2009

Cyberattacks: Does Physical Boundry Matter?

Qiu-Hong Wang
Huazhong University of Science and Technology, qhwang@mail.hust.edu.cn

Seung Hyun Kim
National University of Singapore, disksh@nus.edu.sg

CYBER ATTACKS: DOES PHYSICAL BOUNDARY MATTER?

Completed Research Paper

Qiu-Hong Wang
School of Management
Huazhong University of Science & Technology
qhwang@mail.hust.edu.cn

Seung Hyun Kim
Department of Information Systems
National University of Singapore
disksh@nus.edu.sg

Abstract

Information security issues are characterized with interdependence. Particularly, cyber criminals can easily cross national boundaries and exploit jurisdictional limitations between countries. Thus, whether cyber attacks are spatially autocorrelated is a strategic issue for government authorities and a tactic issue for insurance companies. Through an empirical study of cyber attacks across 62 countries during the period 2003-2007, we find little evidence on the spatial autocorrelation of cyber attacks at any week. However, after considering economic opportunity, IT infrastructure, international collaboration in enforcement and conventional crimes, we find strong evidence that cyber attacks were indeed spatially autocorrelated as they moved over time. The policy and managerial implication is that physical boundary should be an important factor in addressing strategic cyber attacks and their potential risks.

Keywords: Information Security, cyber attacks, interdependence, physical boundary

Introduction

Information security issues are characterized with interdependence of risks. First, millions of thousands of computers and network systems are connected to the Internet while few software vendors are dominant in IT markets. Thus, one kind of vulnerability or risk in any particular system can easily spread to the whole network via physical linkage or be found in other systems using the same software platform. Second, IT has enabled in-depth-and-breadth collaboration across organizational or country boundaries. Hence the security of any particular user is often dependent on the effort of other users in the same value chain (Kunreuther and Heal 2003; Varian 2004). Third, information and communication technology has facilitated information security violators to attack across national boundaries. While conventional criminals tend to be localized, cyber criminals can easily cross national boundaries and exploit jurisdictional limitations between countries (Kshetri 2006).

The interdependent nature of information security has important implications for public policies and business strategies. Government can directly address information security through enforcement against attackers. In an empirical study about the impact of information security enforcement on cyber attacks, Png et. al (2008) find insignificant deterrent effect of domestic enforcement on cyber attacks. However, they find compelling evidence of a displacement effect: U.S. enforcement substantially increases attacks originating from other countries. Understanding the nature of country-level interdependence can guide governments to identify its counterparts to collaborate with and to effectively reduce the volume of attacks. Organizations manage information security risk through elimination, mitigation absorbance and transference (Böhme and Kataria 2006). In a review of the evolution of cyber-insurance, Majuca et al. (2006) propose cyber-insurance as a powerful strategy for firms to transfer the residual information security risk. However, given the rampantly growing market for malicious online activities (Symantec 2008), the cyber-insurance market is both underdeveloped and underutilized due to the interdependent risks (Böhme and Kataria 2006). As discussed by Anderson and Moore (2008), "Interdependence can make some cyber-risks unattractive to insurers – particularly those risks that are globally rather than locally correlated".

The importance of interdependence in information security has attracted academia interests. The existing analytical work focus on user's incentives in network systems (Kunreuther and Heal 2003; Varian 2004) and the empirical work focus on modeling risk arrival process and estimation of correlations within and between firms via simulation and honeypot experiments (Böhme and Kataria 2006). To our best knowledge, no study has examined the fundamental issue that whether and how cyber attacks are correlated at the country level. A better understanding of the nature of interdependence at the country level would be the first step towards international collaboration and advanced cyber-insurance.

In this paper, we study the above issues using a sample of attacks originating from 62 countries over the period between January 2003 and December 2007. We first employ spatial autocorrelation (Moran 1950) into the static analysis of cyber attacks across countries. Further, we develop a two-stage model to enable a panel data analysis of the interdependence of cyber attacks movement between countries. Specifically, we model country-level cyber attacks through worldwide-systematic risk and non-worldwide risk. We further divide the non-worldwide risk into country-specific risk and country-to-country interdependent risk. For any pair of countries, their interdependence in cyber attacks is measured by the correlation of the residuals that cannot be explained by worldwide systematic risk and country-independent risk during the period of year t. Although in this study, we are most interested in examining whether and to what extent physical boundaries contribute to cyber attack interdependence, we control for any other possible impacts following the interdependence theory in the literature of international economics. While interdependence theory links country conflicts to countries' relative status in democracy, economic growth, alliance, political change, and trade interdependence, etc. (Oneal and Russett 1997), we explain the country-to-country interdependence in cyber attacks through countries' relative status in aspects that may affect attackers' economic incentives. Those aspects are captured from the dimensions of economy, technology, industry, international cooperation in enforcement and criminal culture. In particular, we measure the international cooperation in enforcement by the status of a country in joining the EU Convention on Cybercrimes.

The Council of Europe, along with the U.S., Canada and Japan signed the Convention on Cybercrimes, Europe Treaty Series No. 185, the first International treaty for crimes performed through Internet and other computer networks, on 23 November 2001. One of the main purposes of the convention is for "setting up a fast and effective

regime of international co-operation".[1] By the end of 2007, 39 EU countries and 4 non-EU countries have signed the convention and 21 countries out of them have further ratified and enacted it. Hence, the status of a country in joining the EU Convention on Cybercrimes can be considered as an important measure of international cooperation in enforcement against cyber attacks.

Our empirical findings are reported as following. Firstly, the static analysis shows that cyber attacks in general were not spatially autocorrelated at any week, with an average autocorrelation as low as 0.022. However, in the two-stage panel data analysis, the physical distance between countries has significantly negative effect on the interdependence of cyber attacks between countries, and the interdependence was relatively higher for continentally neighbored countries. These findings suggest that although, in the short term, no-discrimination cyber attacks including worms and viruses may randomly spread over the Internet, in the long term, attackers do discriminate targets with different physical locations. Further we find that the impact of physical distance on the interdependence is lower for any pair of countries with different status in joining the EU Convention on Cybercrimes. This evidences the belief that cyber attacks may strategically migrate to distant countries to exploit jurisdictional limitations between countries. The implication is that the jurisdictional boundaries could reduce the spatial autocorrelation in cyber attacks.

The remainder of the paper is structured as follows. Section 2 briefly reviews the relevant literature in the economics of information security. Section 3 presents our model and methodology. Section 4 introduces the data. Section 5 presents the empirical results. In the last section, we discuss the policy implications to public authorities, cyber insurance companies and organization users and the future research direction.

Literature Review

Poor security incurs economic losses to firms. For example, several studies have examined the impact of information security breaches on the market value of companies (Campbell et al. 2003; Cavusoglu et al. 2004; Kannan and Telang 2005). Telang and Wattal (2007) have studied the impact of vulnerability disclosure on the software vendors' stock prices. Perceiving the economic costs, one of the important questions is how to reduce the security risks. Png et al. (2008) study the deterrent and displacement effect of enforcement on the number of cyber attacks. August and Tunca (2006) compare the effectiveness of different policies on software patching under negative network externalities. Cavusoglu et al. (2005) have found the deterrent effect of intrusion detection systems. Nizovtsev and Thursby (2007) study the conditions where full disclosure of vulnerabilities enhances social welfare by considering the interactions among white hat users, black hat users, and a vendor. Anderson et al. (2008) emphasize the importance of an appropriate regulatory framework and make policy recommendations to tackle information and network security. For example, they recommend, "the European Commission put immediate pressure on the 15 EU Member States that have yet to ratify the Council of Europe Convention on Cybercrime." These studies show that the security policies play a critical role in managing the security issues and the policies should consider the economic incentives of involved parties. Another important implication in the literature is that the interdependent nature of cyber attacks and risks poses a major challenge to policy makers (Kunreuther and Heal 2003; Varian 2004). The interdependence has important implications for development of cyber insurance as well. When risks are interdependent, one entity's decision to invest in cyber insurance influences the risks carried by other entities (Bolot and Lelarge 2008). The highest level of interdependence is at the country level (Böhme and Kataria 2006). The discussion of the literature naturally leads to the research question that we aim to study in the paper: what government policies will help address the cyber risks and interdependence at the country level.

Model and Methodology

We first employ spatial autocorrelation into the static analysis of cyber attacks across countries. Moran's I (Moran 1950) is a commonly adopted measure of spatial autocorrelation to detect departures of the same phenomenon from spatial randomness. Moran's I requires a matrix of spatial weights and is calculated as

$$I = \left[N / \sum_i \sum_j w_{ij} \right] \cdot \sum_i^N \sum_j^N w_{ij} \left(x_i - \bar{x}\right)\left(x_j - \bar{x}\right) \Big/ \sum_i^N \left(x_i - \bar{x}\right)^2$$

[1] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

where w_{ij} is the weight between i and j, $\bar{x}$ is the sample mean, and N is the number of spatial units. Thus, positive (negative) value means positive (negative) spatial autocorrelation. The Moran's I can also calculate Z score to test for statistical significance of spatial autocorrelation. When the Z score indicates any statistical significance, the Moran's I value near 1.0 indicates positive clustering. The Moran's I value near zero with statistical significance indicates dispersion. By generating the spatial weights matrix based on the longitudes and latitudes of the 62 countries, we are able to compute Moran's I, the global spatial autocorrelation statistics for cyber attacks at any given time.

However, this approach would not give us a longitudinal view of the spatial autocorrelation of cyber attacks. Therefore, we further use a two-stage model to measure and characterize the cross-country interdependence of cyber attacks. We are particularly interested in examining the effect, if any, of physical distance and country boundary on the interdependence, and how it may be affected by other factors.

We divide overall cyber attacks into worldwide systematic effects and non-worldwide effects. The worldwide systematic effect refers to the risk associated with aggregate worldwide cyber attacks to which every country is vulnerable. The non-worldwide effect implies the risk associated with the cyber attacks to which only a subset of countries is vulnerable. There are three important reasons to support the existence of worldwide systematic attacks. First, some cyber attacks such as worms may spread to any randomly chosen hosts over the network that is not constrained by country borders. Second, the worldwide effects can be caused by the disclosure and exploit of any vulnerability in a standard software platform or the evolution of knowledge base in attacker community. Third, strategic attackers choose any source of attacks to reduce the detection probability and increase the chance of success as well. To the contrary, some attacks may not be associated with the aggregate level risk that should be the function of characteristics pertaining to specific country. For instance, more attacks may originate from a particular country as its Internet user base is large. Some hackers may systematically choose a particular country as a source of bot net attacks as they are more familiar to the country.

Since the cyber space is digitalized and the network systems of every country are closely linked with each other via the Internet, the transportation cost in cyber space is almost negligible, which increases the inherent interdependence between countries. On the other hand, some risks may be very unique to a particular country and do not contribute to the risks faced by other countries. Based on the reasoning, we further divide the non-worldwide effect into country-specific effect and country-to-country interdependent effect.

In the literature on the economic analysis of crime in general, potential criminals weigh the benefits and cost of crime (Becker 1968; Freeman 1999; Polinsky and Shavell 2000). Following Png et al. (2008), we consider the country-specific effect as those that affect attackers' economic incentives (i.e., opportunity cost, expected risk, and potential benefit), but is independent of other countries. While they include domestic enforcement event to measure the attackers' expected risk, we replace it with the indicator about the status of a country in joining the EU Convention on Cybercrimes. With dedicated principles related to international co-operation including extradition and mutual assistance, the EU Convention on Cybercrimes may deter attackers who are not constrained by physical boundaries. We further include control variables related to IT industry infrastructure and conventional crimes.

For any pair of countries, their interdependence in cyber attacks is measured by the correlation of the residuals during the period of year t that cannot be explained by worldwide systematic effects and country-specific effects. Following the literature in the independence theory where relationships between countries are used to explain the country conflicts (Oneal and Russett 1997), we explain the country-to-country interdependence in cyber attacks by the geographical distance and the non-geographical distance between a pair of countries. The geographical distance is measured by physical distance between countries and whether countries share some continental boundary. The non-geographical distance refers to the relative status between countries from the perspectives that are identified in country-specific effects. Figure 1 presents our cyber-attack interdependence model. In the next section, we will discuss the measurements for each factor listed in Figure 1.

INSERT FIGURE 1 ABOUT HERE

In the first stage of the regression, the dependent variable is the ratio of the number of attacks originating in country i in week w over the total number of attacks from all countries, denoted by r_{iw}. By using the ratio rather than absolute volume, we can filter out fluctuation in cyber attacks resulted from worldwide-systematic effects. We regress the ratio of attacks per country per week on the country-specific independent variables C_{iw}, year dummy

variables, Y_t and a set of country dummy variables, N_i. By equation (1), we derive the residual $\hat{e}_{iw}$, which captures the observable and unobservable country-specific time-variant characteristics and international time-variant characteristics that are shared among a few countries.

$$r_{iw} = \alpha + Y_t + \gamma C_{iw} + N_i + e_{iw} \quad (1)$$

Worldwide-systematic effects | Non-worldwide effects

Note that *c* and Y_t together capture the worldwide systematic effects while the rest captures the non-worldwide effects. In the second stage, we first calculate the interdependence between any country pair (*i*,*j*) in year *t* as the correlation of their residuals within the period,

$$r_t^{ij} = corr(\{\hat{e}_t^{i1},...,\hat{e}_t^{is}\}, \{\hat{e}_t^{j1},...,\hat{e}_t^{js}\}), \quad (2)$$

where *1*, …, *s* are the sequence of weeks in year *t*. Then we regress the interdependence between any country pair (*i*,*j*) in year *t* on the geographical distance variables, G^{ij}, non-geographical variables, D_t^{ij}, and year dummies Y_t. Since G^{ij} variables do not vary with time, we use the random effect model. The equation for the second stage is

$$r_t^{ij} = \alpha' + \beta' G^{ij} + \gamma' D_t^{ij} + Y_t + \varepsilon_t^{ij}. \quad (3)$$

Data

The SANS Institute established the Internet Storm Center (ISC) in 2001 to assist Internet Service Providers and end-users to defend against malicious attacks through the Internet. The ISC follows the data collection, analysis, and warning system used in weather forecasting. The ISC draws millions of intrusion detection samples from many diverse locations to provide an accurate representation of Internet activity every day. This information is compiled in the DShield database. Previous study like Png et al. (2008) that uses the same datasets may be biased due to the limitation of ISC statistics: they only identify the originating country of the attacking packets by IP address although the originating computers may be under the remote control of attackers located in other countries. This is not a critical problem in our study because our model takes into account the number of attacks as a result of the interdependence between countries. For instance, if some attacks originating from country i are actually caused by attacks originating country j, they cannot be explained in the first stage regression by the worldwide-systematic effects or country-specific effects, and thus be captured by residual factor $\hat{e}_{iw}$. Further, if this interdependence between country i and country j is not accidental but strategic, we would see a correlation r_t^{ij} in the time series of $\hat{e}_{iw}$ which can be explained in the second stage regression.

Our ISC country-level reports include the daily number of attacks for more than 200 countries from January 2003 onward.[2] We cut off our data collection on December 31, 2007. The sample period comprises 60 months or about 1826 days. However, for unknown reasons, ISC did not report attacks for some periods. Thus, the actual number of observations in our dataset ranges between 1,050 and 1,402 days per country. We focus on 62 countries with the number of internet users over 500,000 as the frequencies of detected attacks from the rest of the countries are low. To avoid the bias caused by time difference among countries, we aggregate the data at weekly basis.

Table 1 lists the measurements for each factor presented in Figure 1. We collected the country level data from the GMID (Global Market Information Database) and the WDI (World Development Indicators) provided by the World

[2] The country-level number of reports published by ISC was defined as the average number of packets reported from each IP address in the respective country.

Bank. Table 2 shows the status and date for each country who have signed the EU Convention on Cybercrimes. Table 3 provides the descriptive statistics of the dependent and independent variables in addition to their sources.

INSERT TABLE 1 ABOUT HERE

INSERT TABLE 2 ABOUT HERE

INSERT TABLE 3 ABOUT HERE

Empirical Results

As a preliminary analysis, we first computed the Moran-I spatial autocorrelation for the number of weekly attacks among the 62 countries during the period from 2003 to 2007. A far-from-zero Moran-I statistics indicates a high spatial autocorrelation (either positive or negative) in cyber attacks among countries. As shown in Figure 2, the spatial autocorrelation ranges from 0.0063 to 0.0375 and does not exhibit any time trend during years 2003~2007. We next replaced the number of weekly attacks originating from each country with the ratio of weekly attacks over the total number of attacks within the 62 countries. The spatial autocorrelations are a bit higher but still at the low level between 0.019 and 0.123. Considering that countries differ in their Internet user base, we further computed the spatial autocorrelation of the weekly number of attacks per Internet user, as shown in Figure 2. However, the change of the measurement on cyber attacks does not affect the observation that cyber attacks were not spatially autocorrelated at any week of our studied period. In other words, statically, neighboring countries do not exhibit similar scale of cyber attacks no matter what measures of cyber attacks are used at least on a weekly basis.

To conduct a panel data analysis on spatial autocorrelation of cyber attacks, we followed the cyber attack interdependence model as presented in Figure 1. We conducted two-stage regressions to estimate equation (1) and (3). The results of the stage 1 using a fixed effects regression are reported in Table 4, column (a). The panel data exhibited high serial correlation, significant heteroskedasticity ($\chi^2(62)= 36549$), and cross-sectional interdependence (Pesaran's test = 28.6). The residuals, with cross-sectional heteroskedasticity and interdependence, were used in stage 2 to calculate the yearly-based country-pairwise interdependence. However, to ensure consistency and efficiency of the coefficients, we further employed linear regression with panel-corrected standard errors that assumes panel-specific AR1 (First-order autoregession) autocorrelation structure and cross-sectional heteroskedasticity and interdependence (Freeman 1999, Donald & Lang 2007). The results are reported in Table 4, column (b).

INSERT TABLE 4 ABOUT HERE

Although not the focus of this paper, the estimates for several coefficients are notable. As expected, the coefficient of GDP per capita is positive and significant. Since the number of hosts reporting to ISC is proportional to a country's Internet scale, the Internet access variable is supposed to adjust the possible sample bias. The coefficient for internet access, however, is significantly negative, which suggests that a larger Internet user base is not necessarily associated with more sources of attacks. For other control variables, the import ratio of computer, communication and other service, and the offences, both have negative and significant coefficients. Most interestingly, the coefficient of the indicator of signature for the EU Convention on Cybercrimes is negative and significant[3]. This suggests strong international cooperation in enforcement against cyber attacks may deter attacks originating from the specific country.

We further included more variables to control for other possible country-specific independent effects (e.g., Internet monthly subscription price, the number of Internet secure servers located in the country, and the unemployment rate with tertiary education). However, the data on these variables are missing for some countries (e.g., China, the United States, etc). Thus, we had only half of the total observations. Table 4, column (c) reports the results with other control variables available to us. The coefficient of the EU Convention on cyber-crime indicator is still negative and significant. The coefficients of the three additional variables had the expected signs. Particularly, the unemployment rate with tertiary education is positively associated with the number of cyber attacks originating from the country. While previous study using general unemployment rate did not show any significantly positive impact of

[3] The coefficients of the indicators for ratification or entry-into-force of the convention are not significant due to the highly correlation between them and the smaller number of observations.

unemployment on cyber attacks (Png et al. 2008), here we find that unemployment rate for tertiary education may be a more accurate measure of the potential workforce for cyber attacks.

Based on the first stage results and referring to equation (2), we calculated the country-pairwise correlations per country pair per year to measure the interdependence between countries. This generated another panel data with 7725 observations. Among them, 4649 observations have positive correlation in the time series of residuals between countries. Hence we first excluded observations with negative interdependence in the following estimation[4]. We regressed the residual correlation between countries on geographical and non-geographical distance variables via a random effect model with adjustment of standard errors. Table 5, column (a) reports the results from the second stage regression. The coefficients of geographical variables are both significant and indicate that cyber attacks originating from countries closer (β = -0.00000302, $p < 0.01$) and even neighboring (β = 0.05118, $p < 0.01$) with each other are more highly correlated in terms of longitudinal movement. To interpret the coefficients, one kilometer increase in distance between a pair of countries is associated with a decrease in country-to-country correlation as much as 0.000003. The effect appears to be quite small as the unit is in kilometer. An increase of 10,000 km in distance, which is almost the distance between Washington D.C. and Tokyo, Japan, would reduce correlation by 0.03. The effect of neighboring is more substantial and is associated with increased interdependence as much as 0.05 in correlation. The coefficient of the distance in Internet access is negative and significant (β = -0.0001870, $p < 0.01$). Therefore, similar countries in terms of the Internet access tend to be more interdependent to each other. The coefficient of the distance in the ratio of computer, communication and other service import is negative and significant (β = -0.001929, $p < 0.01$). The coefficient of the distance in international collaboration in enforcement as measured by status of signature is negative and significant (β = -0.0006458, $p < 0.01$). Overall, the estimation results indicate a good match of our proposed model to cyber attack interdependence and provide strong evidences of the interdependence due to the inherent relationship between countries. Among the independent variables, continental adjacency is found to be one of the most influential drivers of country level interdependence. In addition, similar states in terms of geography, Internet access, IT service import, and international collaboration tend to fortify interdependence between two countries.

INSERT TABLE 5 ABOUT HERE

In the next specification, we include the interaction effects between non-geographical distance variables and physical distance. In the interaction terms, we center each non-geographical distance variable by its mean. Thus the coefficient of any non-geographical distance variables has absorbed the moderating effect from the physical distance. We exclude the convention indicator about ratification because it is highly correlated with the indicator about entry-into-force. Table 5, column (b) reports the results with the interaction effects. Generally, including the interaction terms does not change the signs of the coefficients. More interestingly, the coefficient of the interaction term between physical distance and the distance in status of joining convention on security (as measured by signing the convention) is positive and significant. This suggests that the negative impact of physical distance on the interdependence is lower (higher) for any pair of countries with different (similar) status in joining the EU Convention on Cybercrimes. An intuitive illustration of this finding is that, attackers, who are physically located in a country that has signed the EU Convention on Cybercrimes, may deliberately relocate their command and control servers for botnet hacking to some distant countries that have not yet signed the convention. By this means, they may evade from legal prosecution. The outcome of this strategic behavior from attackers is that the correlation between the two countries in terms of the cyber attack movement in longitudinal settings may not match with their correlation in physical locations. It further suggests that the jurisdictional boundaries could reduce the spatial autocorrelation in cyber attacks.

As a robust check, we repeat the above regressions in the whole samples with 7725 observation. The results, as reported in Table 5, columns (c) and (d), are almost the same, except that the coefficient of the indicator of neighboring countries is positive but not significant.

Concluding Remarks

Many researchers have emphasized the importance of cross-country collaboration and legislation to address the issue of cross-country interdependence of attacks, but the nature of interdependence of attacks across countries is

[4] As a robust check, we did not find any significant difference by including or excluding the observations with negative interdependence.

little known yet. Little knowledge on the nature of interdependence has limited governments' participation in the high-level efforts. In this study, we focus on better understanding of the interdependence of cyber attacks across countries and how physical boundaries may affect cross-boundary cyber attacks. Our first finding on the role of physical boundary is that cyber attacks are not spatially autocorrelated within the same week. Thus, in the short term, the interdependence among nearby countries is not significantly higher than that among any pair of distantly located countries. The policy implication is that international collaboration to effectively manage the short-term interdependence of cyber attacks should not be constrained by country boundaries.

However, we do find evidence that physical distance and adjacency between countries significantly influence cross-country interdependence of cyber attacks in the longitudinal setting. Based on the findings, we believe that hackers are discriminating their targets in the long term. The most interesting finding is that the degree of discrimination by physical boundaries may be moderated by the level of collaboration between a pair of countries, which is operationalized by joining the EU Convention on Cybercrimes in this paper. That is, little collaboration between distantly located countries tends to increase interdependence between them. It implies that cyber attacks by hackers may strategically migrate to distant countries to exploit jurisdictional limitations between countries.

One interesting extension of our study would be to examine the nature of interdependence across different communication ports. For instance, "the Well Known Ports are assigned by the IANA (Internet Assigned Numbers Authority) and on most systems can only be used by system (or root) processes or by programs executed by privileged users" while "the Registered Ports are listed by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users." As different communications ports are used for different purposes, the interdependence may be better studied at the port level.

Our study has a few limitations. First, we were unable to collect the data on the number of attacks between a pair of two countries. That is, we could not observe the targeted countries of the attacks. If we had the data, we could have directly measured the amount of interdependent attacks between a country pair. Second, some country-specific variables are available only at the yearly level while the attacks are measured at the weekly level in the first stage. Third, since our data only covers 62 countries, bias may be introduced in the dependent variable, in which the ratio of the number of attacks originating in country i in week w over the average weekly attacks from the 62 countries rather than from all the countries in the world. The overall implication of this study is clear. International collaboration does not have to be constrained by physical distances and adjacency to manage the short term interdependence. However, the long term interdependence can be better managed if the physical boundary of countries is taken into account. Despite some limitations, our study is one of the first attempts to examine the country-level interdependence using econometric methods.

Acknowledgements

We are pleased to acknowledge financial support from the U.S. Air Force Asian Office of Aerospace R&D (award FA4869-07-1-4046), the National University of Singapore Academic Research Fund (grant R-313-000-076-112 & R-253-000-067-133), and NUS School of Computing. We thank Ivan Png for helpful advice.

Appendix: Figures and Table

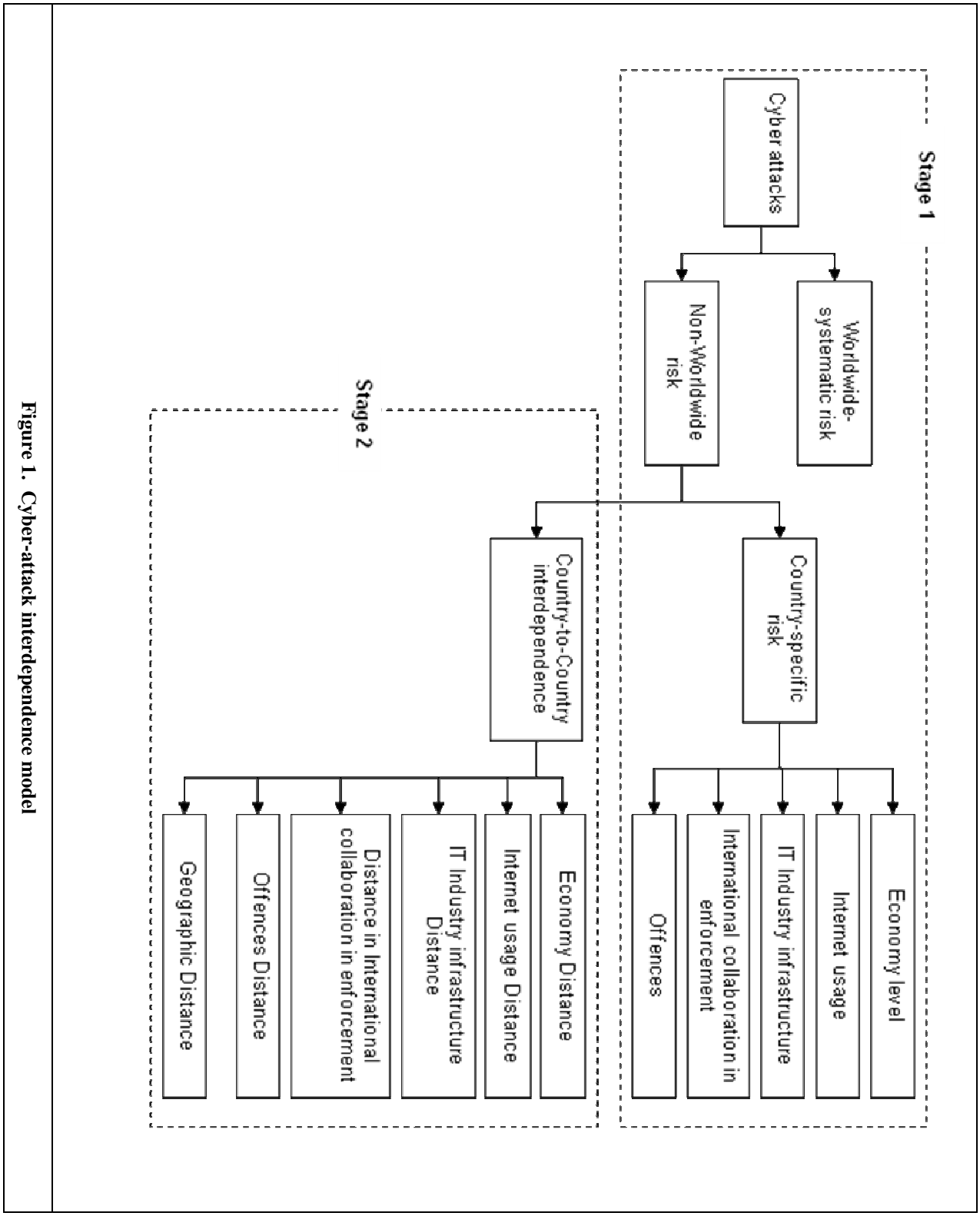

Figure 1. Cyber-attack interdependence model

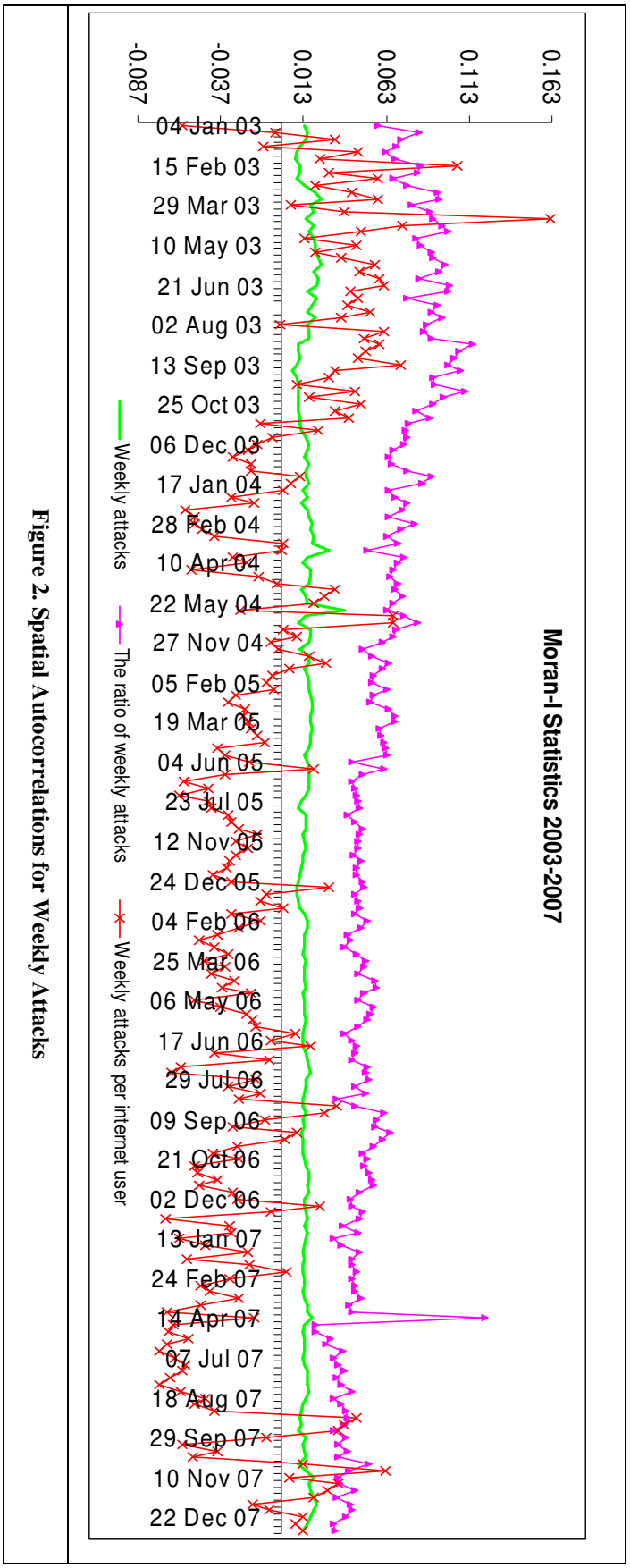

Figure 2. Spatial Autocorrelations for Weekly Attacks

Table 1. Independent variables.

Factors as independent variables	Measurements
Economy level	GDP per capita, GDP_{iw}.
	Unemployment with tertiary education, UMP_{iw}.
Internet usage	Internet user base, $IUSER_i$.[5]
	Price basket for Internet monthly subscription, $IPRICE_{iw}$.
IT Industry infrastructure	Computer, communications and other services (% of commercial service imports), IMP_{iw}.[6]
International collaboration in enforcement	Status with the convention on Cybercrimes: signature(=1), $CONSIGN_{iw}$.
	Status with the convention on Cybercrimes: ratification(=1), $CONRAT_{iw}$.
	Status with the convention on Cybercrimes: entry into force(=1), $CONFOR_{iw}$.
Offences	The number of offences per 100,000 inhabitants, OFS_{iw}.
Economy distance	Maximum(GDP_{iw}/GDP_{jw}, GDP_{jw}/GDP_{iw}), the value is constant within a year.
	Maximum(UMP_{iw}/UMP_{jw}, UMP_{jw}/UMP_{iw}) , the value is constant within a year.
Internet usage distance	Maximum($IUSER_{iw}/IUSER_{jw}$, $IUSER_{jw}/IUSER_{iw}$) , the value is constant within a year.
	Maximum($IPRICE_{iw}/IPRICE_{jw}$, $IPRICE_{jw}/IPRICE_{iw}$) , the value is constant within a year.
IT Industry infrastructure Distance	Maximum(IMP_{iw}/IMP_{jw}, IMP_{jw}/IMP_{iw}) , the value is constant within a year.
Distance in International collaboration in enforcement	Absolute value ($\Sigma CONSIGN_{iw}$- $\Sigma CONSIGN_{jw}$), $\Sigma CONSIGN_{iw}$ is the aggregation within one year.
	Absolute value ($\Sigma CONRAT_{iw}$- $\Sigma CONRAT_{jw}$), $\Sigma CONRAT_{iw}$ is the aggregation within a year.
	Absolute value ($\Sigma CONFOR_{iw}$- $\Sigma CONFOR_{jw}$), $\Sigma CONFOR_{iw}$ is the aggregation within a year.
Offences distance	Maximum(OFS_{iw}/OFS_{jw}, OFS_{jw}/OFS_{iw}) , the value is constant within a year.
Geographic Distance	Distance in kilometers, time-constant value.
	Indicator of neighboring country, time-constant value.

[5] Note that we adopt the Internet user base instead of the Internet penetration rate. The rationale is that the number of nodes in network is an important determinant of cyber attacks originating from a particular country. In addition, the Internet penetration rate is somewhat redundant as it is highly correlated with the economy level.

[6] Another or probably better measurement for IT industry infrastructure is the IT and related products and services produced in the nation. However, the data is not available.

Table 2. Status of countries that have joined the EU convention on Cybercrimes.[7]

States	Signature	Ratification	Entry into force	States	Signature	Ratification	Entry into force
Albania	11/23/2001	6/20/2002	7/1/2004	Hungary	11/23/2001	12/4/2003	7/1/2004
Armenia	11/23/2001	10/12/2006	2/1/2007	Ireland	2/28/2002		
Austria	11/23/2001			Iceland	11/30/2001	1/29/2007	5/1/2007
Azerbaijan	6/30/2008			Italy	11/23/2001	6/5/2008	10/1/2008
Bosnia and Herzegovina	2/9/2005	5/19/2006	9/1/2006	Japan	11/23/2001		
Belgium	11/23/2001			Liechtenstein	11/17/2008		
Bulgaria	11/23/2001	4/7/2005	8/1/2005	Lithuania	6/23/2003	3/18/2004	7/1/2004
Canada	11/23/2001			Luxembourg	1/28/2003		
Switzerland	11/23/2001			Latvia	5/5/2004	2/14/2007	6/1/2007
Montenegro	4/7/2005			Moldova	11/23/2001		
Serbia	4/7/2005			Former Yugoslav Rep. of Macedonia	11/23/2001	9/15/2004	1/1/2005
Cyprus	11/23/2001	1/19/2005	5/1/2005	Malta	1/17/2002		
Czech Republic	2/9/2005			Netherlands	11/23/2001	11/16/2006	3/1/2007
Germany	11/23/2001			Norway	11/23/2001	6/30/2006	10/1/2006
Denmark	4/22/2003	6/21/2005	10/1/2005	Poland	11/23/2001		
Estonia	11/23/2001	5/12/2003	7/1/2004	Portugal	11/23/2001		
Spain	11/23/2001			Romania	11/23/2001	5/12/2004	9/1/2004
Finland	11/23/2001	5/24/2007	9/1/2007	Sweden	11/23/2001		
France	11/23/2001	1/10/2006	5/1/2006	Slovenia	7/24/2002	9/8/2004	1/1/2005
United Kingdom	11/23/2001			Slovakia	2/4/2005	1/8/2008	5/1/2008
Georgia	4/1/2008			Ukraine	11/23/2001	3/10/2006	7/1/2006
Greece	11/23/2001			United States	11/23/2001	9/29/2006	1/1/2007
Croatia	11/23/2001	10/17/2002	7/1/2004	South Africa	11/23/2001		

[7] Source: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

Table 3. Descriptive statistics

Variable	Unit	Source	Mean	Std. Dev.	Min	Max
Attacks in week t for country i	–	Internet Storm Centre	2103702	7468585	9	115000000
GDP per capita	Thousands	GMID	18.56	12.42	1.75	53.08
Internet access	Thousands	GMID	14711.22	30866.12	500	216622.5
Secure Internet servers	per 1 million people	WDI	117.08	190.67	0.14	1060.39
Price basket for Internet	US$ per month	WDI	20.58	10.75	1.81	63.21
EU Convention on security	‘1’as signature	Council of Europe	0.48	0.5	0	1
Computer, communications and other services	(% of commercial service imports	WDI	34.33	12.9	0.75	73
Offences	per 100,000 inhabitants	GMID	3511.04	3209.43	67.9	13997
Unemployment with tertiary education	% of total unemployment	WDI	18.67	12.58	0.2	72.8

Table 4. Systemic interdependence and country-specific effects (both dependent variable and independent variables are in natural logarithm forms except the indicator of convention on information security)

Independent variables	Dependent variable: ratio over the average weekly attacks		
	Fixed effects (d)	OLS: panel-corrected standard error (e)	OLS: panel-corrected standard error (f)
GDP per capita	3.2333*** (0.2455)	3.2333*** (0.2341)	1.9543*** (0.5316)
Internet access	-0.1747*** (0.05677)	-0.1747** (0.07124)	-0.05381 (0.1076)
Ratio of internet security servers	–	–	-0.1648 (0.1357)
Internet price	–	–	-0.1326*** (0.03873)
Convention on security	-0.2242*** (0.08517)	-0.2242*** (0.05504)	-0.3215*** (0.07224)
Ratio of IT service import	-0.4638*** (0.07246)	-0.4638*** (0.06733)	-0.3091*** (0.08948)
Ratio of offences	-1.6216*** (0.1388)	-1.6216*** (0.1348)	-1.9470*** (0.3907)
Unemployed with territory education	–	–	0.9653*** (0.1159)
Year 2004	-0.01844 (0.03203)	-0.01844 (0.02976)	0.1749** (0.07397)
Year 2005	-0.02578 (0.04130)	-0.02578 (0.03519)	0.1876* (0.1057)
Year 2006	-0.2207*** (0.05596)	-0.2207*** (0.04530)	0.1955 (0.1790)
Year 2007	-0.2507*** (0.07251)	-0.2507*** (0.05812)	0.00000000 (0.00000000)
Constant	5.4203*** (1.1733)	0.00000000 (0.00000000)	11.9081*** (4.3830)
No. of Observations	11870	11870	5845
No. of countries	62	62	55

*** p<0.01, ** p<0.05, * p<0.1

Table 5. Country-specific interdependence (Dependent variable: the correlation of residuals by country and year from stage 1)

Independent variables	Dependent variable: the correlation of the residuals between countries per year; the residuals were derived from regression of the ratio over the weekly average attacks in stage 1.			
	Random effects (a)	Including moderating effects (b)	Random effects (c)	Including moderating effects (d)
Physical distance	-0.00000302***	-0.00000690***	-0.00000959*** (0.00000115)	-0.00001171*** (0.00000218)
Neiboring country	0.05118*** (0.01558)	0.04530*** (0.01560)	0.02443 (0.01882)	0.02135 (0.01892)
Distance in GDP per cap	0.0009928 (0.0009908)	0.001532 (0.001033)	-0.003737*** (0.001165)	-0.003977*** (0.001195)
Distance in GDP per cap * Physical distance	–	0.00000136*** (0.00000042)	–	0.00000070 (0.00000050)
Distance in internet access	-0.0001870** (0.00009001)	-0.0001051 (0.0001098)	-0.0003021*** (0.0001010)	-0.0001301 (0.0001350)
Distance in internet access * Physical distance	–	-0.00000005 (0.00000004)	–	-0.00000008* (0.00000004)
Distance in days with signature of convention on security	-0.0006458*** (0.0001254)	-0.0006889*** (0.0001256)	-0.001075*** (0.0001595)	-0.001146*** (0.0001610)
Distance in days with signature of convention on security * Physical distance	–	0.00000010*** (0.00000004)	–	0.00000009* (0.00000005)
Distance in days with ratification of convention on security	-0.0001451 (0.0003316)	–	0.0005348 (0.0004473)	–
Distance in days with entry-into-force of convention on security	-0.0001918 (0.0003652)	-0.0003612** (0.0001819)	-0.0005304 (0.0004868)	0.00003507 (0.0002240)
Distance in days with entry-into-force of convention on security * Physical distance	–	0.00000003 (0.00000005)	–	0.00000011* (0.00000006)
Distance in the ratio of IT service import	-0.001929*** (0.0004439)	-0.002011*** (0.0005194)	-0.0003378 (0.0004555)	-0.0002020 (0.0005703)
Distance in IT service import ratio * Physical distance	–	-0.00000010 (0.00000021)	–	0.00000014 (0.00000021)
Distance in offences	-0.00006509 (0.0002326)	0.00002248 (0.0002669)	-0.0002039 (0.0002750)	0.0003010 (0.0002988)
Distance in offences per 100000 * Physical distance	–	-0.00000019 (0.00000012)	–	-0.00000035*** (0.00000012)
Constant	0.3001*** (0.008449)	0.31679935*** (0.01057507)	0.1777*** (0.01076)	0.1882*** (0.01426)
No. of observations	4649	4649	7725	7725
No. of pairs of countries	1786	1786	1830	1830

*** p<0.01, ** p<0.05, * p<0.1. All models include year fixed effects

References

Anderson, R., R. Böhme, R. Clayton, and T. Moore, "Security Economics and European Policy," Workshop on the Economics of Information Security (WEIS), Dartmouth College, Hanover, NH (USA), June 2008.

Anderson, Ross and Tyler Moore, "Information Security Economics – and Beyond", working paper, Computer Laboratory, University of Cambridge, 2008. http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf.

August, T., T. Tunca. 2006. Network Software Security and User Incentives. *Management Science* 52(11) 1703–1720.

Becker, G., "Crime and punishment: An economic approach." *Journal of Political Economy*,76, 2 (March–April 1968), pp.169–217.

Böhme R. and G. Kataria, "Models and Measures for Correlation in Cyber-Insurance," Workshop on the Economics of Information Security (WEIS), University of Cambridge, UK, June 2006.

Bolot, Jean and Lelarge, Marc. Cyber Insurance as an Incentive for Internet Security. *The Seventh Workshop on the Economics of Information Security*, June 25-28, 2008, Tuck School of Business at Dartmouth College.

Cavusoglu H, Mishra B and S Raghunathan (2004) 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' International Journal of Electronic Commerce, 9(1), 69

Cavusoglu, Huseyin, Birendra Mishra, Srinivasan Raghunathan. 2005. The value of intrusion detection systems in information technology security architecture. Information Systems Research 16(1) 2846

Donald, Stephen G. and Kevin Lang. 2007. "Inference with Difference-in-Differences and Other Panel Data." Review of Economics and Statistics. 89 (2): 221-233.

Freeman, R.B. The economics of crime, Chapter 52, In Orley Ashenfelter and David E. Card, (eds.), *Handbook of Labor Economics*, Volume 3C, 1999, Amsterdam, Netherlands: Elsevier, pp.3529-3571.

Freeman, R.B., The economics of crime. In O. Ashenfelter and D.E. Card (eds.), *Handbook of Labor Economics*, volume 3C. Amsterdam: Elsevier, 1999, pp. 3529–3571.

Garderen, Kees Jan Van and Chandra Shah, "Exact interpretation of dummy variables in semilogarithmic equations", *Econometrics Journal*, Vol. 5, No. 1, 2002, 149-159. IANA, http://www.iana.org/assignments/port-numbers, as of March 7, 2009.

Johnson, David W. and Roger Johnson, "New developments in social interdependence theory, (SOCIAL INTERDEPENDENCE THEORY)", *Genetic, Social, and General Psychology Monographs*, Heldref Publications, 2005.

Kannan, K., Rees, J., and Sridhar, S., "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *International Journal of Electronic Commerce*, 12(1), 69-91. 2007.

Kennedy, P. E., "Estimation with correctly interpreted dummy variables in semilogarithmic equations", *American Economic Review*, Vol. 71, No. 4 (Sep., 1981), 801.

Kshetri, N., "The simple economics of cybercrimes", *IEEE Security & Privacy*, 4, 1 (January/February 2006), 33-39.

Kunreuther, Howard and Geoffrey Heal, "Interdependent Security", *Journal of Risk and Uncertainty*, Vol. 26 Nos. 2-3, March 2003, 231-249.

Kunreuther, Howard and Geoffrey Heal, "Modeling Interdependent Security", *Risk Analysis*, Vol. 27 No. 3, June 2007, 621-634.

Majuca, R. P., W. Yurcik, and J. P. Kesan. "The evolution of cyberinsurance," *ACM Computing Research Repository (CoRR)*, Technical Report cs.CR/0601020, 2006.

Moran, P.A.P. (1950). Notes on continuous stochastic phenomena. Biometrika 37, 17–23.

Nizovtsev, D. M. Thursby. 2007. To Disclose Or Not? An Analysis of Software User Behavior. *Information Economics and Policy* 19(1) 43-64.

Oneal, John R. and Bruce M. Russett, "The Classical Liberals Were Right: Democracy, Interdependence, and Conflict, 1950-1985", *International Studies Quarterly*, 1997, 41, 267-294.

Png, Ivan P.L., Wang, Chen-Yu, and Wang, Qiu-Hong "The Deterrent and Displacement Effects of Information Security Enforcement: International Evidence," *Journal of Management Information Systems*, 25:2, Fall 2008, 125 - 144.

Polinsky, A.M., and Shavell, S., "The economic theory of public enforcement of law," *Journal of Economic Literature*, 38, 1 (March 2000), pp.45–77.

Sharpe, William F., "Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk", *Journal of Finance*, 1964, 19:3, pp. 425-442.

Symantec, Report on the Underground Economy for July 07–June 08, November 2008.

Telang R., S. Wattal. 2007. " Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis", *IEEE Transactions on software Engineering,* 33(8), 544-557.

Varian, Hal R., "System reliability and free riding", University of California, Berkeley, November 2004.