Interdependent risk networks: the threat of cyber attack

Annette Hofmann*

Institute for Risk and Insurance,
University of Hamburg,
Von-Melle-Park 5, 20146 Hamburg, Germany
E-mail: hofmann@econ.uni-hamburg.de
*Corresponding author

Hidajet Ramaj

Institute of Entrepreneurial Studies and Innovation Management,
Humboldt-Universitaet zu Berlin,
Dorotheenstrasse 1, 10117 Berlin, Germany
E-mail: hidajet.ramaj@wiwi.hu-berlin.de

Abstract: This article presents an economic model that explicitly reflects the interdependent risk structure of a cyber network. We find that due to this interdependent risk structure, the level of cyber risk protection in the community is inefficient from the community's overall viewpoint. The analysis further suggests that decision processes should take into account the interdependent risk structure of the underlying internet-based network. Therefore, an organisation that invests in comprehensive cyber risk protection should be rewarded by other organisations for the benefits (in the form of lower exposure risk) that it has brought to the network. Another promising way to improve protection is to subsidise high-exposure organisations. It is also important that states implement laws to prevent cyber attacks and to protect organisations. Formal contractual agreements between different organisations specifying their data and information exchange and other interactions may also prove a promising strategy. A successful agreement may involve using rewards as coordinative mechanisms; for instance, in using non-monetary web certificates. Finally, the development of international standards for tracking and tracing technologies is essential in order to improve cyber safety.

Keywords: cyber harassment; cyber risk; cyber attack; cyber networks; cyber risk protection; cyber security; economic model; interdependencies; interdependent risks; information network; positive externalities; public goods.

Reference to this paper should be made as follows: Hofmann, A. and Ramaj, H. (2011) 'Interdependent risk networks: the threat of cyber attack', *Int. J. Management and Decision Making*, Vol. 11, Nos. 5/6, pp.312–323.

Biographical notes: Annette Hofmann is a Post-doc at the Institute for Risk and Insurance, Faculty of Economics and Social Sciences, Hamburg University (Germany), where she obtained her PhD in Business Administration in 2009. Her research focuses on risk and insurance economics, health economics and industrial organisation.

Hidajet Ramaj is a Post-doc at the Humboldt-Universität zu Berlin (Germany), School of Business and Economics, Institute for Entrepreneurial Studies and Innovation Management. Before joining the Faculty at Humboldt-Universität in 2009, she received her PhD in Finance from Hamburg University (Germany). Her research focuses on entrepreneurial finance, firm disclosure credibility and capital markets.

1 Introduction

Information technology is growing rapidly, and the volume of available and valuable information and the avenues for attaining it constitute a challenge for information security (Hoo, 2000). According to Internet World Stats (2010), more than 1.9 billion people worldwide use the internet today. People can distribute information rapidly through the internet to anyone in the world. Because internet and computer-based systems today communicate more and more with one another, mostly as anonymous partners, they are becoming increasingly vulnerable to *cyber harassment* and *cyber attacks* (Meadows, 2001).

Cyber harassment is the online version of traditional peer harassment, where a bully directs harassment at a victim in view of an audience of peers (Espelage and Swearer, 2003). In legal terms, harassment is generally defined as a form of uninvited and/or unwanted conduct that annoys, threatens, intimidates, or even alarms. In the USA, it is governed by state law. Cyber harassment can take different forms, ranging from touching or verbal insult that is derogatory (section 240.25 Common Law) to shoving, and physical contract that is aimed at intimidating (section 240.30). Also, cyber harassment can be committed against various groups, e.g., individuals, organisations and society at large.

In contrast, *cyber attack* is an amorphous/undefined term that describes various actions, such as for example cyber espionage, denial-of-service attacks, malicious software, and the distribution of an electronic virus. All these examples do not fit under either of the legal classifications mentioned above. This form of cyber crime fits into the realm of an assault or even battery. According to McGavran (2009, p.261) “legal regimes are less than adequate in dealing with the threats and opportunities posed by different types of cyber attacks”. Our theoretical model in Section 2 will refers to the definition of cyber attacks, but does not exclude cyber harassment.

There is a specific growing pattern of attacks against organisations. Organisations often use the internet now to undertake commercial, social, informational, political or other activities (Adomi and Igun, 2008). As a result, it is no surprise that information security is a growing priority for many organisations (Gordon and Loeb, 2002). Most organisations greatly depend on their IT systems and networks. Substantial amounts of data are either stored or transmitted on a daily basis between computers that are interlinked in complex communication networks (Buzzard, 1999). For example, organisations that use the internet for e-commerce truly need their IT systems if they are to function properly (Garg et al., 2003). Many organisations are faced with an extremely complex information security environment to which they must pay close attention to neutralise individual risks (Kotulic and Clark, 2004). Thus, information security is highly important for organisations looking to secure/save their data from different kinds of malicious acts or attacks (Buzzard, 1999), including viruses, which proliferate via e-mail or through the internet and therefore can harm not just one but many organisations (Garg et al., 2003).

The problem has become pressing in many internet-based communication channels (e.g., blogs and social media websites), and organisations are seeking cost-efficient remedies. "Information security is a major IT priority for many firms, and spending on security products and services is ballooning according to the CSI/FBI report and others" [Kumar et al., (2007), p.25]. Such investments in protection measures implicitly benefit others because one party's investment decision will have an impact on the utility of the other parties connected to it (Kumar et al., 2007). For example, such an externality effect arises when interconnected systems are attacked by internet worms (Kumar et al., 2007). An important feature of the problem is that it takes place via an underlying network, i.e., the vulnerability of a party to harassment or a cyber attack depends on interactions with other parties in the community. In other words, cyber risks are interdependent (Kearns, 2005). Networks, including virtual networks, become increasingly valuable when they include an increasing number of users (Anderson, 2001; Kakade et al., 2005). Due to the structure of networks, different actors' levels of risk of becoming the victim of a cyber attack are interdependent. These interactions play a prominent role in the management of cyber risk. As a result, studying the economic incentives of the parties involved can provide a great deal of insight.

Most research on information security is anecdotal (e.g., Adomi and Igun, 2008; Blakley et al., 2001; Anderson, 2001; Finne, 2000; Buzzard, 1999; Ellison and Akdeniz, 1998), and there is little empirical research in this area (e.g., Kotulic and Clark, 2004; Hoo, 2000). Theoretical models of information security do focus on other issues like investment (Gordon and Loeb, 2002) or external effects on a micro-decision level (Kumar et al., 2007). However, external effects in an interdependent risk network are highly relevant, and the aim of this paper is to address this gap by offering an appropriate model. Our model applies the concept of interdependent risks (Kunreuther and Heal, 2003) to cyber harassment risk networks. We then discuss the implications of the model for efforts to combat cyber harassment risk. In particular, the model builds on the work of Kunreuther and Heal (2003) on interdependent security (IDS) models but is different in the following respects:

1 we assume heterogeneous players instead of homogeneous players

2 we use a continuum of players instead of a discrete setting

3 the probabilities are endogenous in our model.

Firms differ in their degree of vulnerability to cyber harassment or cyber attacks (e.g., a virus). According to Kumar et al. (2007), firms face different levels of risk exposure with regard to cyber harassment. "When comparing two real world enterprises, one with the divisions having very similar IT systems (and similar configuration) the CIO must deploy a lower level of countermeasures than in an enterprise when the systems are very different (say Windows and Unix) ceteris paribus" [Kumar et al., (2007), p.25]. For example, an information provider wants information to be available to its users on its website. A small online travel agency wants its services to be available to customers all day long. When its website is attacked, the travel agency may incur considerable losses due to business interruption. However, this small firm needs a different level of information protection than a large credit card firm, which will need a significant amount of personal data about its customers to be protected from cyber attacks. This firm would be substantially affected if these data were to be made public. Because both firms would be exposed in different ways, they would also incur different monetary, legal and/or reputational losses. To protect themselves against these risks, firms need different technologies to prevent cyber harassment, and these technologies involve different costs. We will therefore assume firms to be heterogeneous in our model below; some have higher protection cost than others.

From a purely economic viewpoint, the problem can be broken down as follows. Some parties invest in protection against cyber attack, which creates some cost (i.e., discomfort, time or money). In return, they receive some benefit through reduced risk, but a part of the benefit is public: the entire community also experiences reduced risk of attack, and thus, everybody else benefits. Hence, in economic terms, there is a *positive externality* associated with investing in protection: decreased risk to others. A well-known result in public economics suggests that when such interdependencies are present, equilibrium behaviour will be inefficient (Pigou, 1920). In our setting, this means the total level of activities used to fight cyber attacks in the community will be 'too low' relative to the overall efficient level. Therefore, the resulting allocation of risk-bearing will not be efficient. The challenge is to find ways to improve the risk allocation and reduce this inefficiency.

The remainder of the paper is organised as follows. The next section introduces our formal model within a simple expected utility framework. We introduce multiple firms and heterogeneity. In the following section, we present the community equilibrium and the associated welfare consequences. A discussion of policy implication that may help to reduce inefficiency in the community and some concluding remarks follow.

2 The model

At the core of the problem is a setting in which corporate decisions to invest in risk mitigation tend to be heavily influenced by natural notions of risk 'contagion'. Kunreuther and Heal (2003) offer a class of economic models called IDS games. They focus on the interdependency of terrorism risk in the context of international airline security for identical players. They also expand their work to include a more general model of IDS games in Heal and Kunreuther (2004). In the general model, three classes of IDS problems are identified: partial protection (class 1 problems), complete protection (class 2 problems), and positive interdependencies (class 3 problem). In an IDS problem of the first (second) class, risk cannot (can) be completely eliminated via an investment in security, and there remains a (no) residual indirect risk due to the behaviour of others. In an IDS problem of the third class, positive interdependencies arise. One example is investments in research and development (Heal and Kunreuther, 2007). Cyber attack risk is a first- or second-class IDS problem.

Consider an economy with many organisations who interact via the internet and are exposed to some risk of cyber attack. All organisations derive some positive utility $\overline{u}$ from using the internet, which is reduced to $\underline{u} < \overline{u}$ in the case of a cyber attack. Now assume that there is some technology that can eliminate the risk of an attack. Such technologies may include anti-malware products or other types of anti-cyber risk software or technology. Each firm must decide whether to invest in such a technology.

We assume that organisations differ in the costs that they must pay to be successful in preventing harassment risk using anti-malware products; i.e., plausible security screening investments may differ. Organisations may need different technologies. Different technologies are associated with different costs. For instance, very powerful internet protection software is more costly than a less suitable software alternative. A small firm may not require a sophisticated product, whereas a larger firm that operates on many different internet sites is more vulnerable and may thus need more sophisticated protection technologies.

Let the probability of a cyber attack be $q(x)$, where x denotes the proportion of organisations *without* protection in the internet community. This reflects the fact that once a firm is infected by malicious software, other organisations may suffer the same fate because they may get the virus via that firm's communication channels. x satisfies $0 \leq x \leq 1$. In general, the greater the proportion of organisations without protection in the economy, the greater each firm's risk of attack. We assume that $q'(x) > 0$ and $q''(x) \geq 0$. $q(x)$ satisfies $0 \leq q(x) \leq \overline{q}$, where $q(1) = \overline{q} < 1$ and $q(0) = 0$. These assumptions may be interpreted as follows. If no firm invests in protection ($x = 1$), then $\overline{q}$ will denote the maximum risk of an attack in the community; this risk will generally be smaller than one. In contrast, if every firm invests in protection ($x = 0$), then the risk of a cyber attack will be zero because every firm will be protected.

Organisations with 'low' cost will tend to invest in protection, whereas those with 'high' cost will not. In our model, it is useful to list organisations in ascending order according to their individual cost. The total number of organisations in the economy is normalised to unity. Protection cost c is distributed via a (non-degenerate) distribution function $F(c)$ and density function $f(c)$, defined over the support $[0, \overline{c}]$. All organisations in the community are free to choose whether or not to invest in a protection technology. The expected utility of a firm that does *not* invest in protection is then

$$EU_{NP}(x) = q(x)\underline{u} + (1 - q(x))\overline{u} \tag{1}$$

whereas the expected utility of a firm that invests in protection at cost c is given by

$$EU_P(c) = \overline{u} - c \tag{2}$$

Since the risk is reduced to zero.[1] Generally, a firm will invest in protection if the *excess* expected utility with a protective investment over the expected utility without such an investment is non-negative: $\Psi(x, c) = EU_P - EU_{NP} \geq 0$.[2] To find the equilibrium, we define the excess expected utility to the marginal firm as $\Psi(x(c_m), c_m) \equiv \Psi(c_m)$ so that

$$\Psi\left(x\left(c_m\right), c_m\right) = EU_P\left(c_m\right) - EU_{NP}\left(x\left(c_m\right)\right) \tag{3}$$

with

$$EU_{NP}\left(x\left(c_m\right)\right) = q\left(x\left(c_m\right)\right)\underline{u} + \left(1 - q\left(x\left(c_m\right)\right)\right)\overline{u} \tag{4}$$

and

$$EU_P\left(c_m\right) = \overline{u} - c_m, \tag{5}$$

Where $x(c_m)$ denotes the proportion of organisations *without* protection against cyber attacks in the community, given that the marginal firm has cost c_m:

$$x\left(c_m\right) = \int_{c_m}^{L} f(c)\,dc = 1 - F\left(c_m\right). \tag{6}$$

$dx(c_m) \,/\, dc_m = -f(c_m) < 0$; i.e., the proportion of organisations without prevention is strictly decreasing in c_m. To simplify our notation, we will write the functions $EU_{NP}(x(c_m))$, $EU_P(c_m)$ and $q(x(c_m))$ in the following as functions of c_m. Along with $0 \le q\left(c_m\right) \le \overline{q} < 1$, it follows that

1 at position $c_m = 0$, $\Psi(0) > 0$

2 at position $c_m = \overline{c}$, $\Psi(\overline{c}) < 0$.

This can be interpreted as follows:

1 if nobody invests in protection and therefore the risk of attack is very high, it is worth undertaking protective measures to reduce expected loss when protection is costless, whereas

2 if everybody invests in protection and therefore the risk of attack is zero, then an investment in protection that is extremely costly $(\overline{c})$ is not worth being undertaken to avoid the risk of an attack.

The derivative of $\Psi(\cdot)$ is negative, so $\Psi(c_m)$ is decreasing in c_m. This ensures that there exists an interior solution c^* for which $0 < c^* <. \ \overline{c}$. The competitive Nash equilibrium c^* satisfies

$$\Psi\left(c^*\right) = EU_P\left(c_m\right) - EU_{NP}\left(c_m\right) = 0, \tag{7}$$

which implies

$$c^* = q\left(c^*\right)[\overline{u} - \underline{u}]. \tag{8}$$

Given that private expected benefits of cyber risk protection are a function of the actual probability of an attack, expected benefits are implicitly determined by c^*. Assuming relatively similar expected benefits from cyber risk protection, excess expected utility is positive for $c < c^*$ and negative for $c > c^*$, so that 'low-cost' organisations with $c \le c^*$ invest in protection whereas 'high-cost' organisations with $c > c^*$ do not. Hence, the Nash equilibrium in the community divides all organisations into two groups: those who invest in cyber risk protection and those who do not.

Let the community's overall welfare be represented in utilitarian fashion as the sum of all firms' utilities. We denote the function $S(c_m)$ as the welfare function, i.e., the 'sum' of the individual expected utility levels of all organisations.[3] The overall optimal protection level in the community is the level that maximises welfare. Overall welfare $S(c_m) \ge 0$ is then given by

$$S\left(c_m\right) = \int_{0}^{c_m} EU_P(c) f(c) dc + EU_{NP}\left(c_m\right) \cdot x\left(c_m\right). \tag{9}$$

The first term in (9) denotes the expected utility levels for all organisations who invest in protection and the second the expected utility for all organisations who do not invest in protection. Due to the interdependencies at play, overall welfare is not maximised in the community equilibrium protection level. Given $f(c_m) > 0$, $S(c_m)$ has an interior maximum at c^{**}, so that

$$c^{**} = \arg \max_{c_m} S\left(c_m\right) \tag{10}$$

where c^{**} is the optimal protection level.[4] Now consider marginal welfare, $dS(c_m) / dc_m$, evaluated at the equilibrium c^*. Together with (7) and $dx(c_m) / dc_m = -f(c_m) < 0$ we find that

$$\frac{dS\left(c_m\right)}{dc_m}\Big|_{c_m=c^*} = \underbrace{f(c^*)\left[q(c^*)\Delta u - c^*\right]}_{=0} - x(c^*)\left[q'(c^*)\Delta u\right] > 0, \tag{11}$$

where $\Delta u \equiv [\overline{u} - \underline{u}] > 0.$ Technically, at the (Nash) equilibrium c^*, social welfare is not maximised but has a positive slope. We thus have $c^{**} > c^*$ due to (11). Hence, $x(c^{**}) < x(c^*)$, i.e., the proportion of organisations without protection is higher under the equilibrium than in the welfare optimum. As a result, the risk of cyber attack in the community is *too high* from an overall welfare viewpoint. Due to the risk interdependencies, the equilibrium outcome is inefficient. In our setting, the parties in the cyber network community invest *too little* in cyber risk protection relative to the overall efficient level.

It should be noted that equation (11) is somewhat general since it simply states the suboptimality of the Nash equilibrium when there are positive externalities. In a cyber network, most systems have some form of default protection (for instance, a virus scanner or probably a firewall). Interestingly, even if there was some level of default protection, as long as there are still positive externalities, the equilibrium outcome would be inefficient.

The next section looks at policy implications and discusses what can be done to ameliorate this problem.

3 Policy implications: decision strategies to respond to cyber harassment and the threat of cyber attacks

3.1 Regulation

Given that the risk of cyber attack is ‘too high’ in the community – i.e., the level of cyber risk protection is inefficient – one may think of regulation as a potential tool for enhancing protection. For instance, one may think of making cyber risk protection mandatory for every firm in the community. However, our model clearly shows that this is not a good solution. Making protection mandatory would result in a protection level of $\overline{c}$, associated with welfare

$$S(\overline{c}) = \int_0^{\overline{c}} (\overline{u} - c) f(c) dc. \tag{12}$$

Now consider the difference

$$S(c^*) - S(\overline{c}) = \int_{c^*}^{\overline{c}} \left[c - q(c^*)\Delta u\right] f(c)dc > 0, \tag{13}$$

which is positive because $c - q(c^*)\Delta u > 0$ for all $c^* < c \leq \overline{c}$. As a result, the Nash equilibrium is associated with higher welfare than under a regulated community in which all organisations are required to protect themselves from cyber attacks. This policy is not recommendable. Economically, the rationale is that such a policy will require those organisations with relatively high protection cost to protect themselves even though this protection is associated with very high firm-level costs. Practically, it seems rather difficult to regulate the cyber community in such a way since this would require a control mechanism to ensure that everyone protects themselves.

3.2 Subsidies

Another way to increase the protection level in the community is to subsidise some organisations in such a way that cyber risk protection becomes less costly for them to implement. A relatively minor subsidisation may be sufficient, i.e., it may create the economic incentive for all other organisations to invest in improved protection. This is an instance of the tipping phenomenon first identified by Thomas Schelling: a case in which a behavioural change by a small collection of players causes a massive shift in the overall population behaviour (Schelling, 1978). Heal and Kunreuther (2007) show that in an IDS game, a critical coalition of players may be sufficient to induce such a tipping phenomenon. This implies that a suboptimal Nash equilibrium may be converted to one with full investment in cyber risk protection by persuading only a subset of the players to change their policies. The least expensive way to guarantee full cyber risk protection is then to identify a critical coalition of players which will tip the entire community to full protection.[5] However, determining a critical coalition seems a rather complicated task given the very large number of players involved in a cyber network.

Alternatively, and probably less sophisticated, a tipping phenomenon may also be initiated by subsidising research and development in the cyber risk protection area. This would make cyber risk protection less costly in the future. There are different ways to collect subsidy funds. For instance, funds might be collected through a levy on internet commerce. As a result, subsidising the cyber harassment protection industry seems like a promising way to improve risk allocation in cyber networks in which the risk of cyber harassment plays an important role. [6]

3.3 Managerial decision processes

Managerial decision processes should take into account the interdependent risk structure of the underlying internet-based network. Therefore, a policymaker may consider introducing a reward mechanism to incentivise risk protection. The essential idea is that an organisation that invests in comprehensive cyber risk protection should be rewarded for the benefits it provides for the network (in the form of lower cyber harassment risk). Although it may seem unrealistic that others would provide compensation for such services, the rewards offered do not need to be monetary in nature to improve incentives. For instance, there may be an independent party that would present awards to organisations for using well-functioning anti-cyber harassment strategies. These awards could function as a signalling device. A certified organisation may then cite such awards or certificates on its website to signal its security efforts to its customers and other users. This would make the award in question valuable to the organisation. As a result, using awards as coordinative mechanisms – for instance, using non-monetary web certificates in this way – may actually be a cost-effective and promising way to promote protection efficiency within the cyber network.

3.4 Jurisdiction/implementation of laws

International borders do not exist for computer networks. Therefore it is important that states enact and implement laws and other measures in order to prevent cyber attacks and to protect organisations. In addition, all countries should coordinate their actions in order to investigate and prevent cyber attacks [G8 Recommendations on Transnational Crime (2002), see report in Part IV, Section D].

3.5 Need for intense international cooperation and collaboration

Prior research focuses on methods that can be used to decrease the risk of cyber attacks such as tracking and tracing techniques. According to Lipson (2002), some techniques overcome privacy concerns which are associated with the logs of internet traffic in a satisfactory manner. In order to establish and build these tracking and tracing techniques and make them effective, hardware enhancement and a substantial amount of technical skills are essential. Thus, providing firms with internet businesses with technical and financial assistance can be valuable (Lipson, 2002).

As cyber attacks can be perpetrated without physical and national boundaries, tracing and tracking techniques require international agreements and cooperation (Lipson, 2002). These agreements should complement the technical ability to trace and track attackers across administrative, jurisdictional and national boundaries [Lipson, (2002), p.52]. An international agreement involving cooperation and collaboration in establishing and supporting such techniques may be of high value to the internet community. International cooperation at a technical level should be intensified. The hacker community continuously shares and exchanges vulnerable information. If defenders do not share technical information and resources, such as for example software tools to support tracking etc., too, they will be outmatched (Lipson, 2002).

International efforts on how to deal with cyber crime have already been started. For example, the G8 Recommendations on Transnational Crime (2002) report in Part IV, Section D, on High-tech and computer-related crimes, which encourages states to work towards domestic and international solutions. The latter includes international agreements and cooperation to address cyber crime. “States should maintain an appropriate balance between protecting the right to privacy, particularly given the threat of new technologies, and maintaining law enforcement’s capacities to protect public safety and other social values” [G8 Recommendations on Transnational Crime (2002), Part IV, Section D].

3.6 Internet best practices

The development of international minimum protection standards including tracking and tracing technologies is essential in order to improve cyber safety. Besides international cooperation, best practices that firms and providers are expected to fulfil may also help evading attempts of cyber attack and thereby protecting attack victims. This approach may establish some level of 'due care' [Lipson, (2002), p.31] which, in turn, can help to improve efficiency. In practice, this approach seems very important given its relatively low cost and high potential to improve cyber risk protection levels in the community.

4 Concluding remarks

Many organisations are facing an extremely complex information security environment. Information security has become a highly relevant topic for most organisations that need to secure their confidential and specific data against different forms of potential cyber attacks. When interconnected systems are subject to attacks by contagious threats, investments in protection measures implicitly benefit others because one party's investment decision will have an impact on the utility of the other parties connected to it. An important feature of the problem is that it spreads via an underlying network; i.e., the vulnerability of one party to cyber harassment attacks depends on its interactions with other parties in the community. These interactions play a prominent role in the management of cyber harassment risk. Due to these interdependencies, the equilibrium protection outcome in the community will generally be inefficient. In our setting, the parties in the cyber network community invest *too little* in cyber risk protection relative to the socially efficient level.

This inefficient situation may be improved using various mechanisms. While regulation is not recommendable, one promising idea would be to make cyber risk protection less costly by subsidising high-exposure organisations. This seems a rather efficient way given that only a relatively small number of organisations would need to be better protected in order to initiate a tipping phenomenon towards a (more) efficient overall protection level.

Additionally, award mechanisms for protective behaviour may be worth using. A certified independent organisation may offer awards or certificates to organisations that they can then use to signal their security efforts to other users, competitors, and customers. Using awards as coordinative mechanisms also seems as though it may be fruitful in promoting protection efficiency in the internet community.

Another potentially helpful tool may be to enact and implement laws and other measures in order to prevent cyber attacks and to protect organisations. Furthermore, all countries should coordinate their actions in order to investigate and prevent cyber attacks as stated in the G8 Recommendations on Transnational Crime (2002). Implementing such laws may ensure some minimum protection standards within an interdependent risk network.

Cyber risk has no physical and national boundaries. Therefore, tracking and tracing techniques are important and require international cooperation. The development of international standards for tracking and tracing technologies is essential in order to improve cyber safety.

Finally, formal contractual agreements between different parties specifying their data and information exchange and other interactions may also prove a promising strategy for decreasing the inefficiency of protection in the network. Such agreements may serve to commit the parties to their cyber risk protection strategy.

References

Adomi, E. and Igun, St. (2008) 'Combating cyber crime in Nigeria', *The Electronic Library*, Vol. 26, No. 5, pp.716–725.

Anderson, R. (2001) 'Why information security is hard – an economic perspective', *Proceedings of 17th Annual Computer Security Applications Conference (ACSAC)*, 10–14 December, New Orleans, La.

Bentham, J. (1970) *An Introduction to the Principles of Morals and Legislation*, Burns and Hart, London.

Blakley, B., McDermott, E. and Geer, D. Jr. (2001) 'Information security is information risk management'. *Proceedings of the 2001 Workshop on New Security Paradigms*, pp.97–104.

Buzzard, K. (1999) *Computer Security – What Should You Spend Your Money on Computer Security*, Vol. 18, No. 4, pp.322–334.

Ellison, L. and Akdeniz, Y. (1998) 'Cyber-stalking: the regulation of harassment on the internet', *Criminal Law Review*, pp.29–48, December Special ed., Crime, Criminal Justice and the Internet.

Espelage, D.L. and Swearer, S.M. (2003) 'Research on school bullying and victimization: what have we learned and where do we go from here?' *School Psychology Review*, Vol. 32, No. 3, pp.365–383.

Finne, Th. (2000) 'Information systems risk management: key concepts and business processes', *Computers and Security*, Vol. 19, pp.234–242.

G8 Recommendations on Transnational Crime (2002) available at http://www.icclr.law.ubc.ca/.../G8%20Recommendations%20on%20Transnational%20Crime%202002.doc (accessed on 27 March 2011).

Garg, A., Curtis, J. and Halper, H. (2003) 'Quantifying the financial impact of IT security breaches', *Information Management and Computer Security*, Vol. 11, No. 2, pp.74–83.

Gordon, L. and Loeb, M. (2002) 'The economics of information security investment', *ACM Transactions on Information ans System Security*, Vol. 5, No. 4, pp.438–457.

Heal, G. and Kunreuther, H. (2004) *Interdependent Security: A General Model*, August, NBER Working Paper No. W10706, available at SSRN: http://ssrn.com/abstract=583704.

Heal, G. and Kunreuther, H. (2006) *Supermodularity and Tipping*, June, NBER Working Paper No. 12281.

Heal, G. and Kunreuther, H. (2007) 'Modeling interdependent risks', *Risk Analysis*, Vol. 27, No. 3, pp.621–634.

Hoo, K. (2000) *How Much is Enough? A Risk-Management Approach to Computer Security*, June, Consortium for Research on Information Security Policy (CRISP) Working Paper, Stanford University, Stanford, Calif.

Internet World Stats (2010) 'Internet usage statistics. The internet big picture', *World Internet Users and Population Stats.*, available at http://www.internetworldstats.com/stats.htm (accessed on 07 October 2010).

Kakade, S., Kearns, L., Ortiz, R., Pemantle, R. and Suri, S. (2005) 'Economic properties of social networks', in Saul, L., Weiss, Y. and Bottou, L. (Eds.): *Advances in Neural Information Processing*, p.17, MIT Press, Cambridge, Mass.

Kearns, M. (2005) 'Economics, computer science, and policy', *Issues in Science and Technology*, Vol. 21, pp.37–47.

Kotulic, A. and Clark, G. (2004) 'Why there aren't more information security research studies', *Information and Management*, Vol. 41, pp.597–607.

Kumar, V., Telang, R. and Mukhopahhyay, T. (2007) 'Optimally securing interconnected information systems and assets', *Proceedings of the Sixth Workshop on the Economics of Information Security*, 7–8 June, Carnegie Mellon University.

Kunreuther, H. and Heal, G. (2003) 'Interdependent security', *Journal of Risk and Uncertainty*, Vol. 26, pp.231–249.

Lipson, H. (2002) *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, CERT Coordination Center, Software Engineering Institute: Pittsburgh.

McGavran, W. (2009) 'Intended consequences: regulating cyber attacks', *Tul. J. Tech & Intell. Prop.*, Vol. 12, pp.259–275.

Meadows, C. (2001) 'A cost-based framework for analysis of denial of service in networks', *Journal of Computer Security*, Vol. 9, pp.143–164.

Pigou, A. (1920) *The Economics of Welfare*, Macmillan and Co., London.

Schelling, T. (1978) *Micromotives and Macrobehavior*, W.W. Norton and Firm, New York.

Notes

[1] Note that this cost formulation is quantitative and implicitly includes all potential cost measures. It implicitly assumes that any other qualitative cost - for instance, the loss of privacy - can be expressed in a quantitative way.

[2] Without loss of generality, we assume that a firm invests in prevention when it is indifferent between investing and not investing.

[3] Utilitarianism goes back to the English philosopher Bentham. For a discussion of welfare and its definition, see Bentham (1970, p.12).

[4] Note that social welfare at c^{**} is indeed maximised because $dS(c_m) / dc_m$ is positive at $c_m = 0$ and negative at $c_m = \overline{c}$.

[5] For a mathematical demonstration and full proofs, the reader is referred to Heal and Kunreuther (2007) as well as Heal and Kunreuther (2006).

[6] Technically, this policy adjusts the cost distribution $f(c)$ to the left in such a way that every firm enjoys a lower cost of protecting itself from a cyber attack.