter the cybercommons problem, see Emily Frye, *The Tragedy of the Cybercommons: Overcoming Fundamental Vulnerabilities to Critical Infrastructure in a Networked World,* 58 Bus L 349 (2002).

of criminal activity. If the general deterrent effect is not internalized by those making these investments, such investments are will be underproduced.[9]

In contrast, if the existence (and lack) of such investments are observable to the criminal ex-ante, then criminals will be deterred from attacking a specific target. However, they may instead substitute a more protected target for a less protected one. Indeed, this substitution effect is more likely when alternative targets are close substitutes and of high value relative to the cost of committing the criminal act.[10] In such cases expenditures merely divert crime to other targets rather than generally deterring crime. In equilibrium, it is possible that there is an inefficient substitution away from generally deterring investments toward such crime diverting investments.

To examine the economic incentives to invest in private security, consider a model of observable private security expenditures in a world without public enforcement.[11] In this model, there are *h* web sites and *t* hackers. Hackers engage in the unauthorized entry of sites, and such unauthorized entry of a site results in a gain to the hacker. The unauthorized entry also causes a loss to the site, which

[9] See Shavell, 11 Intl Rev L & Econ (cited in note 5).
[10] See Hui-Wen and P'ng, 14 Intl Rev L & Econ (cited in note 7).
[11] The basic model is from Shavell. See Shavell, 11 Intl Rev L & Econ 123 (cited in note 5). Given the nature of cybercrime, where the release of costly viruses and worms is not accompanies by monetary or significant utility gains by the hacker, the model in this section is modified to allow for costly criminal activity where the loss from an attack l is greater than the gain g to the criminal. Shavell's model assumed that the activity inducing the security expenditures took the form of costless transfers.

can be different than the gain to the hacker.[12] In the absence of observable differences, hackers randomly choose between the *h* sites. Each of the *t* hackers choose a level of effort *e* in order to maximize the net gain from unauthorized entry:[13]

$$G(e,x) = eg(x) - c(e), \qquad (1)$$

where *c(e)* is the cost of effort, and *g(x)* is the gain to the *hacker*.[14] The amount of the gain from unauthorized entry into a site will be a decreasing function of the level of site's security expenditures *x.*[15] The hacker's first order condition is given by

$$g(x) = c'(e), \qquad (2)$$

[12] The two are equal only when the unauthorized entry results in a costless transfer from the site to the hacker.
[13] Heuristically, *e* is the number of attacks initiated by a hacker.
[14] It is assumed that $g'(x) < 0$, $g''(x) > 0$. $c'(e) > 0$, and $c''(e) > 0$. Note that in many cases, a hacker can simultaneously launch cyber-attacks at many sites (*e.g.,* through a cleverly designed worm or virus, suggesting decreasing returns. However, diminishing returns will apply to the up front effort and resources needed to initiate the attack, with increases in *e* resulting in a more widespread attack.
[15] In this model, expenditures on security have a protective effect, that is, they reduce the amount of gain to the hacker when an attack is launched, and also reduces the amount of loss suffered by the site (and its users) when an attack takes place.

so that $e = e(x)$.[16]

Implicitly differentiating the first order condition yields:

$$e'(x) = g'(x)/c''(e) < 0.^{17} \qquad (3)$$

This means that security expenditures decrease efforts by hackers to enter sites. If all potential victims choose equal levels of security expenditures, the frequency of unauthorized entry $\phi(x)$ faced by each of h sites equals

$$\phi(x) = (t/h)e(x). \qquad (4)$$

Intuitively, if all sites have the same equilibrium security, then hackers will attack sites randomly. Thus, the total number of attacks, $t^*e(x)$, will be uniformly distributed among the h sites.

[16] As noted in note 15, supra, the direct effect of security expenditures is to decrease the gain from any given attack, which in turn decreases the incentive of the hacker to expend costly effort at mounting attacks. This model does not consider expenditures that directly affect the effort of hackers independent of altering the expected gain from an attack. Modification of the model would then require that firms consider two types of expenditures, those that reduce the loss when attacks occur, and those that alter hackers' incentives directly. If we denote the latter type of expenditures by z, then the hacker's effort function can be expressed as $e = e(x,z)$. Such expenditures would be more akin to law enforcement expenditures that are generally publicly provided, such as efforts to detect and subsequently sanction those that commit attacks, and are not considered in this paper.

[17] Following Shavell, it is assumed that $e''(x) > 0$. See Shavell, 11 Intl Rev L & Econ 123 (cited in note 5).

If all h sites simultaneously increase x, the marginal effect on the frequency that a given site will suffer an attack is given by

$$\phi'(x) = (t/h)e'(x).^{18} \tag{5}$$

Potential victims are assumed to choose observable security expenditures x to minimize the cost of these expenditures plus the expected loss from crime:

$$L_o(x) = \phi\,(x|x')l(x) + x, \tag{6}$$

where x' is the level of expenditures of others, $\phi\,(x|x')$ is the frequency that a site will suffer a loss given expenditures x and x',[19] and $l(x)$ is the magnitude of the loss to the victim.[20] The first order condition is given by

[18] This formulation assumes that hackers independently choose which site to attack, and that sites can be profitably attacked numerous times.

[19] If we assume that hackers observe the level of x_i with error ε_i, and these observation errors are independent, then the probability that a given hacker will choose to attack site i equals the probability that $\varepsilon_i < x' - x + \varepsilon_{(1)}$, where $\varepsilon_{(1)}$ is the lowest order statistic given h-1 draws. If the error terms ε_i have a probability density function given by $f(\varepsilon_i)$, and cumulative density function given by $F(\varepsilon_i)$ then the probability that a site will be the subject of any given attack equals. The frequency of attacks will equal $\phi(x|x') = te(x)F(x' - x + \varepsilon_{(1)})$.

[20] We assume that $l'(x) < 0$, and $l''(x) > 0$. This assumption is consistent with expenditures on security reducing the losses suffered by attacked sites, but with diminishing returns. In a more complex model, this may not be the case. For example, higher levels of security may be simultaneously associated with higher costs for legitimate transactions. For example, the use of trusted systems may deter some consumers from visiting sites that use such systems. The resulting foregone transactions can at some point outweigh the decreased loss from unauthorized transactions, causing $l'(x)$ to be positive. For purposes of this paper, we assume that the relevant range includes levels of security expenditures in which $l'(x) < 0$.

$$-\phi_1(x|x')l(x) - \phi(x|x')l'(x) = 1. \qquad (7)$$

Assuming that $\phi(x|x) = \phi(x)$, the first order condition under conditions of symmetry ($x' = x$) becomes:

$$-\phi_1(x|x)l(x) - \phi(x)l'(x) = 1. \qquad (8)$$

Let x_o denote the solution to (8).

As an alternative to uncoordinated security expenditures, sites could cooperatively choose security levels to eliminate the diversionary spillover effects. If *h* sites collectively agree on a uniform level of expenditures, they would choose a level of expenditures to minimize

$$h\ \phi(x)l(x) + hx. \qquad (9)$$

The first order condition is given by

$$-\ \phi'(x)l(x) - \phi(x)l'(x) = 1. \qquad (10)$$

Let $x*$ denote the solution to the cooperative first order condition (10).

Finally, we can consider the social optimum, which considers the cost of resources used by the hackers and the losses caused by their behavior. The social objective function is to minimize the costs of precaution by the sites and effort by the hackers plus the amount of social loss from the unauthorized activity:

$$hx + t(c(e(x)) + e(x)s(x)). \qquad (11)$$

Where $s(x) = l(x) - g(x)$ is the social cost of the hacker's activity.

The first order condition equals:

$$-(t/h)(c'(e)e'(x) + s'(x)e(x) + s(x)e'(x)) = 1. \qquad (12)$$

The social first order condition can be rewritten as

$$-\phi'(x)(c'(e) + s(x)) - \phi(x)s'(x) = 1 \qquad (13)$$

Given that the hacker sets the marginal cost of effort equal to the gain from the crime, $g(x) = c'(e)$, and the first order condition is given by:

$$-\phi'(x)l(x) - \phi(x)s'(x) = 1 \tag{14}$$

Table 1 lists the three first order conditions for the individual, cooperative, and social objective functions in the private goods case.

Table 1 – First Order Conditions: Private Goods Case

	First Order Condition	Level of Security
Social	$-\phi'(x)l(x) - \phi(x)s'(x) = 1.$	x^{**}
Individual	$-\phi_1(x\|x')l(x) - \phi(x\|x')l'(x) = 1.$	x_o
Cooperatives	$-\phi'(x)l(x) - \phi(x)l'(x) = 1.$	x^*

Assuming that $-s'(x) = -l'(x) + g'(x) < -l'(x)$, it is clear that $x^* > x^{**}$. That is, the cooperatives have an incentive to overinvest in security expenditures. Intuitively, a cooperative's marginal incentive to invest in security is based upon the marginal reduction in the loss including the amount of the transfer, while social incentives are based upon the smaller loss net of the transfer amount. These additional expenditures on security are induced by a desire to reduce the amount of the transfer, which is not a social loss.[21] This overinvestment effect is most pronounced in the case of pure transfers that are large in magnitude.[22] On the other hand, this effect is small for crimes that cause large losses relative to the gains to the criminal.[23]

The relationship between the individual, uncoordinated level of security and the collective amount is ambiguous, and depends upon both the magnitude of the private and social losses and upon the relative magnitude of the marginal deterrence effect - $\phi'(x)l(x)$ and the diversion effect $-\phi_1(x|x)l(x)$. If $-\phi_1(x^*|x^*)l(x^*)$ > (<) - $\phi'(x^*)l(x^*)$, then x_o > (<) x^*. Because of this ambiguity, it is also the case that the individual level can be greater than or less than the socially optimal level.

To illustrate these relationships, Figure 1 shows a simulated equilibrium under the individual, cooperative, and social first order conditions. For purposes of the simulation, we assume that $c(e) = \alpha e^2$, and $g(x) = G/(k(1+x))$, and $l(x) = G/(\lambda(1+x))$, where $k \geq \lambda$. This latter assumption is made so that the gain from unauthorized entry is less than the loss imposed on the site. When $k = \lambda$, the unauthorized entry results in a costless transfer where the gain to the hacker equals the loss to the site. With the specific forms assumed above, $e(x) = G/(2\alpha k(1+x))$, and $p(x) = tG/(2h\alpha k(1+x))$.

[21] See Shavell, 11 Intl Rev L & Econ 123 (cited in note 5).
[22] Id.
[23] One example would be acts of vandalism that cause large losses to property, but are of little value to the vandal.

[Insert Figure 1 about here]

Figure 1 shows a the first order conditions listed in Table 1 and the equilibrium levels of security for $k = \lambda = 20, G = 100, h = 16, t = 10,$ *and* $\alpha = .1.$ The assumption that $k = \lambda = 20$ means that the gain to the hacker equals the loss to the site, so that the direct social loss from unauthorized entry is zero. Under these assumptions, the social level of security x^{**} equals 3.2 units per site. The cooperatively set level of security x_o equals 4.3 units per site, and shows the overincentive such cooperatives have to invest in security to prevent privately costly but socially neutral transfers.

The example also illustrates the incentive to invest in security in order to divert hackers towards other sites. The individual, uncoordinated level of security x^* equals 9.9 units per site, which is over three times the level of social level of security x^{**}.[24]

[Insert Figure 2 about here]

[24] Normal scores have been extensively computed. See Herbert A. David and H. N. Nagaraja, *Order Statistics* (Wiley-Interscience 3d ed, 2003).

Figure 2 illustrates the equilibrium where the unauthorized entry results in a direct social loss. Specifically, the simulation depicted in Figure 2 shows the equilibrium when $k = 20, \lambda = 10, G = 100, h = 16, t = 10,$ *and* $\alpha = .1.$ Under these assumptions, the ratio $l(x)/g(x) = k/\lambda = 2$. In order to model the individual first order conditions, we assumed that the ε_i, and identically and independently normally distributed with mean zero and standard deviation equal to one. Under these assumptions, the probability that site *i* will be the subject of any given attack equals the probability that $\varepsilon_i < x' - x + \varepsilon_{(1)}$, where $\varepsilon_{(1)}$ is the expected lowest order statistic given h-1 draws (also known as the normal score when the ε_i, have a standard normal distribution).[25] Under these assumptions, the social level of security x^{**} equals 5.1 units, the cooperatively set level, x_o equals 5.7 units, and the individual level x^* equals 14.3 units. The introduction of socially costly cyber attacks moves the cooperative and social level of security closer together, but increases the divergence between the individual, uncoordinated level of security and the social level of security.

Uncoordinated production of security does not necessarily produce the large overincentive illustrated in Figure 2. To illustrate this, Figure 3 shows the equilibrium when standard deviation of the ε_i is increased to 20. A larger standard deviation reduces the individual incentive to produce security so that the individual level x^* falls to 5.5 units, below the cooperative level, but still above,

[25] In the example, this is true both in absolute and percentage terms.

in this example, the individual level. Intuitively, a larger standard deviation for the ε_i, reduces the marginal effect of expenditures on x by making it more likely that marginal expenditures will be overcome by the random noise.[26]

[Insert Figure 3 about here]

III. PUBLIC SECURITY GOODS

Prior models have examined the provision of private security goods such as door locks or security guards. In the cybersecurity context, expenditures on security are likely to be investments in information about the nature and frequency of past attacks, information about pending attacks, and information about the existence of vulnerabilities to and potential defenses against cyberattacks. Such information is a classic public good that once produced, can be consumed by multiple sites in a nonrivalrous fashion.[27]

In this section, the model presented in Section I is modified to examine the private and social incentives to produce intangible security goods that have the characteristics of public goods. In order to model the production and use of public good security expenditures, we assume that a unit of x produced by one site

[26] For a similar analysis of the effect of uncertainty in the litigation context, see Richard Craswell and John E. Calfee, *Deterrence and Uncertain Legal Standards,* 2 J L, Econ, & Org 279 (1986).

[27] See Amitai Aviram and Avishalom Tor, *Overcoming Impediments to Information Sharing*, 55 Ala L Rev 231 (2004) (noting non-rivalrous nature of information, and analyzing strategic barrier to information sharing).

can be used in a nonrivalrous fashion by the other $h - 1$ sites.[28] Under these assumptions, the social objective function would be to minimize the costs of precaution, effort at crime, and the social loss of crime:

$$x + t(c(e(x)) + e(x)s(x)). \tag{15}$$

The first order condition is given by:

$$-t(c'(e)e'(x) + s'(x)e(x) + s(x)e'(x)) = 1. \tag{16}$$

The social first order condition can be rewritten as

[28] Note this does not imply that security expenditures are conducted in a centralized fashion. Indeed, the collection of information often requires examining global information from many individual sites in order to analyze and detect patterns of attacks. Thus, the benefit of a given total level of security expenditures will exhibit network effect – that is, a given level of security expenditures distributed over *h* sites will have a greater effect in reducing losses to the site and gains to the criminal than the same level of expenditure by a single site. In terms of the model, $l = l(x,s)$, *where* $l_2(x,s) < 0$. Similarly, information collected from numerous diverse sources may be more valuable than the same number of repeated observations by a few firms. See generally, Friedrich Hayek, *The Use of Knowledge In Society,* 35 Am Econ Rev 519 (1945). This analysis suggests that firms have a great incentive to share information in such a setting. Similar incentives for sharing of information between competitive firms have raised antitrust concerns. For example, McCarran Ferguson Act (U.S. Code Title 15, Chapter 20) makes the cooperative gathering of data for the purpose of ratemaking exempt from the federal antitrust statutes when undertaken by state regulated insurance companies. For an analysis of information sharing and antitrust in the cybersecurity context, see Aviram and Tor, 55 Ala L Rev 231 (cited in note 27). For economic analyses of information sharing between competing firms, see Olivier Armantier and Oliver Richard, *Exchanges of Cost Information in the Airline Industry,* 34 Rand J Econ 461 (2003); Barry S. Eisenberg, *Information Exchange Among Competitors: The Issue of Relative Value Scales for Physicians' Services,* 23 J L & Econ 461 (1981); Esther Gal-Or, *Information Transmission-Cournot and Bertrand Equilibria,* 53 Rev Econ Stud 85 (1986).

$$-h(\phi'(x)l(x) + \phi(x)s'(x)) = 1 \qquad (17)$$

Ceteris paribus, the level of security applied to each individual is higher than in the private goods case because each unit of *x* is now simultaneously applied to *h* potential victims. Total spending can be less than in the private goods case, as any unit of *x* is not separately incurred by each of the *h* potential victims.

If the *h* sites cooperatively choose a level of expenditures, they would attempt to minimize:

$$h\,\phi(x)l(x) + x. \qquad (18)$$

The first order condition is given by

$$-h(\phi'(x)l(x) + \phi(x)l'(x)) = 1. \qquad (19)$$

Comparing (19) to the social first order condition (17), we see that the public goods case preserves the relative relationship between the cooperative and socially optimal level of security expenditures. That is, cooperative spending results in the overproduction of public as well as private security goods due to an excessive incentive to reduce the size of transfers that do not represent a social loss.

Finally, consider the case where individuals choose to invest in public security goods. Consider first the case where such investments cannot be appropriated by those who make them, so that any private investments can be used by all participants in the market. The objective function on each individual is to minimize:

$$\phi(x_T)l(x_T) + x, \tag{20}$$

where x_T equals the total expenditures on x by all h potential victims.

The first order condition equals

$$-\phi'(x_T)l(x_T) - \phi(x_T)l'(x_T) = 1. \tag{21}$$

Table 2 summarizes the first order conditions for the public goods case.

Table 2 – First Order Conditions – Public Goods Case

	First Order Condition
Social	$-h[\phi'(x)l(x) + \phi(x)s'(x)] = 1.$
Individual	$-\phi'(x_T)l(x_T) - \phi(x_T)l'(x_T) = 1.$
Cooperatives	$-h[\phi'(x)l(x) + \phi(x)l'(x)] = 1.$

Note that by definition $\phi'(x_T) = \phi'(x),$ and that the first order condition (21) is satisfied at $x_T = x^*$, the cooperative level of expenditure in the private goods case. The total level of expenditures implied by the first order condition (21) is less than the cooperative level implied by (19). Note that this result differs from the private goods case. As shown in the simulations contained in Section II, it is possible for the individual uncoordinated level of private security expenditures to exceed those that would be set cooperatively. Intuitively, the potential to divert criminals towards another site can provide a powerful marginal incentive to spend on security. However, in the public goods case considered here, private expenditures simultaneously protect others' sites. Thus, such expenditures do not serve to divert hacker from the investor's site toward these other sites.

Moreover, the first order conditions do not yield a unique allocation of the security expenditures among the *h* sites. Thus, while individual expenditures equal to x^*/h by all *h* sites is an equilibrium, there are also multiple equilibria in which *h-k* sites spend zero, and *k* spend x^*/k. Any individual site would prefer and equilibrium where they were one of the *h-k* spending zero. Indeed, this result is the familiar free-riding problem in the presence of non-appropriable public goods. The existence of multiple equilibria and the potential for free-riding suggests that some mechanism to mitigate the free riding problem and/or solve the coordination problem is required.

To gain a sense of the relative magnitude of the problems, Figure 3 shows the results of a market simulation of relative levels of private security under the individual, cooperative, and social first order conditions for a public good. For the purposes of this simulation, assume the same functional forms as the private good simulations above.

[Insert Figure 4 about here]

Figure 4 shows the individual, cooperative and social first order conditions when the entry results in a pure transfer. Specifically, the simulations depicted in Figure 1 assume that *$k = \lambda = 20$, $G = 100$, $h = 50$, $t = 30$, and $\alpha = .1$.* Under these assumptions, the first order conditions yield a cooperative level of precaution equals 18.5 units, and an individual level of precaution equals 4.3 units. This is compared to the social level of precaution, which equals 14.5 units. Thus, for this particular simulation, the cooperatively set level of precaution results in a 27.6 percent increase over the level given by the social first order condition. Not that, in contrast to the private goods case in which the individual, uncoordinated level of security exceeded the social level, the individual first order condition in the public goods case yields a total level of precaution that is 29 percent of the level given by the social first order condition.

[Insert Figure 5 about here]

Figure 5 shows the first order conditions when *k* is increased to *50*. Under these assumptions, the ratio *g(x)/l(x)* = 20/50 = .4, so that the gain from an authorized entry is 40% of the loss caused the unauthorized entry. Under these assumptions, the individual, social, and cooperative level of security equals 2.9 units, 12.3 units, and 13.4 units respectively. Note that the cooperative level of precaution is only 8.9 percent greater than the social level, while the individual level is only 23 percent of the social level. Thus, under these conditions, an increase in the relative social cost of unauthorized entry will decrease the overproduction associated with the cooperative level of security, and increase the underproduction associated with uncoordinated security expenditures.

The foregoing analysis suggests that the relative efficiency of coordinated and individual uncoordinated public good security expenditures will depend upon the gain to harm ratio. The issue of social versus private losses in the cybersecurity context is a complex one. Take for example a directed denial of service attack that prevents consumers from accessing a particular e-commerce site, which at first blush, seems analogous to vandalism, an act with a low gain to loss ratio. However, if customers make purchases at a competitor's site, then the lost sales of the attacked site would be private but not social losses, thus resulting is a gain to loss ratio that is close to one. The release of destructive worms and viruses may be more akin to vandalism. In many cases, the release of the destructive or disruptive worm or virus is not apparently associated with an attempt to directly or indirectly transfer resources, with the apparent benefit to the person releasing it being the utility he obtains from the act.[29] As noted above, in such a case, any distortion between the cooperative and social level of private security expenditures will be small.

IV. THE PRIVATE PRODUCTION OF PUBLIC SECURITY GOODS

The results from the private good case suggest that uncoordinated markets may under or over produce private security relative to the social optimum. Further, in

[29] On the other hand, worms and viruses may be ways in which hackers are collecting information about how to lower the cost of transferring wealth in the future. In this sense, the release of a worm of virus may be a form of planning expenditures. These expenditures can induce marginal social costs by accelerating the level of defensive as well as offensive security expenditures, which are social costs. Thus, claims by hacker that they are providing a social service by exposing potential security flaws may not be true, especially if the flaw is publicly disclosed. Any benefits from the information gained from the worm may be outweighed by the direct costs caused by the virus, and by the increased present value of resources induced to protect sites from such worms. Even if the information gained is not publicly disclosed, the accelerated rate of defensive expenditures that are induced by such attacks may increase social costs. For a discussion of the positive informational externalities that result from the commission of crimes, see Kermit Daniel and John R. Lott, Jr., *Should Criminal Penalties Include Third-Party Avoidance Costs?,* 14 J Legal Stud 523 (1995).

this model, collective action to provide private good security expenditures will result in the overproduction of private security expenditures. Thus, while uncoordinated markets will not in general produce the first-best allocation of private security expenditures, neither will cooperative security investments.

The analysis in Section II shows that the public good nature of cybersecurity investments presents additional issues that are not present in the private goods case. The nonrivalrous nature of public good security expenditures suggests that such goods, once produced, should be made available for use by all sites. On the other hand, absent some way to appropriate the gains from public security investments, individual firms or groups may not have sufficient individual incentives to make such investments.

One implication is that the presence of public goods in the cybersecurity context would result in a great incentive to form cooperative security arrangements in such situations.[30] However, absent the existence of enforceable intellectual property rights or some other mechanism to appropriate the returns from private security expenditures, potential victims would have an incentive to

[30] Indeed, the use of prior contracts is suggested by Friedman as a solution to externalities present in the private law enforcement context. See Friedman, 8 J Legal Stud 299 (cited in note 1). For an analysis of the use of prior contracting as a way to produce public goods, including innovation, see Ben T. Yu. *Prior Contracting and Innovation,* 24 J L & Econ 215 (1981). See also Frye, 58 Bus L at 361 (cited in note 8) (describing private sector groups that have formed to share information and address cybersecurity issues, including Information Sharing and Assessment Centers (ISACs) in the financial services, energy, transportation, vital human services, and communication information services sectors, as well as the Partnership for Critical Infrastructure Security (PCIS), which coordinates the activities of the industry based ISACs).

free ride by refusing to join the cooperative security venture, then free riding on the public good output of the coalition.

To illustrate this point, consider the example used in the simulation contained underlying Figure 4, with $k = 50, \lambda = 20, G = 100, h = 50, t = 30,$ *and* $\alpha = .1$. Under these assumptions, the cooperative level of security equals 13.4 units with *h* sites participating. If each of the *h* sites agrees ex-ante to pay an equal share of the total costs of security, the expected loss plus pro-rata share equals .413 for each site.

Now suppose one site refuses to join. The remaining h-1 sites will seek to minimize:

$$(h-1)\ \phi(x)l(x) + x. \qquad (22)$$

The cooperative level of security chosen by *h-1* sites equals 13.3 units. If the site that refused to join the cooperative is able to free ride on the expenditures of the *h-1* sites in the cooperative, it will face a lower expected loss equal to .147. Thus, the slight increase in expected loss resulting from the lower security expenditures is more than offset by the savings of their pro rata share of cooperative security costs. Further, it can be demonstrated that a there is a similar incentive to defect from the *h-1, h-2 … 2* size cooperative under these circumstances.

Concerns over inadequate private investment in cybersecurity have led the federal government to suggest that some type of government regulation may be required.[31] It has been suggested, for example, that the government mandate minimum security standards, or require that private firms disclose the nature and frequency of cyber attacks aimed at their sites and networks.[32] However, such government mandates can generate their own inefficiencies. For example, the government choice of standard may result in a choice that is inferior to whatever potentially imperfect choice would have been made by the market.[33] Further, government choice of a standard may stifle experimentation and innovation the can lead to dynamic inefficiency.[34] Mandatory disclosure can be overinclusive, requiring the disclosure of information with a marginal value less than the marginal cost of collection and disclosure.[35] Further, mandatory disclosure can

[31] See Jonathan Krim, *Help Fix Cybersecurity or Else, U.S. Tells Industry,* Washington Post E02 (Dec 4, 2003) (Bush administration official warning regulation looms if private companies do not increase private efforts at providing cyber-security). The Bush administration has taken a relatively hands off approach to this issue. See, e.g., *The National Strategy to Protect Cyberspace* (February 2003).

[32] See Frye, 58 Bus L 349 (cited in note 8).

[33] See, e.g., Stan J. Liebowitz and Stephen E. Margolis, *Winners, Losers and Microsoft: Competition and Antitrust in High Technology* (Independent Institute, 1999).

[34] See Bruce H. Kobayashi and Larry E. Ribstein, *State Regulation of Electronic Commerce,* 51 Emory L J 1 (2002).

[35] See, e.g., Frank H. Easterbrook and Daniel R. Fischel, *Mandatory Disclosure and the Protection of Investors,* 70 Va L Rev 669 (1984) (discussing mandatory disclosure rules contained in the securities laws).

induce firms to engage in less information collection, and greater free riding problems.[36]

One an alternative to government standards or mandated disclosure would be for the government to encourage firms to produce information through use of property rights to information.[37] What is critical is that sites that undertake cooperative investments in public good security expenditures find some way to exclude non-payers.[38] A mechanism to exclude non-payers will prevent a firm refusing to join the collective from free riding on the expenditures of the collective. Further, given that the level of protection applied to a firm that does not join the collective will be below that applied to members of the collective, non members will suffer more frequent attacks. If this is not done, then sites will refuse to join the cooperative and attempt to free ride off the information provided by the cooperative.

As is the case with any idea or informational public good, the private production of public goods can be induced through intellectual property

[36] See D. Bruce Johnsen, *The Limits of Mandatory Disclosure: Regulatory Taking under the Investment Company Act,* mimeo, George Mason University (2003) (discussing SEC disclosure rules and their suppression of information production).

[37] See generally*,* Harold Demsetz, *The Private Production of Public Goods,* 13 J L & Econ 293 (1970).

[38] The clear definition of intellectual property rights, as well as members' responsibility for preventing the further dissemination of sensitive information, should be central issue when an information sharing group or security cooperative is formed. No systematic analysis of the contractual agreements regarding intellectual property rights and the maintenance of secrecy currently has been done. A closely related survey of the treatment of intellectual property rights for private standard setting organizations found wide variation in the treatment of intellectual property rights. See Mark Lemley, *Intellectual Property Rights and Standard Setting Organizations*, 90 Cal L Rev 1889 (2002).

protection. For example, security research firms use proprietary technology to collect and analyze data about cyber attacks.[39] While security expenditures that involve the collection and analysis of information may not be protected under the federal copyright laws, or rise to the level of novelty or nonobviousness required for protection under the federal patent laws,[40] the computer programs used to track and analyze such data may be. Further, patent protection may be available for novel and nonobvious computer programs and business methods.

Even if use of statutory intellectual property right protection, such as copyright or patents, is not be feasible, security collectives can use secrecy, supported by contractual restrictions on the members, to prevent widespread free riding.[41] In this context, secrecy means that the existence and content of a specific security level x is not disclosed ex-ante to other sites or to potential hackers. This form of secrecy has two offsetting effects. First, it allows individuals to appropriate the gains from their private expenditures by precluding other sites from appropriating information it possesses.[42] To the extent secrecy

[39] See, e.g., Leslie Walker, *The View from Symatec's Security Central*, Washington Post E01(Jan 9, 2003) (describing the use of proprietary software and systems to monitor and analyze the nature and frequency of cyber attacks. The information and analysis is subsequently sold to subscriber networks).

[40] Under the U.S. Supreme Court's decision in *Fiest Publications v Rural Telephone Service,* 499 US 340 (1991), protection for factual compilations under the federal copyright laws is limited. Congress has recently considered federal database protection. See, e.g., Database and Collections of Information Misappropriation Act, HR 3261, October 8, 2003.

[41] See, generally Bruce H. Kobayashi and Larry E. Ribstein, *Privacy and Firms,* 79 Den L Rev 526 (2002).

[42] Note that such protection is not perfect. See, e.g., William M. Landes and Richard A. Posner, *The Economic Structure of Intellectual Property Law* at 354-371 (Belknap, 2003) (discussing the

prevents free-riding, its use can encourage private expenditures on public good security expenditures. On the other hand, use of secrecy may not allow for the diverting effect generated by expenditures that are publicly disclosed. Thus, its use may suppress the incentive for individuals to expend private resources on public good security expenditures.

To examine the effect of secrecy consider the objective function for each cooperative of size *s*. Such a cooperative will attempt to minimize:

$$s^* \phi\,(x|x')l(x|x') + x, \qquad (21)$$

If secrecy is not perfect, both the probability and the amount of the loss are conditional on *x'*, the amount spent by the other *h - s* potential victims. The conditional probability and loss amounts capture two distinct effects. The first is the diversion effect that results from criminals substituting into less protected targets. The second effect is the spillover from expenditures by others *x'* that can be appropriated by the cooperative *s*. The first order condition equals

$$-s(\phi_1(x|x')l(x|x') + \phi\,(x|x')l'(x|x')) = 1. \qquad (22)$$

economics of trade secret law). However, in the context of some cybersecurity settings, a timing advantage can be used to appropriate the returns from expenditures on information. For example, timely notice of IP addresses being used to launch distributed denial of service attacks or other types of cyber attacks allow the targets to block incoming mail from these addresses before large scale damage is incurred. Small delays in the transmission of this information can delay such preventative measures, and will increase the amount of loss from such attacks.

To simplify matters, suppose that secrecy turns the security goods into the equivalent of an unobserved private good so that security measures are not observable ex-ante, either by criminal or by other potential victims. In this case, $\phi_1(x|x') = 0$, as both the diversion effect and the spillover effect of expenditures by others on the probability of loss will be zero. Further, under these circumstances, there will be no spillover effect of expenditures by others on the amount of loss, i.e., $l'(x|x') = l'(x)$. If the cooperative of size s takes the frequency of an attack ϕ as exogenous, the first order condition becomes

$$-s\phi\, l'(x) = 1 \qquad (23)$$

If $s = 1$, then each individual spends less than the cooperative level. Using the numbers and the example used to generate Figure 2, and if we assume that $\phi = \phi(x)$,[43] then each of the h sites will set their level of security at 2.1 units. The total amount of security produced is 2.1*50 = 105 units. However, only 2.1 units of security would be applied to any given site. In contrast, the uncoordinated

[43] Hially-Ü}ô the criminals expectation of the equilibrium level of expenditures on security x may differ from that implied by the first order condition (23). If criminals have operated in an environment of low security in the past, and are not informed ex-ante of the increase in x, the criminal's estimate of x would be lower than the actual level of x, and his estimate of ϕ will be higher than $\phi(x)$. Given this, the levels of spending given by (23) will underestimate the actual level. Over time, criminals will adjust their estimate of x over time so that $\phi = \phi(x)$, and sites will adjust x until equilibrium is reached.

individual equilibrium level of security would result in the production of 2.9 units of security that would be simultaneously applied to all *h* sites. Thus, the result of individual investments with secrecy would be a low protection, high cost equilibrium.

This result suggests the inefficiency of investment by individual firms in public good security expenditures that are kept secret. However, such an inefficiency would be eliminated if individual firms formed collectives. The individual members would have to agree ex-ante to pay a pro-rata share of the costs of the security collective. Furthermore, they would also have to agree to protect the information generated and shared by members of the collective from disclosure to non-members.[44] As noted above, failure to do so would give individual sites an incentive to free ride by remaining outside the cooperative.

To see this point, suppose that $s = h$. A collective with *h* members would produce 10.4 units of security. This level is below both the collective level given in equation (21) and the social level given in equation (17). Thus, if secrecy is necessary for the stability of cooperative spending, there could be some underproduction of security. However, this is not necessarily the case. Because, the cooperative level of security is greater than the social optimum, the reduced incentive to spend on secrecy can move security expenditures toward the socially

[44] The security collectives would likely also include requirements that members maintain minimum security standards, and may require that members collect and report information in a timely manner.

optimal level. Consider, for example, the case where the unauthorized entry results in a pure transfer, so that k = 20. In this case, secrecy results in a security expenditure of 14.5 units, which coincides with the social level.

V. CONCLUSION

The foregoing analysis has examined the incentive to produce private security expenditures. While prior analyses have examined the provision of security goods that have the characteristics of private goods, the analysis in this paper examined expenditures on security, such as information, that have the characteristics of public goods.

In contrast to the private goods case, where individual uncoordinated security expenditures can lead to an overproduction of security, the public goods case can result in the underproduction of security expenditures, and incentives to free ride. Thus, the formation of collective organizations may be necessary to facilitate the production of public security goods, and the protection of information produced by the collective organization should be a central feature of such organizations.

FIGURE 1 – Equilibrium with Private Security Goods – Pure Transfer Case

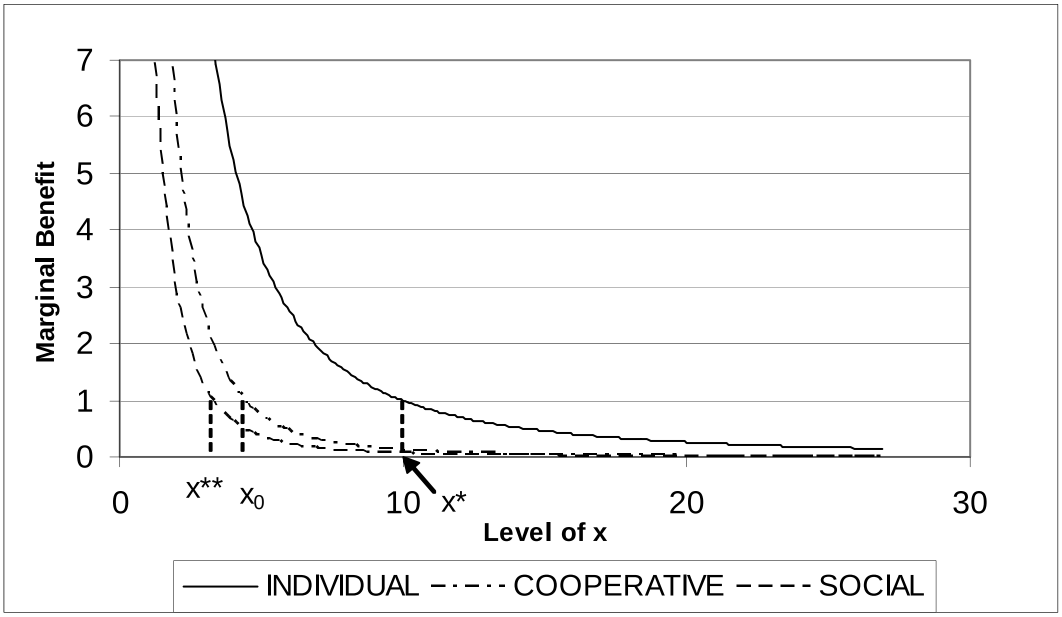


FIGURE 2 – Equilibrium with Private Security Goods – Social Loss Case

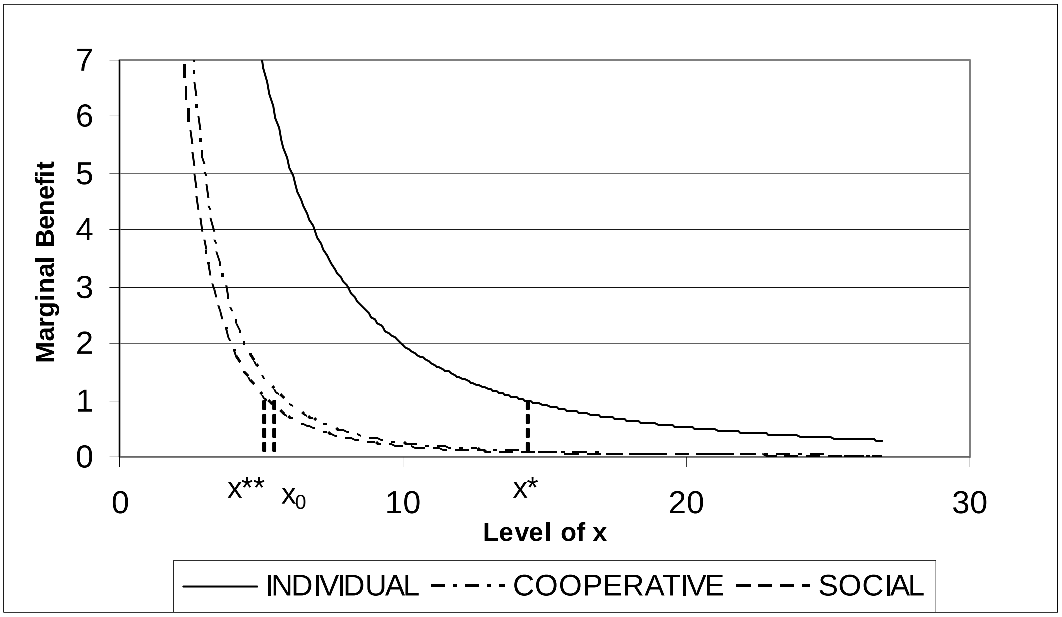


FIGURE 3 – Equilibrium with Private Security Goods – Social Loss, High Variance Case

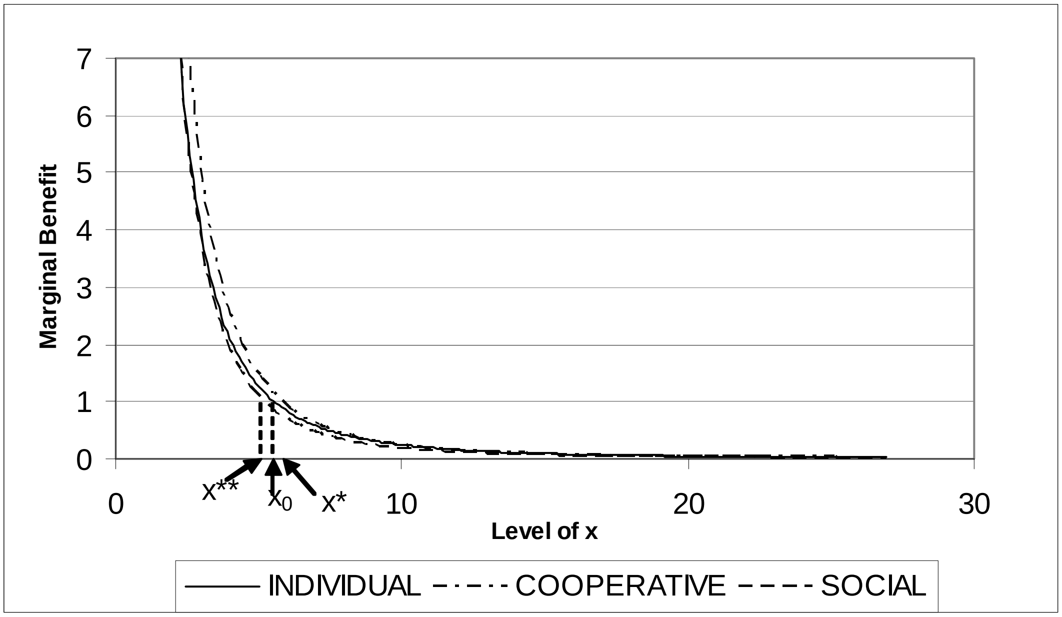


FIGURE 4 – Equilibrium with Public Security Goods – Pure Transfer Case

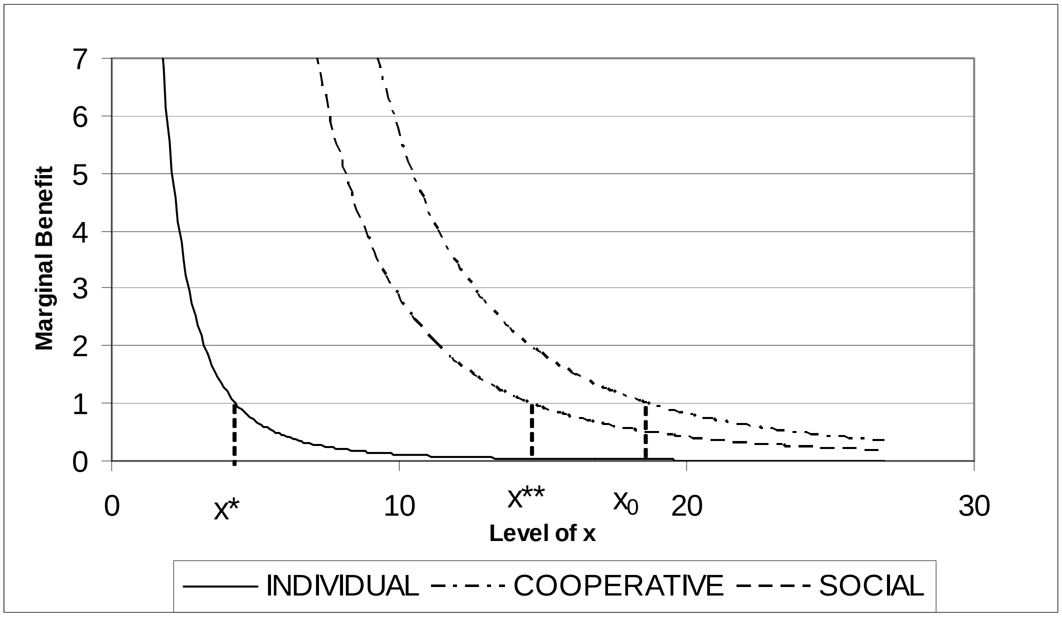
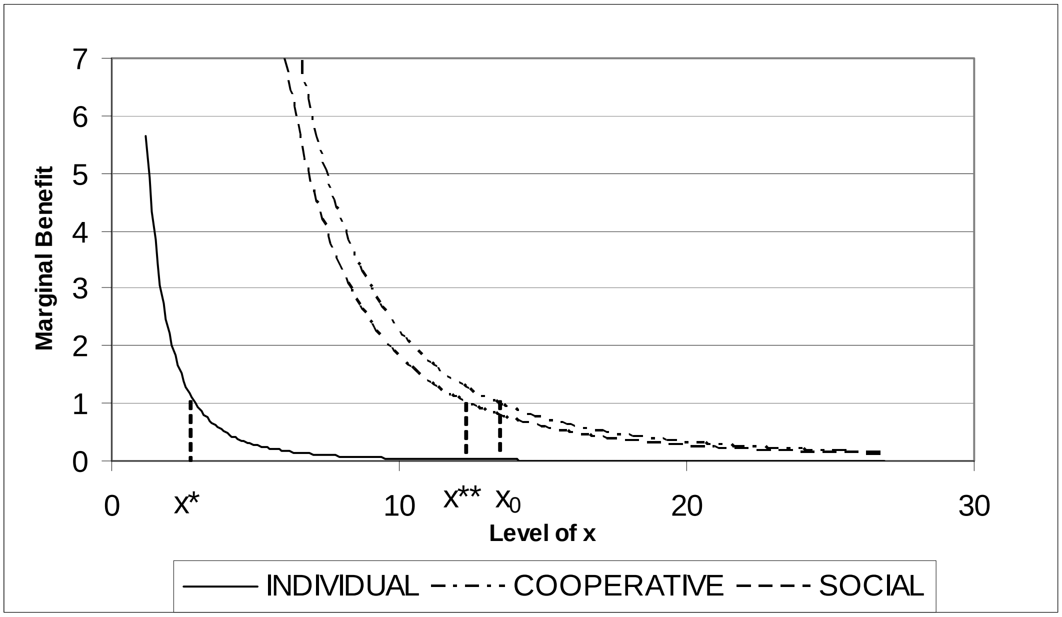


FIGURE 5 – Equilibrium with Public Security Goods – Social Loss Case


Marginal Benefit
X*
X**
X0
Level of x
INDIVIDUAL
COOPERATIVE
SOCIAL