Income, interdependence, and substitution effects affecting incentives for security investment

Kjell Hausken

Abstract

Firms in cyber war compete with external intruders such as hackers over their assets. Each firm invests in security technology when the required rate of return from security investment exceeds the average attack level, or when the formal control requirements dictate investment. Each firm invests maximally in security when the average attack level is 25% of the firm's required rate of return. The income effect eliminates or "freezes" parts of the agent's resource, attack tools, and competence. The security investment decreases in the income reduction parameter when the agent's resource is low, is inverse U shaped when the resource is intermediate, and drops to zero when the external threat is overwhelming. A sufficiently strong income effect eliminates the external threat. When two firms are interdependent, security investments and attacks impact both firms. With increasing interdependence, each firm free rides by investing less, suffers lower profit, while the agent enjoys higher profit. The substitution effect causes the agent to allocate his attack optimally between the firms. The attack distribution is endogenized. Each firm's security investment increases in its asset and investment efficiency. The attack against each firm increases in the product of the firm's asset and investment inefficiency. Specific analyses are made of how the substitution effect impacts security investment for differently sized firms.

Keywords: Cyber war; Conflict; Contest success function; Security technology investment; Security breaches; Income; Interdependence; Substitution

1. Introduction

The intensity of cyber war has increased through the Internet revolution. Firms are bombarded with attacks of all kinds, and invest increasingly in security technology. A variety of principles are applied to determine the size of the investment. The common approach in today's literature is to assume that the external threat is fixed and immutable. This means that the nature of cyber war is not fully appreciated. This article develops a model that accounts for the cyber war between firms as strategic players on the one hand and the external threat phrased as a strategic player on the other hand. None of the warring sides are fixed and immutable. They adapt to each other. Available resources by all players, and strategic choices, depend on all strategic choices and the nature of cyber war. As developed in the conflict and rent seeking literature, the firms and the external agents wage war over the firms' assets. This approach has not been made earlier in this literature, and generates new and interesting insights.

Three effects which with a few exceptions are ignored in today's literature are discussed. The income effect eliminates parts of the external agent's resource, or weakens the agent's ability to convert resources into an attack, which reduces the attacker's overall ability or willingness to conduct cyber war. The interdependence effect means that two firms in varying degrees are intertwined, dependent, and influenced by each other, so that one firm's security investment benefits both firms, and the attack on one firm also affects the other firm. The substitution effect causes the external agent to consider the firms' strategies and substitute into the most optimal and least costly attack allocation across the two firms. The three effects cause quite different optimal strategies regarding security investment and information sharing for firms.

The article describes the external agent as hackers or perpetrators intending to break through the security of firms to get access to assets. The model is phrased as cyber war, but applies for all kinds of external agents with hostile intentions directed towards appropriating firms' assets. Examples are terrorists, crime syndicates, thieves, proletarians, and various agencies, firms, or other actors engaged in asset appropriation. Firms in cyber war are well advised to apply competitor analysis (Porter, 1980), adopted to information security by Gordon and Loeb (2001), and which may be adopted further to the competition or war between firms and external attackers. We consider attackers as competitors. Attackers come in all shapes and forms, many are unknown, and their skills and objectives differ. See Kjaerland (2005) for a clas-sification of computer security incidents. Gordon and Loeb (2001, p. 73) argue that, "once your competitors have been identified, the next move is to determine the type of information about your firm that competitors would find most beneficial".

Gordon and Loeb (2003) provide a formal model of how two rivals invest in competitor analysis and information security. Competitor analysis enables a firm to capture a portion of the market's profits currently earned by the rival. Information security involves e.g. reducing the threat that the firm's information system will be breached by the firm's rival or by others. In this article we assume that competitor analysis and information security operate jointly. Firms apply competitor analysis when adjusting the size and kind of security investments to protect assets, and external agents apply com-petitor analysis when adjusting their attacks to appropriate assets.

Firms' incentives to invest in security technology are influenced not only by external agents, but also by law. The Sarbanes-Oxley Act of 2002 (SOX) places strict requirements on firms. Especially, the internal control provisions of Section 404 of SOX require senior management of publicly traded companies both to (i) establish and maintain adequate internal controls for financial reporting, and (ii) assess annually the effectiveness of those controls. Furthermore, the law establishes attestation requirements for public accounting firms to assess management's certification of the effectiveness of its internal controls over financial reporting. Bagby (2005) argues that a confluence of SOX, privacy law, national and institutional security, and trade secrecy, jointly and reinforcingly place pressures for internal control progress on various functions (finance, accounting, IT, eCommerce and internet Services) within firms and across industries and professions. The assumption is that control systems are the key security methods for information assets, which are pathways to other assets. Dhillon et al. (2004, p. 551) argue ''that organisations which focus exclusively on tech-nical and formal control measures in their systems fall short of protecting their resources''. They propose ''that organizations should focus more on the pragmatic control measures'' ''related to good management practices and management communication''.

In our framework, firms have incentives to abide by the formal control requirements directed by law if the benefits of such compliance exceed the costs, which is always the case when the fines and sanctions for non-compliance are large. Firms abide by the pragmatic control requirements directed by culture, custom, good management practices, and other concerns to the extent the benefits outstrip the costs. Examples of costs are loss of reputation and customers, which reduce the firms' assets. As we will see, there are cases where firms have no incentives to invest in security, such as when the required rate of return is lower than the average level of attack, or the threat is tremendous. This presupposes that no formal control requirements dictate investment, while

pragmatic control measures may or may not exist. That is, with regulation the firms always have to invest in security to comply with the formal control requirements, while without regulation the firms have incentive not to invest in some cases. Formal and informal control measures to some extent have the same impact as external agents in the sense that firms' assets are reduced unless firms invest sufficiently in security either to comply with the control measures, and/or to prevent the external agents from appropriating their assets.

Section 2 discusses a few characteristics of today's literature. Section 3 develops the benchmark model with no effects, and attacks against n different firms. Section 4 analyzes the income effect and attacks against n equivalent firms. Sections 5 and 6 consider the interdependence effect and substitution effect for two different firms. Section 7 considers the joint operation of the interdependence and substitution effects. Section 8 analyzes the joint operation of all the three effects. Section 9 considers future research and limitations of the current work. Section 10 concludes.

2. A few characteristics of today's literature

Although the model in this article confines attention to security investment, the strategic complementarity of security investment and information sharing is such that it is useful to consider the intertwined literatures of both. Some recent papers discuss security based information sharing organizations. Schenk and Schenk (2002) illuminate incentives for reporting security breaches, Campbell et al. (2003) and Cavusoglu et al. (2004) consider the cost and impact of security breaches, and Schechter and Smith (2003) analyze the benefits of sharing information to prevent information security breaches. Gal-Or and Ghose (2003) analyze how market characteristics affect information sharing and security investment which in turn affect demand and costs. Gal-Or and Ghose (2005) present a two stage Bertrand-Nash model where firms choose security investment, information sharing, and prices, focusing on demand side effects. Gordon and Loeb (2002) determine the optimal investment for information protection. Gordon et al. (2003) focus on the cost side effects of how information sharing affects the overall level of security, where free-riding may cause under-investment in security. The free-rider dilemma is further analyzed by Anderson (2001) with respect to security investments, Varian (2002) related to system reliability, and Hausken (2002) regarding how agents incur costs in various games to ensure system reliability. Ziv (1993) shows that truth telling may not be an equilibrium.

The analysis of information sharing in the cyber war era can draw upon the general literature on cooperative relationships, joint ventures, and trade associations (Gal-Or, 1985; Kirby, 1988; Novshek and Sonnenschein, 1982; Shapiro, 1986; Vives, 1990). The latter typically considers a two stage game where

information is first shared and then the firms compete (Bertrand or Cournot) without collusion in the product market. E.g., Gal-Or and Ghose (2005) let in the first stage two firms choose security investment and information sharing simultaneously. In the second stage the two firms choose prices simultaneously. The second stage is solved first, which gives prices dependent on all the four first stage decision variables. Inserting the prices into the first stage gives an optimization problem where both firms choose positive security investment and information sharing. The problem with this approach is that each firm chooses information sharing in the first stage taking into account how the price it chooses optimally in the second stage depends on information sharing by both firms. This means that the information sharing chosen by the other firm has a direct impact on the information sharing chosen by the first firm. This direct impact is questionable since it reduces the incentive each firm has to free ride on the other firm's information sharing. Each firm prefers to receive information from the other firm, but does not necessarily have an incentive to provide information. Consequently, Gal-Or and Ghose's (2005) two stage game, and other games in the literature, are designed such that the free rider dilemma is partly eliminated.

Alternatives to the typical two stage game are a one stage game where all six decisions are made simultaneously, or a two stage game where the decisions are sequenced differently, or a three stage game. Security investments differ from the other decisions in that they require planning, sustained effort through time, involving buildup of infrastructure, culture, and competence. Hence security investments in the first stage seem plausible. Information sharing and prices (or quantities) can be determined in the second stage, simultaneously and independently, or in the second and third stages. All these alternatives give six first order conditions which may give illuminating results that can be tested for robustness and other characteristics.[1]

The main shortcomings of today's literature are that the external threat is considered to be fixed and immutable in quantity and quality, directed in a fixed and immutable manner against each firm, and does not depend on the kind of interaction between the firms. This article intends to overcome these three shortcomings.

Let us consider a cyber war between firms on the one hand seeking to defend assets, and external agents on the other hand as an external threat seeking to attack assets. The number of external agents, their resources, competence, and objectives are not fixed and immutable. The two warring sides adapt to

[1] The author has set up some of the six FOCs for the Gal-Or and Ghose (2005) model with the given functional forms, additionally accounting for the contest success function developed in Section 3, and the income, interdependence, and substitution effects. The FOCs typically cover half a page which means that the implicit function approach cannot be used and one would have to rely on simulations to gain insights.

each other. As firms invest in security technology, and share information, parts of the resources and competence of the external agents may become obsolete. This eliminates parts of the external threat. If the cyber war grows too intense, some of the external agents may give up, may change into other activities, or may change objectives. Some may invest to develop new competence, which is costly and time consuming. Others may explore new avenues of attack which may or may not prove successful. Firms' investments may thus permanently or temporarily reduce the external threat. This may benefit some firms in particular, or all firms in general.

If one firm, in terms of quantity, quality, and nature, invests otherwise in security technology, and share information otherwise than another firm, external agents can be expected to attack the firms differently. That is, the external threat faced by each firm depends on the strategic choices made by that firm, and the strategic choices made by other firms.

Two firms may operate in different markets and be relatively independent, they may operate in the same market through market sharing, they may be strong competitors in the same market, they may depend on each other through vertical integration, outsourcing, or other cooperative arrangements, or they may be so strongly interconnected that an attack on one is tantamount, in varying degrees, to an attack on the other. These kinds of interaction between firms influence the cyber war and strategic choices of both firms and external agents.

The income effect has to the author's knowledge been considered twice earlier related to terrorism.[2] First, Enders and Sandler (2003) mention the possibility of "freezing terrorist's assets" which "reduces their 'war chest'". Second, Lakdawalla and Zanjani (2002, p. 10), who also use the term deterrence effect, consider public intervention versus self-protection and show that "protection reduces the payoff to terrorism". The interdependence effect has been considered by Kunreuther and Heal (2003), where one target's defense benefits all targets. Examples occur within the airline industry, computer networks, fire protection, theft protection, bankruptcy protection, vaccinations. The substitution effect has been considered twice earlier. First, Enders and Sandler (2003) refer to "the installation of screening devices in US airports in January 1973 <which> made skyjackings more difficult, thus encouraging terrorists to substitute into other kinds of hostage missions or to stage a skyjacking from an airport outside of the United States". Second, Lakdawalla and Zanjani (2002, 10), who also use the term displacement effect, state that "with the total level of terror investments fixed at T, increases in self-protection by one target cause terrorists to substitute toward other targets... Each target's probability of

[2] I thank an anonymous referee of this journal for referring me to Lakdawalla and Zanjani (2002).

attack falls with its own self-protection, but rises with the self-protection investments of others''. The objective of this article is to consider how these three effects operate in cyber war related to security investment.

Let us look more closely at the Gal-Or and Ghose (2005) model. Although market characteristics, consumer demand, and sensitivity toward price and quantity of course depend on the strategic choices of the two firms, the nature of the external threat is fixed and immutable. In their Proposition 3(i) they find that ''a lower level of firm loyalty leads to lower levels of security information sharing and security technology investment''. Other models may show that the only way out of low firm loyalty is higher investment in security and e.g. publi-cized demonstrated participation in information sharing alliances, to build con-sumer confidence. In their Proposition 3(ii) they find that ''the extent of information sharing and amount of security technology investment by both firms increase when the degree of product substitutability increases''. Increased com-petition generally causes price cuts. As firms' surplus decrease due to price cuts, the opposite result may follow where less may get invested in security, and information sharing may be too risky. In their Proposition 4(i) they find that ''security information sharing and security technology investment levels increase with firm size,'' which is ''consistent with the well known result that a monopolist benefits more from cost-reducing innovations than a firm competing in a duopoly, given that it can extract a higher proportion of the surplus from the market''. In an industry with one strong dominant firm and one weak inferior firm, this result is questionable. Frequently, the strong firm may not trust the weak firm and may refuse to share information with it. Fearing exploitation, the weak firm may also be reluctant to share information. Further, if the competence of the external agents is too low to attack the strong firm, the weak firm may get attacked, leading the weak to invest more than the strong as a percentage of firm size. Both Gal-Or and Ghose's (2005) and Gordon et al.'s (2003) models are highly valuable contributions, but it should be realized that they make specific assumptions. Future research needs to question and develop also alternative assumptions to allow for comparison. This article is one such alternative.

Analyzing incentives for security investment should be supplemented with analyzing incentives for learning and acquiring information about how to invest wisely.[3] This permits better understanding of the pressures, drivers and mechanisms involved when deciding how to invest. Some incentives to learn might include (thus could be modeled): 1. Information of industry-pervasive vulnerability may enable remediation at competitor/supplier/customer/service organization. 2. Learning may counteract the market perception that vulnerability is pervasive across industry or corporate functions (e.g. IT, accounting, human resources). 3. One may learn to exploit competitive

[3] I thank John Bagby for pointing out the relevance of learning.

advantage, and thus correct the market misperception, that vulnerability is pervasive, which may ensure competitive advantage over vulnerable firms. 4. One may learn to exploit vulnerability to misappropriate confidences (data, secret theft). 5. One may try to model the amount of information about security investment not accurately received, misunderstood, and misinterpreted.

3. The benchmark model: no effects, fixed resource R, fixed distributed attack β_i

Firm i has an asset r_i, $i = 1, \ldots, n$, and there are n firms. Each firm i invests t_i in security technology to defend its asset, where t_i is the security investment cost, which we refer to as the investment. The security investment expenditure is f^i, where $\partial f^i/\partial t_i > 0$. We consider the simple case $f^i = c_i t_i$, where c_i is the inefficiency of security investment for firm i.[4] Higher c_i means greater inefficiency, where $1/c_i$ is the efficiency. (c_i may alternatively be interpreted as the unit cost of security investment, where t_i does not have to be discrete.) Firm i employs security experts, installs firewalls, applies encryption techniques, access control mechanisms, develops intrusion detection systems, and designs the optimal defense. External agents, which we for simplicity consider as one unitary agent, mount attacks against the firms. The external agent (henceforth simply agent) has a resource R which is transformed into an investment T directed as an attack against all firms. The inefficiency of the transformation is a, and the efficiency of the transformation is $1/a$. (a may alternatively be interpreted as the unit transformation cost.) Firms and agent are assumed risk neutral.[5] Both

[4] I thank an anonymous referee of this journal for referring me to Dalvi et al. (2004) and pointing out that "one can easily envisage a scenario where the costs of investments in security for a firm increase proportionally with the level of attack investments made by the external agency because every additional unit of investment is now that much less 'effective' because of a corresponding investment in T by the adversary". The security investment expenditure would then be $f^i = c_i t_i T_i$. To compare with the alternative scenario, assume that the purchase and installation of a given firewall cost x dollars. This cost is fixed regardless of how many attempt to break through it, and regardless of how many succeed in breaking through it. This gives a security investment expenditure $c_i t_i$. Dalvi et al.'s (2004) approach is philosophically related to assuming the expenditure $c_i t_i T_i$. The difference between their approach and the approach in this article is that Dalvi et al. assume no contest success function for the competition between Classifier and Adversary. With a contest success function $h^i = t_i/(t_i + T_i)$, and an expenditure $c_i t_i T_i$, the attack T_i by the agent on firm i has a double impact. The first impact is to increase firm i's security investment expenditure. The second impact is to reduce firm i's share h^i of the asset r_i. As is common in the economic conflict literature and in the war literature, and to avoid the double impact, this article confines attention to the second impact, which gives the expenditure $f^i = c_i t_i$.

[5] An alternative analysis may assume that the agent as an attacker is risk seeking while the firms as defenders are risk averse. Assuming risk neutrality simplifies the analysis. Much of the economic conflict literature related to production, appropriation, defense, and rent seeking assumes risk neutrality. See Skaperdas (1991) for an exception.

the expenditures $c_i t_i$ and aT can be capital and/or labor. A fraction β_i of the attack is directed as T_i at firm i, that is,

$$T = R/a, \quad T_i = \beta_i T, \quad \sum_{i=1}^{n} \beta_i = 1. \tag{1}$$

The agent's attack T is constant in this simplest model. If β_i is also constant, T_i is constant and the agent has no optimization problem. Examples of constant β_i are $\beta_i = 1/n$ and $\beta_i = r_i / \sum_{i=1}^{n} r_i$. The agent's objective is to get a fraction of the firms' assets.[6] The agent seeks to break through the security defense of the n firms in order to appropriate, get access to, or confiscate, something of value in the firms, or secure information which can be used as means of appropriating fractions of the firms' assets. The appropriation may be money if the firm's bank accounts can be hacked, assets that can be converted into money, anything of value controlled by the firm, secure information which may be used to the firm's disadvantage, or information that can be used to blackmail the firm. Merely announcing credibly with T_i to a firm that it will be hacked unless it pays may be enough to secure a fraction of the firm's assets. The investment T_i can also be used to get information from firm i which can be used to get something of value elsewhere. This may for firm i cause competitive disadvantage, bad publicity, or some other effect which indirectly reduces firm i's asset r_i. We assume that the cyber war between firm i and the agent for the asset r_i takes the form that is common in the conflict and rent seeking literature (Hausken, 2005; Hirshleifer, 1989; Skaperdas, 1996), where firm i gets a fraction h^i, and the agent gets the remaining fraction $1 - h^i$, where h^i is the contest success function, $\partial h^i / \partial t_i > 0$, $\partial h^i / \partial T_i < 0$. We shall use the common ratio formula[7]

$$h^i = \frac{t_i}{t_i + T_i}. \tag{2}$$

Summing up, firm i invests t_i in security technology at an expenditure f^i, and gets to keep a fraction h^i of its asset r_i in cyber war with an agent who invests T_i. Firm i's profit u_i and the agent's profit U are

$$u_i = \frac{t_i}{t_i + T_i} r_i - c_i t_i, \quad U = \sum_{i=1}^{n} \frac{T_i}{t_i + T_i} r_i - aT. \tag{3}$$

Whereas each firm has a variable expenditure $c_i t_i$, the agent has a fixed expenditure $aT = R$ which can be conceived of as a budget constraint. There are several reasons for this. First, firms are often (but not always) more resourceful

[6] This objective can be interpreted as financial gain. Other possible objectives are political gain, leisure activities, a desire for challenges, and a desire for causing destruction, see Howard (1997).

[7] It can more generally be written as $h^i = \lambda t_i^m / (\lambda t_i^m + \lambda T_i^m)$, where λ and m are parameters. Another example is the logit or difference form where $h^i = e^{mt_i} / (e^{mt_i} + e^{mT_i})$.

and thus less likely to be affected by budget constraints. Second, and most importantly, for the substitution effect we focus explicitly on how the agent makes a tradeoff between attacking several firms. For two firms this is accomplished by setting $T_j = T - T_i$, letting T_i be the free variable, and differentiating $\partial U/\partial T_i = 0$. With a variable expenditure $aT_i + aT_j$, there are two free variables, and the substitution effect cannot be analyzed unless a budget constraint is introduced. Third, if aT at least to some extent is labor expenditure, such labor expenditure for the agent is unlawful. Whereas a firm may more easily hire and fire labor, an agent trained in unlawful behavior, and possibly burdened by a criminal record, may not that easily find alternative outlets for his effort. If so, his working capacity is his effort which may be constant to a larger extent than for each firm. Fourth, a variable expenditure for the agent less easily facilitates analytical solutions.

Firm i invests t_i in technology to maximize profit u_i, that is

$$\frac{\partial u_i}{\partial t_i} = 0 \Rightarrow t_i = \sqrt{\beta_i R/a}\left(\sqrt{r_i/c_i} - \sqrt{\beta_i R/a}\right),$$
$$u_i = c_i\left(\sqrt{r_i/c_i} - \sqrt{\beta_i R/a}\right)^2 \tag{4}$$

which require $\sqrt{r_i/c_i} > \sqrt{\beta_i R/a}$. For n equivalent firms, $r_i = r$, $c_i = c$, $\beta_i = 1/n$, this gives

$$t_i = \sqrt{\frac{R}{an}}\left(\sqrt{\frac{r}{c}} - \sqrt{\frac{R}{an}}\right) = \sqrt{\frac{r}{c}}\sqrt{\frac{R}{an}} - \frac{R}{an}, \quad u_i = c\left(\sqrt{\frac{r}{c}} - \sqrt{\frac{R}{an}}\right)^2,$$
$$T_i = \frac{R}{an}, \quad U = \sqrt{\frac{Rrcn}{a}} - R. \tag{5}$$

Especially prominent in Eqs. (4) and (5) are the ratios r_i/c_i and R/an. On the one hand r_i/c_i is the ratio of firm i's asset and investment inefficiency, or the product of firm i's asset and investment efficiency. On the other hand, inserting (2) into (3) gives $u_i = h^i r_i - c_i t_i$, which gives $\partial u_i/\partial h^i = r_i$ and $\partial u_i/\partial t_i = -c_i$. Dividing the first with the latter gives $(\partial u_i/\partial h^i)/(-\partial u_i/\partial t_i) = r_i/c_i$ which is the percentage of the marginal utility from increased successful defense to the marginal disutility from incremental investment cost. A similar concept in economics is termed the marginal rate of substitution (MRS): the amount of good x that the consumer must be given to compensate him for a one-unit marginal reduction in his consumption of good y. Here $r_i/c_i = (\partial u_i/\partial h^i)/(-\partial u_i/\partial t_i)$ means the amount of security success that the firm must get to compensate for the firm's marginal expenditure in security investment, similar to the concept of required rate of return from security investment. The ratio R/an is on the one hand the agent's resource divided by his inefficiency and divided by the number of firms. On the other hand, (1) states that the agent's attack

equals $T = R/a$. Dividing both sides with n gives $T/n = (1/n)R/a$ which can be interpreted as the average level of attack on each firm, when there are n firms.[8]

Proposition 1. (*i*) *Firm i invests in security technology when the required rate of return from security investment exceeds the average attack level, i.e. when* $r/c > R/an$. *Otherwise firm i does not invest in security technology.* (*ii*) *The agent attacks if* $rcn > Ra$, *and does otherwise not attack.*

By comparing the required rate of return from security investment with the average attack level, firm i knows whether to invest or not, and using (5) the firm knows how much it shall invest, the profit it earns, and the profit the agent earns. Proposition 1 can also be formulated such that firm i invests in security technology when the ratio of its asset and investment inefficiency is larger than the ratio of the agent's resource and investment inefficiency divided by the number of firms. A firm must have a sufficiently large asset for it to be worthwhile defending it, and the investment inefficiency must not be too large. If the resource of the agent is too large, the firm does not defend, unless the agent's transformation inefficiency a is high or many firms are attacked in parallel (n is large) which decreases the attack on each firm. Of course, the agent may single out one firm, or a subset of firms, for attack. In that case (5) applies for $n = 1$ or for the subset of n chosen. No security investment is not counterintuitive against an overwhelming threat. As an example, a firm's investment into a security code is wasted if the agent's resource is such that it almost effortlessly can break the code. In this case the firm may as well refrain from developing the code. The agent attacks if the firms are valuable, their investment inefficiencies are low, and there are many firms (rcn is large), as compared with the agent's resource and transfor-mation inefficiency (Ra). If the formal control requirements dictate invest-ment, the firms will nevertheless invest to avoid an even larger loss in terms of fines and sanctions. However, pragmatic control requirements are not sufficient to justify investment if the required rate of return is lower than the average level of attack.

Proposition 2. *Firm i's security technology investment increases concavely in the required rate of return from security investment* r/c, *and is inverse U shaped in the average level of attack* R/an. *Maximum investment* $t_i = r/4c$ *giving utility* $u_i = r/4$ *occurs when* $R/an = r/4c$, *which is* 25% *of the required rate of return.*

[8] I thank an anonymous referee of this journal for suggesting these two interpretations of r_i/c_i and R/an.

As a firm's asset becomes more valuable, defending it becomes more important, and the firm increases its security investment. There is diminishing marginal return on investing in security. Each firm invests maximally in security when the average level of attack is 25% (that is, 1/4) of the firm's required rate of return from security investment r/c. The firm finds that this large investment is an appropriate counterweight to the agent's attack, and the defense expenditure is acceptable. The inverse U shape in the average level of attack R/an means that if R/an is lower than 25% of r/c (the agent's resource R is low, or a or n is high), then there is no need for each firm to invest significantly in security since the agent constitutes no significant threat on each firm's asset. Conversely, if R/an is higher than 25% of r/c, then the threat on each firm's asset is so high that each firm chooses low investment since a higher expenditure is not justified by the benefit. This means that the firm finds the threat overwhelming, and partly gives up fighting against it.

Let us compare this result with Gordon and Loeb's (2002) analysis. They consider two classes of security breach functions,[9] and analyze how a firm's security investment depends on its vulnerability. For both classes there is no investment if the vulnerability is below a certain level. For the first class the investment increases concavely. For the second class the investment is inverse U shaped, and equals zero for a sufficiently high vulnerability. Tanaka and Matsuura (2005) and Tanaka et al. (2005) find support for the second class, considering computer viruses attacking Japanese firms, and measuring the vulnerability level as the number of e-mail accounts. Proposition 2 can be said to be compatible with the second class if we interpret a firm to be more vulnerable if the agent's resource is higher (or if the transformation inefficiency is lower or if fewer firms are under attack).

4. Income effect and fixed distributed attack for n equivalent firms

One way of increasing the pressure on the agent is to assume that the agent's ability to attack gets reduced dependent on the firms' security investments. Such reduction can occur in three manners. The first is that a firm's security investment decreases the agent's efficiency in attacking through increasing the transformation inefficiency a, in other words, $\partial a/\partial t_i > 0$. Since the firms' security investments increase a which reduces the agent's transformation ability, the attack $T = R/a$ will be reduced.[10] The second is that a firm's security investment decreases or erodes the agent's resource R, in other words, $\partial R/\partial t_i < 0$. The third is that a firm's security investment eliminates parts of the

[9] Hausken (2006) extends to six classes.

[10] I thank an anonymous referee of this journal for pointing out that this first manner of reduction can be referred to as an income effect.

agent's resource R, which amounts to subtracting a term from the agent's initial resource. We refer to these three manners of reduction as the income effect since the agent's efficiency is reduced, or his available resources are reduced, or parts of his resources are taken out of circulation. The first two manners of reduction have an impact that was analyzed in Section 3, simply increasing a or decreasing R. No further analysis of the first two manners is necessary. This section focuses on the third manner where parts of the agent's resource is taken out of circulation.

Firms' security investments in antivirus, intrusion detection systems, firewalls, virtual private networks, and access control may reduce the agent's income in all these three manners. All three interpretations can be given for some or most security investments. For example, assume that a firm's security investments make parts of the agent's scanning tools or other attack equipment obsolete, or that a new firewall makes some equipment or competence by the agent useless.[11] For concreteness, assume that the agent has two tools labeled A and B. Tool A runs through all combinations of 16 digit passwords and makes an entry into a system when the correct password is found. Tool B has some other function. Without security investment, assume the agent can use both tools A and B. Assume that the firm's security investment abandons all 16 digit passwords in favor of more sophisticated security. That tool A becomes useless in this manner can mean that the agent's efficiency gets reduced (first interpretation) since he can now only use tool B, that his resource gets reduced (second interpretation), and that parts of his resource (tool A) gets eliminated (third interpretation). Regarding the third interpretation, abandoning 16 digit passwords is not equivalent to confiscating tool A from the agent. However, since tool A is now useless for the agent, the impact for all practical purposes is such that tool A might as well have been confiscated. Parts of the agent's resource is thus eliminated.

Let us consider an analogy. Applying the income effect to terrorism, Enders and Sandler (2003) refer to "freezing terrorist's assets" which "reduces their 'war chest' and their overall ability to conduct a campaign of terror". This corresponds to our third interpretation. One way to freeze a terrorist's assets is to freeze his bank accounts. Governments and certain other authorities can implement such freezing for criminals and certain other individuals. This is not equivalent to confiscating or appropriating the bank accounts, since the accounts with their given holdings are still there. However, the owners of the bank accounts cannot use the accounts, so for all practical purposes the

[11] Information sharing, which is a strategic complement to security investment under some assumptions (Gal-Or and Ghose, 2003) may also eliminate parts of the agent's resource. This may occur if the reporting of security breaches allows for straightforward elimination as useless some of the agent's attack tools. Alternatively, Schechter and Smith (2003) show that information sharing by firms can deter hackers.

holdings of the accounts might as well have been confiscated for a limited or unlimited time. Firms' security investments have the same impact, which is that parts of the agent's resource is directly or indirectly or implicitly rendered useless, obsolete, taken out of circulation, which for practical purposes means that it is eliminated.

Although many of today's cyber-security investments are less aggressive than for anti-terrorism, this may not necessarily be so in the future. The cyber era is currently in its early phase. We already see firms engaged in security investment and investigation to identify and track down perpetrators. Firms often have to incur the expense of early investigation and sometimes have to pressure law enforcement authorities to continue criminal investigation. Authorities occasionally confiscate hackers' computers, software, and associated hacking tools, which means eliminating parts of the agent's resource. Firms' security investments to combat cyber attacks may very well in the future, possibly in more extensive liaisons with law enforcement authorities, turn out to be more aggressive than the current war on terror in the sense of attempting to eliminate the agent's resource.[12]

Let us compare the approach in this section with that of Lakdawalla and Zanjani (2002, 10) who show that "protection reduces the payoff to terrorism". They define the terrorist's profit as $v(A) + D(T; s_1, \ldots, s_N)$ s.t. $A + T \leqslant R$, where R is the resource, A is non-violent activities, T is vio-lent terror, $v(A)$ is concave, $D()$ is expected damage, and s_i is self-protection by the N targets. They show that "Deterrence ⟨i.e. income reduction⟩ takes place insofar as private self-protection raises A and lowers the total amount of violent terror investments" (Lakdawalla and Zanjani, 2002, p. 11). This means that the income effect analyzed by Lakdawalla and Zanjani (2002) follows from substitution from violent terror T to non-violent activities A, i n their notation.

In contrast, the income effect analyzed in this article is more in the spirit of Enders and Sandler's (2003) approach where parts of the agent's resource R is eliminated. Knowledge, tools, and attack methods change and evolve rapidly or explosively in a field such as information security technology. Agents not staying abreast of the development quickly get their resource base eroded. As firms invest in security technology, and share information, parts of the resources and competence of the external agents may become useless or obsolete against the firms' new defense systems. Accordingly, we assume that the firms' security investments t_i's reduce the agent's cyber war chest, that is, resource R so that the total attack T decreases, i.e. $\partial T/\partial t_i < 0$. In order to ana-

[12] An anonymous referee of this journal has argued that today's security investments by firms do not eliminate the agent's resources, but rather weaken the agent's ability and efficiency of attacks, i.e. not as aggressive as in the anti-terrorism case. This section presents a more nuanced view where three interpretations are possible.

lyze the symmetric case of n equivalent firms with assets $r_i = r$, we let firm i invest t_i, while the $n-1$ other firms equally invest t_j each. Each firm suffers a fraction $\beta_i = 1/n$ of the attack T. We replace (1) with

$$T = [R - b(t_i + (n-1)t_j)]/a, \quad T_i = T/n, \tag{6}$$

where $b(t_i + (n-1)t_j)$ is that part of the agent's resource base that gets eliminated due to the n firms' security investments. In equilibrium $t_i = t_j$ which gives $T = [R - bnt_i]/a$, where b is an income reduction parameter that scales the sum of the security investments relative to the agent's resource, so that they get the same denomination. If b is large, the agent's resource gets reduced significantly, and the income effect has impact. Inserting (6) into (3) and differentiating firm i's profit with respect to t_i, $\partial u_i/\partial t_i = 0$, and thereafter setting $t_i = t_j$ gives

$$t_i = \frac{ra\left(b(2Rc/ra - n + 1) - 2Rc/r + \sqrt{b^2(n-1)^2 + 4Rc(an-b)(a-b)/ra}\right)}{2(a-b)^2cn} \tag{7}$$

which reduces to t_i in (5) when $b = 0$. As b increases sufficiently, T eventually decreases toward zero. No matter how finitely large is the agent's resource R, there always exists a sufficiently large b that eliminates it. Solving (6) and (7) for $t_i = t_j$ and $T = 0$ gives

$$T = 0 \Rightarrow b = \frac{\sqrt{Rac}}{\sqrt{r}} \Rightarrow t_i = \frac{\sqrt{Rr}}{n\sqrt{ac}}, \quad u_i = r - \frac{\sqrt{Rrc}}{n\sqrt{a}}, \quad U = 0. \tag{8}$$

Proposition 3 considers the security investment t_i with no income effect $b = 0$ and income effect so large that the agent's attack is eliminated, i.e. $b = \sqrt{Rac}/\sqrt{r}$ causing $T = 0$.

Proposition 3. (*i*) *When* $b = 0$, *the security investment* t_i *decreases in* b *when* $R < ra(n-1)^2/4cn$, *increases in* b *when* $ra(n-1)^2/4cn < R < ran/c$, *and equals zero when* $R > ran/c$. (*ii*) *When* $b = \sqrt{Rac}/\sqrt{r}$ *causing* $T = 0$, t_i *decreases in* b *when* $R < ra(n-1)^2/4c$, *and increases otherwise.*

Three effects operate when $b = 0$. First, when the agent's resource R is sufficiently small, the agent does not constitute a considerable threat. As b increases above zero, the firms immediately start to cash in on the benefit of an increased income reduction parameter. There is no longer a need to invest a large t_i, since the larger b above zero accomplishes the same for a lower t_i, through reducing the agent's small income to an even lower level. The exception occurs when the formal control requirements nevertheless

dictate a large investment. Second, when R is above a small level but below a large level, the agent does constitute a considerable threat. In fact, the threat is so large that the firms would like to invest more, which is too expensive when $b = 0$. However, as b increases above zero, the firms find an incentive to invest since they get an immediate return on their investment in the form of reducing the agent's income. Third, when R is above a large level, the agent's threat is so overwhelming that the firms refrain from investment. This follows from the contest success function $t_i/(t_i + T_i)$ when T_i is extremely large. Even a very small investment t_i causes the securement of a smaller fraction of the asset r than the expenditure $ct_i$of such investment justifies, see (3). The contest is like the one between an unarmed army and an army with overwhelming firepower, where the weaker party gives up. However, the large level $R > ran/c$ is such that if each firm's asset r is large, or the transformation inefficiency a is large, or there are many firms (n is large), or the investment efficiency $1/c$ is low, then the agent's resource R must be quite substantial in order for the firms to refrain from investment. For all the three levels of R in Proposition 3(i), r, a, n play a role in the numerator, while c plays a role in the denominator.

Proposition 3(ii) has two points rather than three since when the agent's resource is about to be eliminated causing zero attack $T = 0$, zero investment is no option for the firms. This follows from the contest success function $t_i/(t_i + T_i)$ which equals one when $T_i = 0$. First, when the agent's resource R is below $R = ra(n-1)^2/4c$, which is n times larger than the low-est R-level in Proposition 3(i), the firms' investment decreases in b. The intu-ition follows from the mathematical logic of the contest success function. When the agent's resource is sufficiently reduced, the firms can relax their
investment. The analogy in war is to start withdrawing forces when the enemy is far weaker and about to go extinct. For a large $b = \sqrt{Rac}/\sqrt{r}$, the firms nevertheless have to keep a certain investment to ensure that the attack gets virtually eliminated. This follows from $t_i/(t_i + T_i)$ where a slightly positive T_i is not acceptable when b is large. As b increases above this level, the firms have to keep their investment intact to ensure that the agent does not revert to attacking. Second, when the agent's resource R is above $R = ra(n-1)^2/4c$, the threat is so substantial that the firms still cash in on larger b's, and are unwilling to invest heavily unless a sufficiently large b ensures a return on their investment. This return is required despite the fact that the agent's resource is about to be eliminated. Consequently, firms increase their investment all the way up to the point where the external threat is eliminated.

Whereas Proposition 3 considers the lower and upper cases $b = 0$ and $b = \sqrt{Rac}/\sqrt{r}$, Proposition 4 specifies what happens in between. The inequality $ra(n-1)^2/4c < ran/c$ holds when $n \leqslant 5$, so we distinguish between $n \leqslant 5$ and

$n > 5$. The intuition for Proposition 4 follows from Proposition 3, applying the logic of interpolation.

Proposition 4-1. *Assume* $n \leqslant 5$. (*i*) *When* $R < ra(n-1)^2/4cn$, t_i *decreases throughout in b.* (*ii*) *When* $ra(n-1)^2/4cn < R < ra(n-1)^2/4c$, t_i *is inverse U shaped.* (*iii*) *When* $ra(n-1)^2/4c < R < ran/c$, t_i *increases throughout.* (*iv*) *When* $R > ran/c$, t_i *equals zero when* $0 \leqslant b < b^*$, *and increases throughout when* $b^* < b < \sqrt{Rac}/\sqrt{r}$, *where* b^* *is defined in* (A.4).

Proposition 4-2. *Assume* $n > 5$. (*i*) *When* $R < ra(n-1)^2/4cn$, t_i *decreases throughout in b.* (*ii*) *When* $ra(n-1)^2/4cn < R < ran/c$, t_i *is inverse U shaped.* (*iii*) *When* $ran/c < R < ra(n-1)^2/4c$, t_i *equals zero when* $0 \leqslant b < b^*$, *and is inverse U shaped when* $b^* < b < \sqrt{Rac}/\sqrt{r}$. (*iv*) *When* $R > ra(n-1)^2/4c$, t_i *equals zero when* $0 \leqslant b < b^*$, *and increases throughout when* $b^* < b < \sqrt{Rac}/\sqrt{r}$.

First, a low R causes the firms to decrease their investment along the entire range of b. The agent is a small threat, and the firms enjoy the increased b by cashing in on this benefit up to the point where the external threat is eliminated and $T = 0$. Second, an intermediate R causes t_i to increase when b increases from zero, and decrease when b approaches the upper extreme. This gives a maximum for t_i when b is between zero and the upper extreme, and an inverse U shape. Third, assume that R is large. When $n \leqslant 5$, the external threat is considerable, and t_i increases throughout the range of b until $T = 0$. However, when $n > 5$, t_i first increases toward a maximum, and thereafter decreases. With more than five firms, the agent's attack gets diluted, and the firms can ease up on their security investment as T approaches zero. Fourth, when R is very

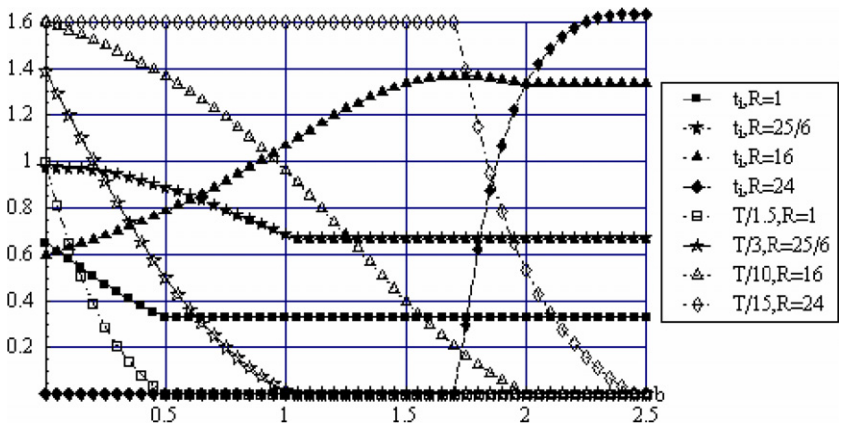

Fig. 1. Security investment t_i and attack T for $R = 1, 25/6, 16, 24$, $r = 4$, $a = c = 1$, $n = 6$.

large, the external threat is overwhelming and the firms refuse to invest in security when b is small. But regardless how large is R, as long as it is finite, there always exists a sufficiently large income reduction parameter b where t_i can be invested by n firms to eliminate the external threat. The investment eventually increases throughout until $T = 0$.

Fig. 1 illustrates Proposition 4 for four values of R, assuming $r = 4$, $a = c = 1$, $n = 6$. The security investment t_i is shown with filled symbols (box, star, triangle, diamond), and the attack T with unfilled symbols. Division of T with 1.5, 3, 10, 15 is for scaling purposes. The first curve sets $R = 1$ which is well below $ra(n-1)^2/4cn = 25/6$. In accordance with Proposition 4(i) t_i decreases throughout. For $b = 0$ the investment is $t_i = 0.65$ and the profit is $u_i = 2.53$. The upper value $b = \sqrt{Rac}/\sqrt{r} = 1/2$ causing $T = U = 0$ gives $t_i = 0.33$ and $u_i = 3.67$. The income effect for $R = 1$ allows the six firms to cut their security investment in half, while earning a 45% higher profit, which eliminates the external threat. Table 1 shows these values for $R = 1$ and three higher values of R.

The four leftmost columns show t_i, u_i, T, U without the income effect, $b = 0$. The next two columns show t_i and u_i when the income effect has eliminated the external threat causing $T = U = 0$, which means $b = \sqrt{Rac}/\sqrt{r}$ listed in the rightmost column. The second column from the right shows b^* when it applies. The second curve in Fig. 1 sets $R = 25/6$ which is exactly the transition value $R = ra(n-1)^2/4cn$ from (i) to (ii) in Proposition 4. The curve for t_i starts out horizontally from $b = 0$ since the derivative of t_i equals zero, and thereafter decreases. The t_i values are larger and the u_i values are lower than for $R = 1$ since the attack is larger.

The third curve in Fig. 1 sets $R = 16$ which is below $ran/c = 24$. Hence Proposition 4(ii) applies, t_i is inverse U shaped, and the attack is eliminated when $b = 2$. For $b = 0$ the investment is lower than when $R = 1$, only $t_i = 0.60$. Security investment is costly when there is no income effect and thus no hope of reducing or eliminating the attack. As b increases from 0 to 2, the profit increases substantially from 0.13 to 2.67.

The fourth curve in Fig. 1 sets $R = 24$ which is exactly the transition value $R = ran/c$ from (ii) to (iv) in Proposition 4. The external threat is now so substantial that the firms do not invest when $b < b^* = 2an/(n+1) = 1.71$, determined from Eq. (A.5). When R is only marginally below 24, t_i is positive for all $b \geqslant 0$. When $R = 24$ and $b > b^*$, t_i increases substantially, is inverse U shaped, but eventually decreases only marginally toward $t_i = 1.63$ when $n = 2.45$. That t_i increases steeplier when $R = 24$ than when $R = 16$ follows from the form of the contest success function, $t_i/(t_i + T_i)$, where a large T_i requires a large t_i for it to be worthwhile for the firms to incur the cost of security investment.

Table 1
Values of t_i, u_i, T, U for various b when $R = 1, 25/6, 16, 24$, $r = 4$, $a = 1$, $c = 1$, $n = 6$

	$b = 0$				$b = \sqrt{Rac}/\sqrt{r},\ T = U = 0$		b^*	$b = \sqrt{Rac}/\sqrt{r}$
	t_i	u_i	T	U	t_i	u_i		
$R = 1$	0.65	2.53	1	4.90	0.33	3.67	N/A	0.5
$R = 25/6$	0.97	1.36	4.17	10	0.68	3.32	N/A	1.02
$R = 16$	0.60	0.13	16	19.60	1.33	2.67	N/A	2
$R = 24$	0	0	24	24	1.63	2.37	1.71	2.45

5. Interdependence effect

When firms are interconnected on a common platform or network such as in a supply chain where upstream suppliers are connected via electronic data interchanges (EDI) to downstream manufacturers or retailers (which is an example of interdependent security), a security vulnerability in either the upstream or downstream firm can also impact the other firms. Consider the following scenario. Firm j is breached by a group of hackers and since firm i is connected to firm j through a common network (e.g. a virtual private network) it is also susceptible to a breach through the network. Now if firm i has invested in the best anti-intrusion technologies (for simplicity let us imagine installation of the most expensive firewalls at the edges – routers and switches), it is less likely to be hacked. Thus, the probability that firm i gets breached because its security risks are interdependent with firm j is likely to be dependent on the security investments made by both itself and the rival firm. Further the extent of the indirect attack would also depend on how closely connected the two firms are.[13]

Kunreuther and Heal (2003) ignore the income effect and substitution effect and focus on the interdependence effect where one target's defense benefits all targets. Examples occur within the airline industry, computer networks, fire protection, theft protection, bankruptcy protection, vaccinations. Kunreuther and Heal (2003, 232) illustrate

> "by reference to an airline that is determining whether to install a baggage checking system voluntarily. In making this decision it needs to balance the cost of installing and operating such a system with the reduction in the risk of an explosion from a piece of luggage not only from the passengers who check in with it, but also from the bags of passengers who check in on other airlines and then transfer to it".

A given airline benefits if all other airlines install baggage checking systems since then all bags transferred from other airlines are secure. The airline usually finds an interest in installing its own baggage checking system, but there is a free rider dilemma in who shall take on the cost of security investment.

In this interdependent case both firms usually find an interest in security investments, but there is a free rider dilemma in who shall take on the expenditure f^i of security investment. There is no free rider dilemma regarding the benefits. That is, firm i's share h^i of the asset r_i increases in both t_i and t_j, $\partial h^i/\partial t_i > 0$ and $\partial h^i/\partial t_j > 0$, in contrast to $\partial h^i/\partial t_j = 0$ in (2). In this section we alter the contest success function h^i in (2) and substitute the profits in (3) with

[13] I am indebted to an anonymous referee of this journal for the formulation in this paragraph.

$$u_i = \frac{t_i + \alpha t_j}{t_i + T_i + \alpha(t_j + T_j)} r_i - c_i t_i,$$
$$U = \frac{T_i + \alpha T_j}{t_i + T_i + \alpha(t_j + T_j)} r_i + \frac{T_j + \alpha T_i}{t_j + T_j + \alpha(t_i + T_i)} r_j - aT, \tag{9}$$

where α is the interdependence parameter, $\alpha \leqslant 1$. The interdependence α can be negative, but the contest success in (9) cannot be negative. With no interdependence, $\alpha = 0$, (9) reduces to (3). At the other extreme, maximum interdependence and $\alpha = 1$, the two firms are so intertwined or interdependent that an attack on one is tantamount to an attack on the other. In this case one firm's security investment defends both firms equally effectively, and the attack on one firm impacts both firms. Think e.g. of a Trojan Horse or self-replicating malevolent virus unleashed on one firm. If two firms are 100% interdependent, the Trojan Horse or virus spreads effectively throughout both firms.

Setting the derivatives of u_i with respect to t_i, and u_j with respect to t_j, equal to zero, $\partial u_i/\partial t_i = 0$ and $\partial u_j/\partial t_j = 0$, applying (1) and solving with respect to t_i and t_j gives

$$t_i = \frac{\sqrt{R/a}\left[\sqrt{r_i/c_i}\sqrt{\alpha + \beta - \alpha\beta} - \alpha\sqrt{r_j/c_j}\sqrt{1 - (1-\alpha)\beta}\right]}{1 - \alpha^2} - \frac{R\beta}{a}, \tag{10}$$

where t_j follows by permuting the indices and substituting β with $1 - \beta$. The profits u_i and U are found by inserting into (9). The symmetric case, $r_i = r_j = r$, $c_i = c_j = c$, $\beta = 1/2$ gives

$$t_i = \sqrt{\frac{R}{2a}}\left(\sqrt{\frac{r}{c(1+\alpha)}} - \sqrt{\frac{R}{2a}}\right), \quad u_i = r - \frac{(2+\alpha)\sqrt{Rrc}}{\sqrt{2a(1+\alpha)}} + \frac{Rc}{2a},$$
$$T_i = \frac{R}{2a}, \; U = \sqrt{\frac{2Rrc(1+\alpha)}{a}} - R \tag{11}$$

which reduces to (5) when $\alpha = 0$ and $n = 2$.

Proposition 5. (*i*) *Firm i invests in security technology when the required rate of return from security investment, divided by* $1 + \alpha$, *exceeds the average attack level, i.e. when* $r/(c(1+\alpha)) > R/an$. *Otherwise firm i does not invest in security technology.* (*ii*) *The agent attacks if* $2rc(1+\alpha) > Ra$, *and does otherwise not attack.* (*iii*) *The security investment* t_i *decreases in* α, *but with a positive second derivative, that is* $\partial t_i/\partial\alpha < 0$, $\partial^2 t_i/\partial\alpha^2 > 0$. (*iv*) *The profit* u_i *decreases in* α, *and with a negative second derivative, that is* $\partial u_i/\partial\alpha < 0$, $\partial^2 u_i/\partial\alpha^2 < 0$. (*v*) *The profit U increases in* α, *in a decreasing manner, that is* $\partial U/\partial\alpha > 0$, $\partial^2 U/\partial\alpha^2 < 0$.

The division of r/c with $1 + \alpha$, which is larger than one and increases in the interdependence, means that an even higher rate of return r/c is required for firm i to invest in security. Furthermore, when the requirement is met, firm i invests less when the interdependence is large, and earns a lower

profit. This means that interdependence causes free riding, which is detrimental for both firms. Each firm cuts down on its own investment and prefers the other to invest. The reason is that an attack on one firm is partly (to a degree α) channeled further to the other firm, and that one firm's defense partly benefits the other firm. This benefits the agent which directs a fixed attack and earns a higher profit due to lower security investment by the firms. The multiplication of $2rc$ with $1+\alpha$ means that the requirement for the agent to attack is more lenient ($2rc$ can be lower). The agent earns a higher utility with interdependence. The profit u_i for each firm decreases detrimentally in the interdependence parameter α. Both the first and second derivatives are negative. The profit U for the agent increases decreasingly with interdependence.

6. Substitution effect when agent moves first

In Sections 3–5 the agent makes attacks with T defined as $T = R/a$, but makes no strategic decision. In this section the agent makes a strategic decision about how to substitute his attack across the two firms. For analytical tractability, the substitution effect requires a two-stage game. The agent moves in the first stage deciding the substitution dependent on the firms' investment decisions t_i and t_j in the second stage. The two firms move in the second stage. The second stage is solved first. Although the games in Sections 3–5 are one-stage games, these can be conceived as two-stage games where T is determined dependent on t_i and t_j in the first stage (without the agent making a strategic decision), and the firms' investment decisions t_i and t_j are made in the second stage. This allows comparing the results in this section with the results in Sections 3–5.

Enders and Sandler (2003) describe for terrorism the substitution effect as follows:

> "If a government action increases the resource outlays necessary to undertake a particular type of operation, then there is a motive to substitute into some less costly operation that achieves a similar outcome at less cost. For example, the installation of screening devices in US airports in January 1973 made skyjackings more difficult, thus encouraging terrorists to substitute into other kinds of hostage missions or to stage a skyjacking from an airport outside of the United States".

Comparing the income (deterrence) and substitution (displacement) effect Lakdawalla and Zanjani (2002, p. 11) state that

> "displacement dominates the deterrence effect in the sense that protection by one target increases the terror investments directed at other targets. This follows directly from the concavity of the problem. Intuitively, protection by one target lowers the return to attacking that target,

but raises the relative return to investments in A and investments in attacking all other targets. Therefore, while private protection lowers the total resources devoted to terrorism T, it still creates negative externalities for other targets by exposing them to more terror risk''.

This statement is correct for Lakdawalla and Zanjani's (2002) model, but not for our model which allows raising the income reduction parameter b arbitrarily much without affecting substitutions. The income and substitution effects depend on each other in Lakdawalla and Zanjani's (2002) model, and are independent in our model. If b is sufficiently large, investment (protection) by one firm may lower the resource of the agent so much that the other firm enjoys a lower attack.

We may distinguish between three kinds of substitutions performed by the agent. The first is to adjust the attacks T_i and T_j against the two firms optimally dependent on all the characteristics of the two firms. The second, applicable when attacks and investments are multi-dimensional, is to substitute optimally between attack tools dependent on the firms' characteristics and how much each firm invests along each dimension. That is, if one firm invests heavily in employing security experts and developing intrusion detection systems, but designs a poor firewall, the agent may exploit the fact that the firm has a poorly designed firewall. The third is substitutions through time, compiling and accumulating resources during times when investments t_i and t_j are high, awaiting times when, hopefully, firms may relax their efforts and choose lower investments t_i and t_j. We focus on the first case where attacks and investments are one-dimensional. In this section we ignore the income effect which allows no analytical solution to the first order conditions when the firms are different. The firms need to be different in at least one respect in order for the agent to decide on a substitution. For two equivalent firms the agent is indifferent about substitutions. A plausible method for the agent is to set $T_j = T - T_i$ and perform the differentiation $\partial U/\partial T_i = 0$. This gives maximum profit through optimal allocation between T_i and T_j accounting for the two firms' security investments, investment inefficiencies, and assets.

Ceteris paribus, if firm i increases its investment t_i, then the agent performs some substitution of his attack from firm i to firm j, decreasing T_i and increasing T_j, realizing that firm i becomes a more difficult target, that is $\partial T_i/\partial t_i < 0$, $\partial T_j/\partial t_i > 0$. Firm i increases t_i if the increased share h^i of the asset r_i, due to the reduced T_i, exceeds the increased expenditure f^i of security investment. The investment t_i has a deterrent impact on the agent. In this section we determine the equilibrium investments t_i and t_j for the two firms, and the equilibrium attack T_i, assuming that the agent performs substitutions between T_i and T_j when the sum $T_i + T_j = T$ is fixed as in (1).

Consider a two-stage game where the agent moves first. The two firms move second, simultaneously, determining t_i and t_j for given T_i and T_j, where $T_j = R/a - T_i$. The second stage is solved first for t_i and t_j as functions of T_i. Thereafter the first stage is solved where the agent chooses T_i to maximize profit. As proved in Appendix, the investments and profits are

$$t_i = \frac{r_i\sqrt{R/a}}{\sqrt{c_i r_i + c_j r_j}}\left(1 - \frac{c_i\sqrt{R/a}}{\sqrt{c_i r_i + c_j r_j}}\right), \quad T_i = \frac{c_i r_i R/a}{c_i r_i + c_j r_j}, \tag{12}$$

$$u_i = r_i \quad 1 + \frac{c_i^2 R/a}{c_i r_i + c_j r_j} - \frac{2c_i\sqrt{R/a}}{\sqrt{c_i r_i + c_j r_j}}\Bigg), \quad U = \sqrt{R/a}\sqrt{c_i r_i + c_j r_j} - R, \tag{13}$$

where t_j and u_j are found by permuting the indices. Interestingly, (12) reduces to (5) for the symmetric case when $r_i = r_j = r$, $c_i = c_j = c$, $t_i = t_j$.

We henceforth introduce a new subscript f to signify investments t_{if} and t_{jf} and attacks T_{if} and T_{jf} for the two stage game where the agent moves first, and the firms move second. Similarly, we introduce the subscript n to signify investments t_{in} and t_{jn} and attacks T_{in} and T_{jn} for the one stage game analyzed in Sections 4 and 5 with no substitution effect.

Proposition 6. (*i*) *Firm i's security investment cost* t_i *increases in* r_i *and decreases in* c_i. (*ii*) *The attack* T_i *on firm i increases in the product* $c_i r_i$. (*iii*) *When* $c_i = c_j = c$ *and the substitution effect operates and the agent moves first, firm i with a larger asset,* $r_i > r_j$, *invests more in security than what the other firm j does in two equivalent firms with and without the substitution effect,* $t_{if} > t_{jf}$ *and* $t_{if} > t_{jn}$. *Furthermore, firm i suffers a larger attack than what firm j does with and without the substitution effect,* $T_{if} > T_{jf}$ *and* $T_{if} > T_{jn}$. (*iv*) *When* $c_i = c_j = c$ *and the substitution effect operates and the agent moves first, firm i invests more in security than what the same firm i does in two equivalent firms without the substitution effect,* $t_{if} > t_{in}$, *given that*

$$\sqrt{\frac{r_i}{c}} > \left(\frac{\sqrt{2r_i}}{\sqrt{r_i + r_j}} + 1\right)\sqrt{\frac{R}{2a}} \quad \textit{and} \quad r_i > r_j. \tag{14}$$

Furthermore, firm i suffers a larger attack with than without the substitution effect, $T_{if} > T_{in}$, *when* $r_i > r_j$.

Proposition 6(i) states that a valuable firm (r_i is high) with high investment efficiency ($1/c_i$ is high) incurs a higher security investment cost. Then firm i is worth defending, its investment is efficient, and it is willing to incur the cost. Conversely, a firm with high investment inefficiency (c_i is high) incurs a lower security investment cost. Proposition 6(ii) states that firm i attracts a large attack (T_i is high) if it is valuable (r_i is high) and has high investment ineffi-

ciency (c_i is high). Then the agent considers firm i as an attractive target, and as an easy prey. In this case the agent substitutes an optimal part of its attack away from firm j, in order to focus more on attacking firm *i*. In other words, a more valuable firm suffers a larger attack, and a firm with a high investment inefficiency suffers a larger attack. The first point is as important as the second. If one firm is x times more valuable than the other firm, but has an investment inefficiency that is a fraction $1/x$ of the inefficiency of the other firm, the substitution effect causes, ceteris paribus, equally large attacks on the two firms. The reason is that the first firm's substantial security investment deters the agent which has nothing to gain by attacking the first firm more than the second.

Proposition 6(iii) compares one firm with the substitution effect with the other firm with and without the substitution effect. The substitution effect causes a larger attack on the more valuable firm, and that firm invests more in security than the other firm.

Proposition 6(iv) compares one firm with the substitution effect with the same firm without the substitution effect. In the first case the firm faces a firm which differs from itself, which allows substitution to be meaningful. In the second case the firm faces a firm that is equivalent to itself, which gives a comparison benchmark. The substitution effect causes a larger attack on the more valuable firm. The RHS of (14) approaches zero when the resource R of the agent approaches zero. The asset r_i appears both on the LHS and RHS of (14). The RHS appearance is both in the numerator and denomina-tor. Hence (14) is satisfied if r_i is sufficiently large, regardless how large is R.

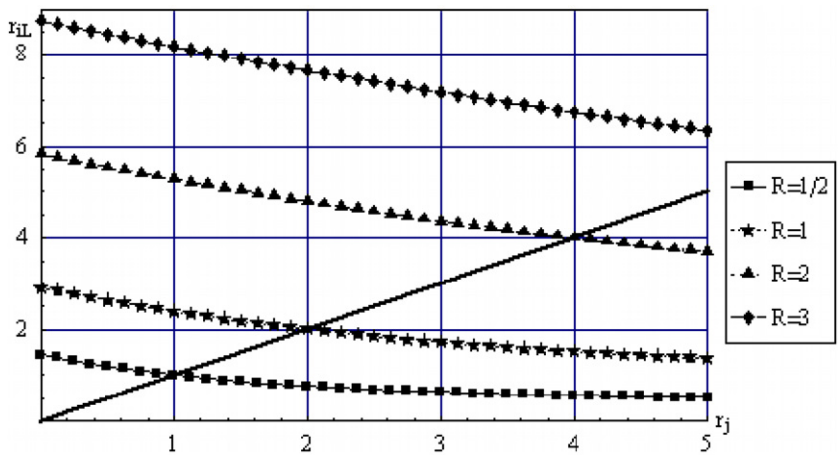

Fig. 2. Lower value r_{iL} of firm i for security investment to occur with substitution. Effect, $R = 1/2, 1, 2, 3$, $a = c = 1$.

The intuition is that the substitution effect causes the agent to direct its attack against the more valuable asset which needs to be protected. This means that firm i must be sufficiently valuable for the security investment to be larger with than without the substitution effect. It is quite possible that firm i is more valuable than firm j, that firm i suffers a larger attack due to the substitution effect, but that it invests less than without the substitution effect. Without the substitution effect firm i merely considers benefit versus cost facing a fixed attack. With the substitution effect firm i considers benefit versus cost while additionally accounting for a variable attack where the agent substitutes. This gives a different optimization scenario. The expenditure of security investment is subtracted linearly, while the benefit is determined by the ratio in the contest success function which does not operate linearly, and which is especially sensitive to the resource R of the agent. Firm i may decide to cut down on its security investment if the attack is overwhelming. We define r_{iL} as the value of r_i where (14) holds as an equality. When r_i is larger than this value, (14) holds as an inequality. Fig. 2 illustrates r_{iL} as a function of the asset r_j of the other firm when $R = 1/2, 1, 2, 3,\ a = c = 1$. The straight line shows $r_{iL} = r_j$. When $r_j = 2$ and R is small, e.g. $R = 1/2$, the requirement for r_i is $r_i > r_{iL} = 0.76$, which is satisfied since we require $r_i > r_j$. When $r_j = 2$ and R is large, e.g. $R = 2$, the requirement is $r_i > 4.79 = r_{iL}$ in order so that firm i invests more in security with the substitution effect than without it. In contrast, when $r_j < r_i < r_{iL} = 4.79$, firm i invests less with the substitution effect than without it. The reason is that the external threat is overwhelming, and the more valuable firm i suffers more of the attack when the substitution effect operates. When r_i is large, firm i suffers even more of the attack than firm j when the substitution effect operates, but the threat is no longer over-whelming, and firm i decides to fight it through a larger investment than without the substitution effect.

7. Interdependence and substitution effects when agent moves first

Analyzing the income effect, as presented in Section 4 where parts of the agent's resource is eliminated by applying the parameter b, together with the interdependence effect or the substitution effect is not analytically tractable. However, analyzing the interdependence and substitution effects is analytically tractable. The income effect can also be accounted for by considering the increase in the transformation inefficiency a, or decrease in the resource R, as pointed out in the beginning of Section 4. The income effect interpreted in this sense is analyzed in Section 3. This section can thus alternatively be conceived as analyzing all the three effects, where the impact of the income effect follows from considering the increase in a and decrease in R is the equations and propositions in this section. Accounting for the interde-

pendence parameter α when determining the investments and profits, as proved in Appendix, (12) and (13) generalizes to

$$t_i = \frac{\sqrt{R/a}}{(1-\alpha)\sqrt{c_i r_i + c_j r_j}} \left(\frac{(r_i - \alpha r_j)}{\sqrt{1+\alpha}} - \frac{(c_i r_i - \alpha c_j r_j)\sqrt{R/a}}{\sqrt{c_i r_i + c_j r_j}} \right),$$

$$T_i = \frac{(c_i r_i - \alpha c_j r_j) R/a}{(1-\alpha)(c_i r_i + c_j r_j)}, \tag{15}$$

$$u_i = r_i + \frac{c_i (c_i r_i - \alpha c_j r_j) R/a}{(1-\alpha)(c_i r_i + c_j r_j)} - \frac{c_i [(2-\alpha^2) r_i - \alpha r_j] \sqrt{R/a}}{(1-\alpha)\sqrt{1+\alpha}\sqrt{c_i r_i + c_j r_j}},$$

$$U = \sqrt{R/a}\sqrt{c_i r_i + c_j r_j}\sqrt{1+\alpha} - R. \tag{16}$$

Using from (1) that $T_i = \beta R/a$ where $\beta_i = \beta$, applying the second equation in (15) implies $\beta = (c_i r_i - \alpha c_j r_j)/[(1-\alpha)(c_i r_i + c_j r_j)]$. Inserting this value of β into (10) gives the first equation in (15). This means that the results for the interdependence and substitution effects are equivalent to the results for the interdependence effect when the appropriate β for the substitution is chosen. Inserting $r_i = r_j = r$ and $c_i = c_j = c$ into $\beta = (c_i r_i - \alpha c_j r_j)/[(1-\alpha)(c_i r_i + c_j r_j)]$ gives $\beta = 1/2$. Inserting the parameter values for this symmetric case into (15) and (16) gives (10).

Eq. (15) assumes that $c_i r_i \geqslant \alpha c_j r_j$. This inequality can be explained such that firm i will be attacked with a large T_i if it is valuable (r_i is high) or if its security investment is inefficient (c_i is high). As the interdependence α increases, the inequality becomes more strict. When the inequality is not satisfied, which means that firm j is so attractive that $c_j r_j > c_i r_i/\alpha$, the agent attacks exclusively firm j, setting $T_j = R/a$ and $T_i = 0$.

Proposition 7. *With* 100% *interdependence*, $\alpha = 1$, *the substitution effect is not a meaningful conception. Any choice* $0 \leqslant T_i, T_j \leqslant R/a$ *s.t.* $T_i + T_j = R/a$ *by the agent is optimal. Firm i chooses* $t_i = \sqrt{R/a}\sqrt{r_i/c_i} - R/a - t_j$, *and firm j chooses* $t_j = \sqrt{R/a}\sqrt{r_j/c_j} - R/a - t_i$, *which is indeterminate.*

When $\alpha = 1$, an attack on one firm is tantamount to and thus as effective as an attack on the other firm. Hence from a substitution point of view, it does not matter which firm the agent attacks. It may well attack firm j even when firm i is more attractive expressed by $c_i r_i > c_j r_j$. Hence any choice $0 \leqslant T_i, T_j \leqslant R/a$ s.t. $T_i + T_j = R/a$ is acceptable. Although firm i can choose the optimal t_i for a fixed t_j, and analogously for firm j, there is no joint solution, leading the firms to apply other considerations. In contrast, when the interdependence is arbitrarily smaller than 100%, the substitution effect applies with the solution described in this section.

8. All the three effects when the firms move first

Consider a two-stage game where the two firms move first. The agent moves second, determining T_i and T_j for given t_i and t_j. The second stage is solved first for T_i as a function of t_i and t_j. Inserting $T_j = [R - b(t_i + t_j)]/a - T_i$ into the second equation in (9) and differentiating with respect to T_i, $\partial U/\partial T_i = 0$, gives

$$T_i = \frac{\sqrt{r_i}\sqrt{t_i + \alpha t_j}\left(R - b(t_i + t_j) + a(t_j + \alpha t_i)\right) - \sqrt{r_j}\sqrt{t_j + \alpha t_i}\left(\alpha[R - b(t_i + t_j)] + a(t_i + \alpha t_j)\right)}{a(1-\alpha)\left(\sqrt{r_i}\sqrt{t_i + \alpha t_j} + \sqrt{r_j}\sqrt{t_j + \alpha t_i}\right)}. \tag{17}$$

Inserting (17) into the first equation in (9) and differentiating with respect to t_i, $\partial u_i/\partial t_i = 0$, gives the first order condition

$$\begin{aligned} & a\sqrt{r_i}\sqrt{r_j}\Big(R(t_j + 2\alpha t_i + \alpha^2 t_j) - (a-b)t_j(t_i - t_j)(1-\alpha)^2\Big) \\ & \quad + 2\sqrt{t_i + \alpha t_j}\sqrt{t_j + \alpha t_i}\big(ar_i[R + (a-b)t_j(1-\alpha)] - c_i(1+\alpha) \\ & \quad \times [R + (a-b)(t_i + t_j)]^2\Big) = 0 \end{aligned} \tag{18}$$

which when $\alpha = b = 0$ simplifies to

$$at_j\sqrt{r_i r_j}(R - a(t_i - t_j)) + 2\sqrt{t_i t_j}(ar_i[R + at_j] - c_i[R + a(t_i + t_j)]^2) = 0. \tag{19}$$

The first order condition for t_j is found by permuting the indices. There is no simple analytical solution. To compare with the earlier sections, inserting $r_i = r_j = r$, $c_i = c_j = c$, and $t_i = t_j$ into (19) and solving with respect to t_i gives

$$t_i = \frac{ar - 4cr + \sqrt{ar}\sqrt{ar + 16cR}}{8ac} \tag{20}$$

which can be compared with

$$t_i = \sqrt{\frac{R}{2a}}\left(\sqrt{\frac{r}{c}} - \sqrt{\frac{R}{2a}}\right) \tag{21}$$

which follows from (12) with the same insertions, and which equals (5) when $n = 2$. Eqs. (20) and (21) give the same value for t_i when $R = ar/2c$. Figs. 3 and 4 illustrate the security investments, attacks, and profits as functions of r_i when $R = 1$, $= 2$, $a = c = 1$, $n = 2$, which satisfies $R = ar/2c$ when $r_i = r_j = r = 2$. The subscript s on the variables refers to the two stage game in this section where the agent moves second, in contrast to subscript f when the agent moves first as in Section 6, and subscript n for the one stage game in Sections 4 and 5 with no substitution effect. The results are similar for both two stage games illustrating

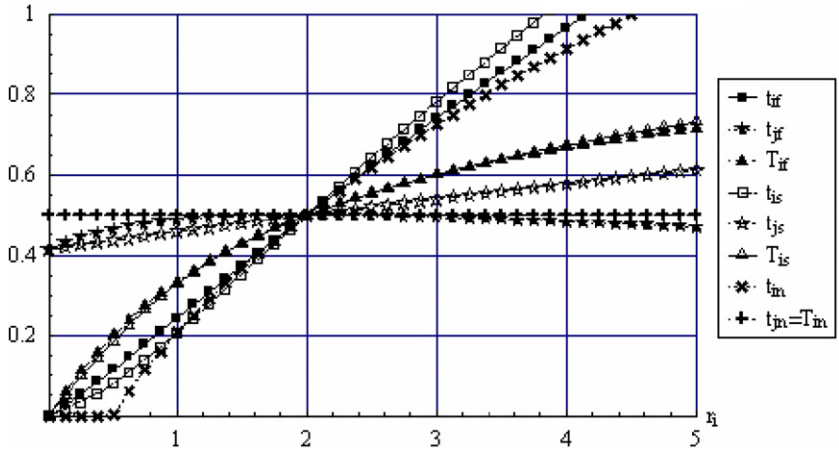

Fig. 3. Security investments $t_{if}, t_{is}, t_{in}, t_{jf}, t_{js}, t_{jn}, T_{if}, T_{is}, T_{in}$ as functions of r_i, $R = 1, = 2$, $a = c = 1$, $n = 2$.

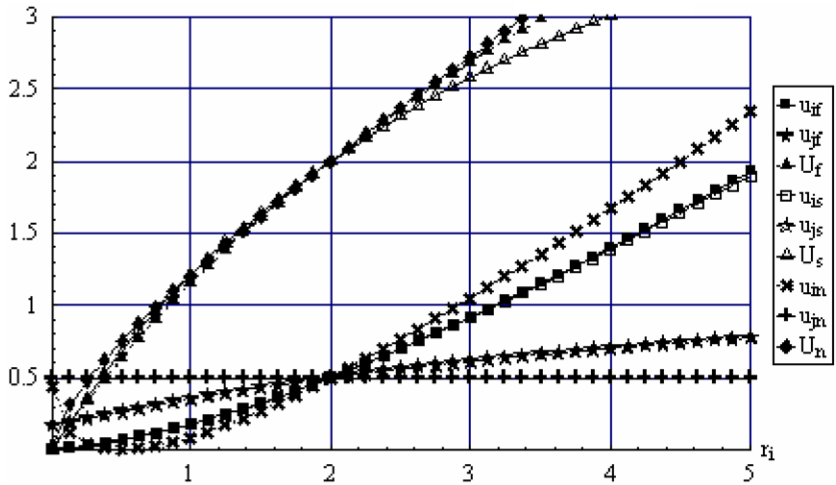

Fig. 4. Profits u_{if}, u_{is}, u_{in}, u_{jf},u_{js}, u_{jn}, U_f, U_s, U_n as functions of r_i, $R = 1, = 2$, $a = c = 1$, $n = 2$.

the substitution effect. Firm i's investment t_{in} without the substitution effect equals zero when $r_i < 0.5$ since the requirement $r_i/c > R/2a$ must be satisfied to ensure investment. Figs. 3 and 4 confirm the results in the propositions. When we increase R to $R = 2$, then $t_{if} < t_{in}$ when $2 < r_i < 4.79$, and $t_{if} > t_{in}$ when $r_i > 4.79$, as discussed after Proposition 6(iv).

9. Future research and limitations of the current work

The income, interdependence, and substitution effects have been analyzed in the context of security investment. A joint treatment of security investment and information sharing in the context of the three effects is complicated, but future research may find a way around this challenge. In their Proposition 2 Gal-Or and Ghose (2005, 193) find that "security technology investments and security information sharing act as 'strategic complements'". In contrast, Gordon et al. (2003) assume an alternative cost function and "find that when firms share information, each firm has reduced incentives to invest in information security". As Gal-Or and Ghose (2005) observe, "the main reason for the different result is the existence of the demand enhancing effects of information security sharing and technology investments in our model". The validity of strategic complementarity under various assumptions should be scrutinized in future research, preferably accounting for the three effects.

This article assumes that the firms' assets are exogenously given as in rent seeking. Future research may endogenize the assets into the production pro-cess (Hausken, 2005), to analyze how firms allocate resources into production versus security investment, and possibly other activities, accounting for infor-mation sharing. The firms are interdependent as specified by an interdepen-dence parameter. Each firm impacts the substitutions the external agent makes across firms, and impacts the agent's income which determines the agent's attack. Each firm's main contest is with the external agent over its asset, and the contest with other firms is indirect. Future research may model how each firm is involved in two contests, one with the agent and one with the other firms. This can be done by considering two contest success func-tions, or by modeling various forms of market behavior and competition between firms. E.g., each firm may produce one or several products which they exchange with each other, choosing prices and quantities optimally. Whereas the income effect has been successfully modeled for n firms, and the number of firms is essential for understanding the income effect, the inter-dependence and substitution effects have for analytical tractability reasons been analyzed only for two firms, which can be extended to n firms in future research. Different kinds of security investment can be analyzed, e.g. of defensive and offensive nature.

Future research may also introduce the time dimension. The income of firms and external agents fluctuate over time, interdependence between firms fluctuate over time according to market conditions, and agents make substitutions through time, sometimes accumulating resources during times when investments are high, awaiting the optimal times for attack. Keohane and Zeckhauser (2003) find that the optimal control of terror stocks relies on both periodic cleanup and ongoing abatement, a logic that applies for the

control of public bads such as pollution, and may apply also for security investment to combat cyber attacks. The intuition is that the economy of scale in reducing the cyber threat may make it optimal to do so only periodically. An example of this logic is Arrow et al.'s (1951) well-known (s, S) model of inventory management where the optimal policy in the face of stochastic demand for a product is to replenish inventory up to a level given by S every time it falls to or below s.

Further modeling possibilities are one sided or two sided incomplete information. The firms may be uncertain about the agent's resource and efficiency of transformation into attack, and the agent's substitution preference across firms and through time. The firms may be uncertain about each others' production, security investments, investment efficiencies, and information sharing. The agent may be uncertain about the firms' assets, production, security investment, investment efficiencies, information sharing, and capacity or willingness to withstand a cyber attack.

10. Conclusion

The article considers several firms in cyber war with external intruders conceived as unitary over the firms' assets. The external agent seeks to break through the security defense of the firms in order to appropriate assets, or to get information that can be converted into assets. Each firm gets to keep a fraction of its asset dependent on its security technology investment relative to the investment of the agent.

With no effects, each firm invests in security technology when the required rate of return from security investment exceeds the average attack level. This occurs when the ratio of the firm's asset and investment inefficiency is larger than the ratio of the agent's resource and transformation inefficiency divided by the number of firms. Otherwise there is no security investment, unless the formal control requirements dictate investment. Each firm's security investment increases concavely in the required rate of return, and is inverse U shaped in the average level of attack, which is the agent's resource divided by his transformation inefficiency and divided by the number of firms. Each firm invests maximally in security when the average level of attack is 25% of the firm's required rate of return from security investment.

The income effect is such that the agent's resource is not fixed, but gets reduced by the firms' security investments. Parts of the resource can be eliminated, attack tools can be made obsolete, intruder competence can be made useless, and the agent's ability to convert resources into an attack can be reduced. The income effect assumes an income reduction parameter which scales how much the firms' security investments reduce the agent's income. The security investments decrease in this parameter when the agent's resource

is low, which allows firms to cash in on the income effect. The agent's income is eventually eliminated. When the resource is intermediate, the security investments are inverse U shaped. It is comparatively expensive to invest when the income reduction parameter is low, and the firms cash in when the income reduction parameter is large. When the agent's resource is large, the security investments equal zero when the parameter is low. The firms realize that any investment against an overwhelming threat is a waste. As the parameter increases above a certain level, security investments increase.

When two firms are interdependent, security investment by one benefits also the other, and an attack against one impacts the other indirectly. Interdependence causes free riding. Each firm cuts down on its own investment and prefers the other to invest. Consequently, the security investments decrease as the interdependence increases. More interdependence causes lower profits for the firms and higher profits for the attacking agent.

The substitution effect means that the agent allocates its attack optimally between the two firms. The distribution of the attack is no longer fixed, but endogenized. Each firm's security investment increases in its asset and in its investment efficiency. The attack against each firm increases in the product of the firm's asset and investment inefficiency. Hence the agent does not go for the largest asset if a high investment efficiency ensures that it is too well protected. The article makes a few more specific analyses of how the substitution effect impacts security investment for differently sized firms.

Acknowledgements

An earlier version of this paper was presented May 26, 2005 at the Annual Forum on ''Financial Information Systems and Cyber Security: A Public Policy Perspective'', Robert H. Smith School of Business, University of Maryland. I thank John Bagby, William Lucyshyn, Chih-Yang Tseng, forum participants, the editors and the referees for their useful comments.

Appendix

Proposition 1 follows from requiring that $u_i > 0$ and $U > 0$ in (5). Proposition 2 follows from

$$\begin{aligned} \frac{\partial t_i}{\partial (r/c)} &= \frac{\sqrt{R/(an)}}{2\sqrt{r/c}} > 0, \quad \frac{\partial^2 t_i}{\partial (r/c)^2} = -\frac{\sqrt{R/(an)}}{4(r/c)^{3/2}} < 0, \\ \frac{\partial t_i}{\partial (R/an)} &= \frac{\sqrt{r/c}}{2\sqrt{R/(an)}} - 1, \quad \frac{\partial^2 t_i}{\partial (R/an)^2} = -\frac{\sqrt{r/c}}{4(R/(an))^{3/2}} < 0. \end{aligned} \tag{A.1}$$

Proof of Proposition 3. (i) Differentiating t_i in (7) with respect to b, thereafter setting $b = 0$, and equating with zero, gives

$$\left.\frac{\partial t_i}{\partial b}\right|_{b=0} = \frac{a(3n-1)\sqrt{Rrcn} - [ra(n-1)+2Rc]n\sqrt{a}}{2a^{5/2}cn^2} = 0 \Rightarrow R = \begin{cases} ra(n-1)^2/4cn, \\ ran/c. \end{cases} \tag{A.2}$$

The first value of R in (A.2) is always less than the second value, and this proves the first part. The second part follows from Proposition 1. (ii) Differentiating t_i in (7) with respect to b, thereafter setting $b = \sqrt{Rac}/\sqrt{r}$, and equating with zero, gives

$$\left.\frac{\partial t_i}{\partial b}\right|_{b=\sqrt{Rac}/\sqrt{r}} = \frac{r\left(-(n-1)\sqrt{ra}+2\sqrt{Rc}\right)}{acn\left((n+1)\sqrt{ra}-2\sqrt{Rc}\right)} = 0 \Rightarrow R = \frac{ra(n-1)^2}{4c}. \quad \square \tag{A.3}$$

Proof of Proposition 4. (i) t_i in (7) is of the first order in b in the numerator, and in the second order in b in the denominator. Proposition 3 implies that t_i decreases throughout when $R < ra(n-1)^2/4cn$. (ii) Proposition 3 specifies initial increase when $b = 0$, and eventual decrease when $b = \sqrt{Rac}/\sqrt{r}$, which gives the inverse U shape. (iii) $ra(n-1)^2/4c < ran/c$ implies $n^2 - 6n + 1 < 0$ which is valid when $n \leqslant 5$. Proposition 3 implies that t_i increases throughout. (v) Proposition 3 implies that t_i equals zero for $b = 0$ when $ran/c < R$. Inserting the upper relevant $b = \sqrt{Rac}/\sqrt{r}$ (which causes $T = 0$) into the expression inside the root in (7) gives $Rc\left((n+1)\sqrt{ra}-2\sqrt{Rc}\right)^2/r^2$ which is always positive. However, the expression $(an-b)(a-b)$ inside the root in (7) is negative when $a < b < an$ which means that a sufficiently large Rc/r can cause negativity under the root. This is prevented by requiring the expression inside the root in (7) to be larger than zero, which implies

$$\begin{aligned} &b^2(n-1)^2 + \frac{4Rc(an-b)(a-b)}{ra} > 0 \\ &\quad \Rightarrow b > \frac{2ac\sqrt{R}\left((n+1)\sqrt{R}+(n-1)\right)\sqrt{R-ran/c}}{ra(n-1)^2+4Rc} = b^* \end{aligned} \tag{A.4}$$

which defines b^*. Inserting $R = ran/c$ into (7) gives

$$t_i = \frac{ra(b(n+1)-2an)}{(a-b)^2cn} \tag{A.5}$$

which causes $b^* = 2an/(n+1)$ which is larger than a when $n > 1$, and equal to a when $n = 1$. Keeping $b = b^*$, but increasing R above $R = ran/c$ causes

unacceptable negativity under the root sign in (7). In this case the firm chooses zero security investment $t_i = 0$ since the resource of the agent is overwhelming. That is, t_i equals zero when $0 \leqslant b < b^*$. Only when $b > b^*$ does the firm choose $t_i > 0$, and it does so as long as $b < \sqrt{Rac}/\sqrt{r}$ which is the upper limit which eliminates the agent's resource causing $T = 0$. This implies that t_i increases throughout when $b^* < b < \sqrt{Rac}/\sqrt{r}$. (iv) Proposition 3 implies that t_i equals zero for $b = 0$ when $ran/c < R$. Proposition 4(v) implies that t_i equals zero when $0 \leqslant b < b^*$. Proposition 3 implies that t_i decreases in b when $b = \sqrt{Rac}/\sqrt{r}$ and $R < ra(n-1)^2/4c$. This implies that t_i is inverse U shaped when $b^* < b < \sqrt{Rac}/\sqrt{r}$ and $n > 5$. □

Both the numerator and denominator of (7) equal zero when $b = a$. Applying L'Hopital's rule twice on (7) gives

$$b = a \Rightarrow t_i = \frac{Rc\left(\frac{r}{c} - \frac{R}{an}\right)}{ra(n-1)}, \quad u_i = \frac{\left(\frac{r}{c} - \frac{R}{an}\right)^2 nc^2}{r(n-1)}, \quad T_i = \frac{Rc\left(\frac{R}{a} - \frac{r}{c}\right)}{ran(n-1)},$$
$$U = \frac{nc\left(\frac{R}{a} - \frac{r}{c}\right)}{(n-1)} \tag{A.6}$$

which gives $T = 0$ when $R/a = r/c$, which gives $t_i = R/an$ and $u_i = r(n-1)/n$.

Proof of Proposition 5. (i) and (ii) follow from requiring that $u_i > 0$ and $U > 0$ in (11). (iii) follows from differentiating $(1+\alpha)^{-1/2}$ in (11) once for the sign of the first derivative, and twice for the sign of the second derivative. (iv) and (v) follow from differentiating u_i and U. □

Proof of Eqs. (12), (13), (15), (16). It suffices to prove (15) and (16), from which (12) and (13) follow from inserting $\alpha = 0$. We insert $T_j = R/a - T_i$ into the first equation in (9) and differentiate with respect to t_i, $\partial u_i/\partial t_i = 0$. We sim-ilarly determine $\partial u_j/\partial t_j = 0$, and solve, which gives

$$t_i = \frac{\sqrt{r_i/c}\sqrt{T_i + \alpha(R/a - T_i)} - \alpha\sqrt{r_j/c}\sqrt{R/a - T_i + \alpha T_i}}{1-\alpha^2} - T_i,$$
$$t_j = \frac{\sqrt{r_j/c}\sqrt{R/a - T_i + \alpha T_i} - \alpha\sqrt{r_i/c}\sqrt{T_i + \alpha(R/a - T_i)}}{1-\alpha^2} - (R/a - T_i) \tag{A.7}$$

as the solution of the second stage, where t_j is found by permuting the indices. For the first stage, inserting (A.7) into the second equation in (9) and differentiating with respect to T_i, $\partial U/\partial T_i = 0$, gives the second equation in (15). Inserting this value of T_i into (A.7) gives the first equation in (15). Inserting into (9) gives (16).

Proof of Proposition 6. (i) Differentiating t_i in (12) with respect to r_i and c_i gives

$$\frac{\partial t_i}{\partial r_i} = \frac{\sqrt{R/a}}{(c_i r_i + c_j r_j)^{3/2}} \left(\frac{c_i r_i + 2c_j r_j}{2} - \frac{c_i c_j r_j \sqrt{R/a}}{(c_i r_i + c_j r_j)^{1/2}} \right) = \frac{r_i}{2(c_i r_i + c_j r_j)}$$

$$\text{when } R = \frac{a(c_i r_i + c_j r_j)}{c_i^2},$$

$$\frac{\partial t_i}{\partial c_i} = -\frac{r_i \sqrt{R/a}}{(c_i r_i + c_j r_j)^{3/2}} \left(\frac{c_j r_j \sqrt{R/a}}{(c_i r_i + c_j r_j)^{1/2}} + \frac{r_i}{2} \right) < 0. \tag{A.8}$$

The negative occurrence of R inside the bracket in the expression for $\partial t_i/\partial r_i$ causes the bracket to be smallest when R is largest. The largest acceptable value of R is $R = a(c_i r_i + c_j r_j)/c_i^2$, which gives $t_i = 0$ in (12). It follows that $\partial t_i/\partial r_i > 0$. (ii) Follows from the second equation in (12). □

Proof of Proposition 6(iii). Eq. (12) implies $t_j = (r_j/r_i)t_i$ when $c_i = c_j$, which implies $t_{if} > t_{jf}$ when $r_i > r_j$. Requiring that $t_i = t_{if}$ in (12) is larger than $t_j = t_{jn}$ in (4) for $\beta_i = 1/2$ gives

$$\frac{r_i \sqrt{R/a}}{\sqrt{c}\sqrt{r_i + r_j}} \left(1 - \frac{c\sqrt{R/a}}{\sqrt{c}\sqrt{r_i + r_j}} \right) > \sqrt{\frac{R}{2a}} \left(\sqrt{\frac{r_j}{c}} - \sqrt{\frac{R}{2a}} \right)$$

$$\Rightarrow \frac{r_i \sqrt{2}}{(r_i + r_j)} \left(\frac{\sqrt{r_i + r_j}}{\sqrt{c}} - \sqrt{\frac{R}{a}} \right) > \sqrt{\frac{r_j}{c}} - \sqrt{\frac{R}{2a}}. \tag{A.9}$$

A weaker requirement is

$$\frac{r_i \sqrt{2}}{(2r_i)} \left(\frac{\sqrt{r_i + r_j}}{\sqrt{c}} - \sqrt{\frac{R}{a}} \right) > \left(\sqrt{\frac{r_j}{c}} - \sqrt{\frac{R}{2a}} \right) \Rightarrow \sqrt{r_i + r_j} > \sqrt{2r_j} \tag{A.10}$$

which is always satisfied when $r_i > r_j$. Eq. (12) with $c_i = c_j$ implies $T_{if} > T_{jf}$ when $r_i > r_j$. Comparing this equation with the third equation in (5) when $n = 2$ implies $T_{if} > T_{jn}$ when $r_i > r_j$. □

Proof of Proposition 6(iv). Replacing r_j with r_i on the RHS of (A.9) gives

$$\frac{r_i \sqrt{2}}{(r_i + r_j)} \left(\frac{\sqrt{r_i + r_j}}{\sqrt{c}} - \sqrt{\frac{R}{a}} \right) > \left(\sqrt{\frac{r_i}{c}} - \sqrt{\frac{R}{2a}} \right) \tag{A.11}$$

which when applying $(x^2 - 1) = (x - 1)(x + 1)$ can be written as

$$\sqrt{\frac{r_i}{c}} \left(\frac{\sqrt{2r_i}}{\sqrt{r_i + r_j}} - 1 \right) > \left(\frac{\sqrt{2r_i}}{\sqrt{r_i + r_j}} - 1 \right) \left(\frac{\sqrt{2r_i}}{\sqrt{r_i + r_j}} + 1 \right) \sqrt{\frac{R}{2a}} \tag{A.12}$$

which abbreviates to (14) when $r_i > r_j$. Comparing T_i in (12) with T_i in (5) implies $T_{if} > T_{in}$ when $n = 2$ and $r_i > r_j$. □

Proof of Proposition 7. Inserting $\alpha = 1$ into (12) and (A.7) gives zero in the denominators. More fundamentally, applying (9) to determine $\partial u_i/\partial t_i = 0$ and $\partial u_j/\partial t_j = 0$ gives the two indeterminate expressions for t_i and t_j in Proposition 7. □

References

Anderson, R., 2001. Why information security is hard: An economic perspective. In: *Proceedings of 17th Annual Computer Security Applications Conference*, December.

Arrow, K.J., Harris, T., Marschak, J., 1951. Optimal inventory policy. *Econometrica* 19, 250–272.

Bagby, J., 2005. *The Confluence of Public Policy on Information Security Controls.* Pennsylvania State University.

Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security* 11 (3), 431–448.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of internet security breach announcements on shareholder wealth. *International Journal of Electronic Commerce* 9 (1), 69.

Dalvi, N., Domingos, P., Mausam, M., Sanghai, S., Verma, D., 2004. Adversarial classification. In: *Proceedings of the 2004 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining Table of Contents,* Seattle, WA, USA, pp 99–108, ISBN:1-58113-888-9.

Dhillon, G., Silva, L., Backhouse, J., 2004. Computer crime at CEFORMA: a case study. *International Journal of Information Management* 24, 551–561.

Enders, W., Sandler, T., 2003. What do we know about the substitution effect in transnational terrorism? In: Silke, A., Ilardi, G. (Eds.), *Researching Terrorism: Trends, Achievements, Failures,* Frank Cass, Ilfords, UK.

Gal-Or, E., 1985. Information sharing in oligopoly. *Econometrica* 53 (2), 329–343.

Gal-Or, E., Ghose, A., 2003. The economic consequences of sharing security information. In: *Proceedings of the Second Workshop on Economics and Information Security*, May 29–30, University of Maryland.

Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. *Information Systems Research* 16 (2), 186–208.

Gordon, L.A., Loeb, M., 2001. Using information security as a response to competitor analysis systems. *Communications of the ACM* 44 (9), 70–75.

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

Gordon, L.A., Loeb, M., 2003. Expenditures on competitor analysis and information security: a managerial accounting perspective. In: Bhimani, A. (Ed.), *Management Accounting in the New Economy.* Oxford University Press, pp. 95–111.

Gordon, L.A., Loeb, M., Lucyshyn, W., 2003. Sharing information on computer systems security: an economic analysis. *Journal of Accounting and Public Policy* 22 (6), 461–485.

Hausken, K., 2002. Probabilistic risk analysis and game theory. *Risk Analysis* 22 (1), 17–27.

Hausken, K., 2005. Production and conflict models versus rent seeking models. *Public Choice* 123, 59–93.

Hausken, K., 2006. Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers* 8(5), in press.

Hirshleifer, J., 1989. Conflict and rent-seeking success functions: ratio vs. difference models of relative success. *Public Choice* 63, 101–112.

Howard, J., 1997. *Analysis of security incidents on the Internet.* Unpublished Doctoral Dissertation, Carnegie Mellon University. Available from <www.cert.org/research/JHThesis/Start.htm>.

Keohane, N., Zeckhauser, R.J., 2003. The ecology of terror defense. *The Journal of Risk and Uncertainty* 26 (2/3), 201–229.

Kirby, A., 1988. Trade associations as information exchange mechanisms. *RAND Journal of Economics* 29 (1), 138–146.

Kjaerland, M., 2005. A classification of computer security incidents based on reported attack data. *Journal of Investigative Psychology and Offender Profiling* 2 (2), 105–120.

Kunreuther, H., Heal, G., 2003. Interdependent security. *The Journal of Risk and Uncertainty* 26 (2/3), 231–249.

Lakdawalla, D., Zanjani, G., 2002. *Insurance, self-protection, and the economics of terrorism.* RAND and NBER, Federal Reserve Bank of New York.

Novshek, W., Sonnenschein, H., 1982. Fulfilled expectations in cournot duopoly with information acquisition and release. *Bell Journal of Economics* 13 (1), 214–218.

Porter, M., 1980. *Competitive Strategy: Techniques for Analyzing Industries and their Competitors.* Free Press, New York, NY.

Schechter, S., Smith, M., 2003. How much security is enough to stop a thief? In: *Proceedings of the Financial Cryptography Conference,* Guadeloupe, January.

Schenk, M., Schenk, M., 2002. Defining the value of strategic security. *Secure Business Quarterly* 1 (1), 1–6.

Shapiro, C., 1986. Exchange of cost information in oligopoly. *Review of Economic Studies* 53 (3), 433–446.

Skaperdas, S., 1991. Conflict and attitudes toward risk. *American Economic* Review 81, 116–120.

Skaperdas, S., 1996. Contest success functions. *Economic Theory* 7, 283–290.

Tanaka, H., Matsuura, K., 2005. *Vulnerability and effects of information security investment: a firm level empirical analysis of Japan.* Presented May 26, 2005 at the University of Maryland Forum: "Financial Information Systems and Cyber Security: A Public Policy Perspective".

Tanaka, H., Matsuura, K., Sudoh, O., 2005. Vulnerability and information security investment: an empirical analysis of E-local government in Japan. *Journal of Accounting and Public Policy* 24, 37–59.

Varian, H., 2002. System reliability and free riding. In: *Proceedings of the First Workshop on Economics and Information Security*, May 16–17, University of California, Berkeley.

Vives, X., 1990. Trade association disclosure rules, incentives to share information, and welfare. *RAND Journal of Economics* 21 (3), 409–430.

Ziv, A., 1993. Information sharing in oligopoly: the truth-telling problem. *RAND Journal of Economics* 24 (3), 455–465.