

Cyber Attacks: Cross-Country Interdependence and Enforcement

Qiu-Hong Wang

Seung-Hyun Kim*

wangqiu@comp.nus.edu.sg

kimsh@comp.nus.edu.sg

May 2009

Abstract

This study empirically characterizes the interdependence in cyber attacks and examines the impact from the first international treaty against cybercrimes (Convention on Cybercrimes: Europe Treaty Series No. 185). With the data covering 62 countries over the period from year 2003 to 2007, we find that, international cooperation in enforcement as measured by the indicator of joining the Convention on Cybercrimes, deterred cyber attacks originating from any particular country by 15.81% ~ 24.77% (in 95% confidence interval). Second, joining the Convention also affected the interdependence in cyber attacks from two angles. First, for any pair of country, closer status in joining or not joining the Convention was associated with less negative or more positive correlation. Second, joining the Convention or joining it earlier was associated with lower correlation between countries over time. We discuss the policy implications from our findings to public authorities, cyber insurance companies and organizational users.

1. Introduction

Information security issues are characterized with interdependence. 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-breath cooperation across organizational or country boundaries. Hence the security of any particular user is not independent but 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:

* Department of Information Systems, National University of Singapore, Tel: +65 6516-1195. 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 Professor Ivan Png for helpful advice.

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. 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 academic 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 measured the interdependence of cyber attacks across real entity (i.e., country in our paper) boundaries, nor attributed the interdependence into entities’ relationships.

Furthermore, the empirical evidence of interdependence in cyber attacks calls for international cooperation in enforcement (Png et al. 2008), whereas, in reality countries are not consistent on this point. The Council of Europe, along with the U.S., Canada and Japan signed the Convention on Cybercrimes, Europe Treaty Series No. 185¹, 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”.² 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. Note that, although the convention has ultimately been embraced by the United States after a long debate, it has not yet entered into force even in several major EU countries (e.g., Germany, the United Kingdom, Belgium, Greece, Ireland, Italy, Sweden, etc.) Anderson et al. (2008) have emphasized that the European Commission must put pressure on the remaining member states to more actively participate in the Convention. Hence, whether the convention is an effective instrument to deter cyber attacks and how it affects the interdependence between countries are subject to empirical investigation.

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. Our empirical strategy models cyber attacks through worldwide-systematic risk and country-specific risk. We further divide country-specific risk into country-independent 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 . 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 with aspects that may affect attackers’ economic incentives. Those aspects are captured from the dimensions of economy,

¹ For brevity, in this paper we use the term “the Convention” to represent this title.

² <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

technology, industry, international cooperation in enforcement and criminal culture. In particular, we measure the international cooperation in enforcement against cybercrimes by two variables: one is the relative status quo in joining the Convention. The other is the common longitudinal status since both countries have joined the Convention.

We find that, firstly, signing the Convention on Cybercrimes deterred attacks from any particular country by 15.81% ~ 24.77% (in 95% confidence interval). Second, joining the Convention also affected the interdependence in cyber attacks from two angles. First, for any pair of country, closer status in joining or not joining the Convention was associated with less negative or more positive correlation. Second, joining the Convention or joining it earlier was associated with lower correlation between countries over time. We discuss the policy implications from our findings to public authorities, cyber insurance companies and organizational users.

The remainder of the paper is structured as follows. Section 2 presents our model and methodology. Section 3 introduces the data. Section 4 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.

2. Model and Methodology

In our empirical analysis, we use a two-stage model to measure and characterize the cross-country interdependence of cyber attacks. We model cyber attacks through worldwide-systematic effects and country-specific effects. This is analogous to the Capital Asset Pricing Model (CAPM) (Sharpe 1964) in finance in which the return on any particular capital asset is determined by the expected return of the market, the sensitivity of the asset returns to market return and the idiosyncratic risk specific to the capital asset. The time series of cyber attacks volume for any particular country and risk-combined return for any particular capital asset share some common features:

First, both entities are a sub-system in a large system consisting of correlated components, thus are influenced by any change in the whole environment. In the financial market, the market-wide effects can be caused by economy growth or downturn, government policies or natural disasters. In cyber attacks, 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.

Second, both types of values depend on participants' distribution of investment. In the financial market, investors choose the proportion of each capital asset in their portfolio to maximize the net return. In cyber attacks, strategic attackers choose the source of attacks to reduce the detection probability and increase the chance of success. Hence, the deviation of both types of values from the system-wide trend is the function of characteristics pertaining to specific entity (country or the capital asset).

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. Hence, we further divide country-specific effects into country-independent factors and country-to-country interdependent factors.

Following Png et al. (2008), we consider the country-independent factors that affect attackers' economic incentives (i.e., opportunity cost, expected risk, and potential benefit). Png et al. (2008) include domestic enforcement events and U.S. enforcement events to measure the


attackers' expected risk. However, they cannot find significant deterrent effect from domestic enforcement but compelling displacement effect from U.S. enforcement. Their finding suggests that international cooperation in enforcement is essential to deter cyber criminals. Therefore, in this study, rather than including domestic enforcement events, we measure the extent of international cooperation by the status of a country in joining the Convention on Cybercrimes. With dedicated principles related to international co-operation including extradition and mutual assistance, the Convention on Cybercrimes may deter attackers who are not constrained by physical boundaries. We further include control variables that measure the importance of ICT service in the economy 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-independent effects. Following the literature in 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 geographical distance and non-geographical distance. The non-geographical distance refers to the relative status between countries from the perspectives that are identified in country-independent effects. Figure 1 presents our cyber-attack interdependence model. In the next section, we discuss the measurements for each factor listed in Figure 1.

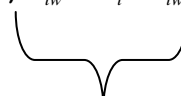
INSERT FIGURE 1 ABOUT HERE

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 62 countries, denoted by r_{iw} . By using the ratio rather than absolute volume, we want to filter fluctuation in cyber attacks resulted from worldwide-systematic effects.³ Since the 62 countries attacks are not the perfect representative of the total attacks all over the world, we would alternatively replace the denominator with the average number of attacks from the 62 countries to reduce the sample bias. 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 country-to-country interdependent effects that cannot be explained by the independent variables in the current stage.

$$r_{iw} = \alpha + Y_t + \gamma C_{iw} + N_i + e_{iw}$$



Worldwide-
systematic effects



Country specific
effects

(1)

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,

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

where $1, \dots, s$ 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

³ We have used the total volume of attacks originating from country i as our dependent variable, but the nature of our results do not change much. However, using the total volume as a dependent variable may result in a more serious endogeneity in the model.

distance variables, D_t^{ij} , and year dummies Y_t . In particular, we measure the international cooperation in enforcement against cybercrimes by two variables: one is the relative status quo in joining the Convention as measured by the difference in the number of weeks for each year over which the countries have been signed the Convention. The other is the common longitudinal status, W_t , as measured by the number of weeks since both countries have signed the Convention. Since G^{ij} variables do not vary with time, we use a random effect model. The equation for the second stage is

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

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 samples from many diverse locations to provide an accurate representation of Internet activity. This information is compiled in the DShield database. The limitation of ISC statistics is that they only identify the originating country of the attacking packets by IP address, even though 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 just takes into account the number of attacks as a result of the interdependence between countries.

Our ISC country-level reports include the daily number of attacks for more than 200 countries from January 2003 onward.⁴ We cut off our data collection on December 31, 2007. The sample period comprised 60 months or about 1826 days. However, for unknown reasons, ISC did not report attacks for some periods. Thus, the actual number of observations was only between 1,050 and 1,402 days per country. The sample comprised 62 countries with the number of internet users over 500,000. 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. In particular, $CONSIGN_{iw}$ equals to 1 if country i signed the Convention in week w , otherwise 0. To measure the status in annual basis, we summed up the value of $CONSIGN_{iw}$ within each year. The higher the sum, the earlier the country joined the Convention. Therefore, the relative status for any pair of countries in year t is measured by the difference of $\sum_t CONSIGN_{iw}$.

INSERT TABLE 1 ABOUT HERE

Table 2 shows the status and date for each country who have signed the Convention on Cybercrimes. Table 3 provides the descriptive statistics of the dependent and independent variables.

INSERT TABLE 2 ABOUT HERE

INSERT TABLE 3 ABOUT HERE

4. Empirical Results

Referring to Figure 1, equations (1) and (3), we empirically address our research questions through two-stage regressions. In the first stage, we work on equation (1) and regress the ratio of the number of weekly attacks on worldwide systematic effects and country-specific independent effects. The purpose is to assess the deterrent impact of joining the Convention on Cybercrimes

⁴ 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.

and further derive the residuals for the next step analysis of the interdependence. Table 4 reports the correlation of the independent variables.

INSERT TABLE 4 ABOUT HERE

As a baseline, we conduct a fixed-effects regression without any adjustment on the standard errors. The residuals are used in stage 2 to calculate the yearly-based country-pairwise interdependence while the explanation of the coefficients is subject to autocorrelation and heteroskedasticity tests. The panel data exhibits high serial correlation, significant heteroskedasticity ($\chi^2 = 36549$) and cross-sectional interdependence (Pesaran's test = 28.6). Thus we employ linear regression with panel-corrected standard errors that assumes panel-specific AR1 (First-order Autoregression) autocorrelation structure and cross-sectional heteroskedasticity and interdependence (Freeman 1999, Donald & Lang 2007). The results are reported in Table 5, column (a). 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. Its coefficient, however, is negative and significant, which suggests that larger Internet user base was not necessarily associated with more source of attacks. Most interestingly, the coefficient of the extent of international cooperation as measured by the status of joining the Convention is negative and significant⁵. With 95% confidence interval, signing the Convention was associated with 16.03% ~24.77% decrease in the number of attacks originating from the country. Considering that the impact of domestic enforcement was very limited (Png et al. 2008), this result shows that international cooperation in enforcement did effectively deter cyber attacks.

For control variables, the ratio of computer, communication and other service over commercial service imports has negative and significant coefficient. We then replace it with the other two variables, the ratio of the same types of service over commercial service exports or the ratio over the total commercial service (incl. imports and exports). The three variables are highly correlated, their coefficients are consistently negative and significant and the coefficients of other variables do not change much. Referring to the definition in WDI (see footnote 5), the ratio of computer, communication and other service over commercial service may be considered as a measurement for the scale of ICT service in economy. This estimation result suggests that countries with larger scale of ICT service in its economy were less likely to be the source of cyber attacks.

Another control variable, the number of offences per 100,000 inhabitants, has negative and significant coefficient. As shown in Table 3, this variable has high and positive correlation with GDP per capita and the indicator of international cooperation in enforcement. Thus the offence level is not an indicator of poverty but a combined result from economy, culture and history. To the best of our knowledge, there has been no study about the possible correlation between cybercrimes and conventional crimes. This finding at least shows that high conventional crime rate was not necessarily associated with high volume of cyber attacks.

INSERT TABLE 5 ABOUT HERE

To check the robustness of our results, we include 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 have only half of the total observations. Table 5, column (b) reports

⁵ 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 smaller number of observations.

the results. The coefficient of the indicator in joining the Convention is still negative and significant and provides even more negative confidence interval, (-33.00% ~ -22.60%). The coefficients of the three additional variables have 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 cannot find significantly positive impact of unemployment on cyber attacks (Png et al. 2008), here we show that unemployment rate for tertiary education may be a more accurate measure of the potential workforce for cyber attacks.

We further conduct a two-way fixed effects regression by incorporating both country-fixed and weekly-fixed effects. The result is reported in Table 5, column (c). The coefficient of the indicator in joining the Convention is similar to the result in column (a), suggesting that signing the Convention was associated with 11.38% ~25.22% decrease in the number of attacks originating from the country.

To reduce the possible sample bias as discussed in Section 2, we replace the dependent variable with the ratio over the average weekly attacks and repeat the regressions in columns (a) and (b). As shown in Table 5, columns (d) and (e), the estimated coefficients and their significance level are very similar to that in columns (a) and (b).

In summary, the first stage estimation and its robustness check show that signing the Convention on Cybercrimes was associated with 15.81% ~ 24.77% decrease in the number of attacks originating from the country.

Based on the first stage results, in the second stage, we further examine the impact of the Convention on the interdependence of cyber attacks between countries. Referring to equation (2), we calculate the country-pairwise correlation per country pair per year to measure the interdependence between countries. This generates another panel data with 7725 observations. Among them, 4649 pairs have positive correlation. Table 6 reports the correlation of the independent variables.

INSERT TABLE 6 ABOUT HERE

To address the impact of joining the Convention on the interdependence between countries, we must answer two questions. First, for any pair of countries, was the closer status in joining the Convention associated with higher correlation in the trend of cyber attacks? Second, for countries that joined the Convention earlier, did they have higher correlation in the trend of cyber attacks? Referring to equation (3), we regress on the whole samples and exclude the year fixed effects via a random effect model with adjustment of standard errors. Table 7, column (a) reports the result.

INSERT TABLE 7 ABOUT HERE

Overall, the estimation result provides strong evidences of the interdependence between countries in the trend of cyber attacks and that interdependence positively increased in similarity. The coefficients of physical distance, the distance in GDP per capita, and Internet access are negative and significant. The coefficient of the relative status in joining the Convention by signature is also negative and significant, indicating that countries with closer status in joining the convention had higher correlation in time series of cyber attacks.

More interestingly, the coefficient of the common longitudinal status in joining the Convention is negative and significant. It suggests that countries that have both joined earlier, compared to those that have not yet joined or joined later, had lower correlation. This is intuitive considering attackers are strategic and profit-maximizing (Png and Wang 2009). To avoid prosecution, they may reduce malicious activities in countries that have strengthened

international cooperation in enforcement against cybercrimes. Therefore, cyber attacks originating from those countries are less likely organized by international attackers who systematically launch attacks originating from a few countries. Hence we may expect that since they joined the Convention, the attacks originating from those countries became less correlated with each other and with countries that have not yet joined the Convention.

To check the robustness of the above results and clarify its implications, we further conduct the following regressions. First, we include year-fixed effects as they may be highly correlated with the common longitudinal status in joining the Convention. Table 7, column (b) reports the result. Including year-fixed effects improves the R-square but does not change much the coefficients of other variables.

Next, the finding in column (a) may be driven by those pairs of countries of which neither have yet joined the Convention, but their relative status is zero. We exclude those pairs of countries and repeated the regression as in column (b). As reported in Table 7, column (c), the result is very similar to that in column (b). It confirms that closer status in joining the convention were associated with higher correlation in time series of cyber attacks

One interesting implication from the negative effect of the relative status within panels is that if a country joined the Convention, it would become less correlated with those that have not yet joined. We test this hypothesis by including only pairs of countries of which one country joined the Convention during our studied period while the other has not yet joined. In this case, the value of the common longitudinal status in joining the Convention is zero and is excluded from the regression. Table 7, column (d) reports the result. The coefficient of the relative status in joining the Convention is negative and significant. This result shows that as one country joined the Convention, its relative status with those who have not yet joined increased, and the correlation between them decreased.

Another interesting implication from the negative effect of the common longitudinal status across panels is that for any pair of countries that have completely the same timing in joining or not joining the Convention, those that have joined were less correlated than those that have not yet joined. We test this hypothesis by including only pairs whose relative status in joining the Convention was always zero during our studied period. In this case, the relative status in joining the Convention is excluded from the regression. The result is reported in Table 7, column (e). Again, the coefficients of all variables are very similar to previous regressions. The coefficient of the common longitudinal status is negative and significant, which confirms our speculation. Further, this regression also evidences the negative effect of the common longitudinal status within panels, i.e., the correlation between countries that have joined the Convention decreased over time.

Lastly, we notice that among 7725 observations, 4649 pairs have positive correlation while the others are negatively correlated. Therefore, if the more distant the relative status in joining the Convention was associated with less correlation between countries, did it lead to higher probability in negative correlation? We test this speculation via a multinomial logistic regression on the subsamples for column (d). Based on the distribution of the correlation between countries, we code it into a categorical variable CAT with three categories, i.e. correlation between -0.1 and 0.1 is coded as 0; correlation larger than 0.1 is coded as 1; correlation less than -0.1 is coded as 2. The distribution of the three categories is 24.21%, 47.97% and 27.82% respectively. Using the category 1 as the base case, the estimation result shows that one week change in the relative status in joining the Convention, the log of the ratio of the two probabilities, $P(\text{CAT}=2)/P(\text{CAT}=1)$, would be increased by 0.0139 with significance

level larger than 99%. This result suggests that if one country that have joined the Convention, its correlation with those that have not yet joined, became less or even significantly negative. The possible explanation is that to avoid prosecution, attackers may strategically relocate the source of attacks from the group of countries that have joined the Convention to those that have not yet. Consequently the number of attacks from the two groups moved in opposite direction.

In summary, the estimates for stage 2 suggest that joining the Convention had two types of effects on the interdependence between countries in time series of cyber attacks. First, for any pair of country, closer status in joining or not joining the Convention was associated with less negative or more positive correlation. Second, joining the Convention or joining it earlier was associated with lower correlation between countries over time.

5. Concluding Remarks

This study has several important implications for government policies, cyber insurers and business organizations. First of all, international legislation is an effective way to counter cyber attacks among member countries. However, joint operations and mutual legal assistance treaties across national borders have long been considered inadequate (Anderson et al. 2008). In the midst of hesitation among a few E.U. member countries, our study provides evidence to support participation in the Convention on Cybercrimes. sheds light on identifying the potential collaborators to reduce cyber attacks originating from other countries. One important source of interdependence is the attacks which control remote terminals to conduct additional attacks in the target country. In such a case, the interdependence is not a desirable feature and needs to be avoided. For cyber insurers, the country-level interdependence can be used as a framework to better assess the risks faced by multinational companies. Based on our results, the overall network security risks may be higher for a company operating in two neighboring countries than the other companies operating in two geographically dispersed locations. For organizations, this study provides the guidance on choosing server locations. For example, it will be more secure to locate backup servers in the country with lower interdependence.

Our study would have some interesting extensions. We can examine the effects of the convention on non-member countries. For instance, the convention may have a displacement effect (Png et al. 2008) such that the convention increases the attacks originating from non-member countries. Second, the nature of attacks and interdependence may be different 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.”

Like many other studies, our study is not without limitations. First, we are unable to collect the data on the number of attacks between two countries. If we had such data, we could have directly measured the amount of interdependent attacks between a country pair. Next, some country-specific variables are available only at the yearly level while the attacks are measured at the weekly level in the first stage. Despite the limitations, our study is one of the first attempts to examine the effectiveness of international conventions in deterring cyber attacks and the country-level interdependence.

Reference

- [1] 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.
- [2] Anderson, Ross, Rainer Boehme, Richard Clayton and Tyler Moore, “Security Economics and European Policy”, *Seventh Workshop on the Economics of Information Security*, Tuck School of Business, Dartmouth College, Hanover, NH, June 25-28, 2008.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] Johnson, David W. and Roger Johnson, “New developments in social interdependence theory, (SOCIAL INTERDEPENDENCE THEORY)”, *Genetic, Social, and General Psychology Monographs*, Heldref Publications, 2005.
- [8] Kennedy, P. E., “Estimation with correctly interpreted dummy variables in semilogarithmic equations”, *American Economic Review*, Vol. 71, No. 4 (Sep., 1981), 801.
- [9] Kshetri, N., “The simple economics of cybercrimes”, *IEEE Security & Privacy*, 4, 1 (January/February 2006), 33-39.
- [10] Kunreuther, Howard and Geoffrey Heal, “Interdependent Security”, *Journal of Risk and Uncertainty*, Vol. 26 Nos. 2-3, March 2003, 231-249.
- [11] Kunreuther, Howard and Geoffrey Heal, “Modeling Interdependent Security”, *Risk Analysis*, Vol. 27 No. 3, June 2007, 621-634.
- [12] 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.
- [13] Png, Ivan P.L., Chen-Yu Wang, and Qiu-Hong Wang "The Deterrent and Displacement Effects of Information Security Enforcement: International Evidence," *Journal of Management Information Systems*, 25:2, Fall 2008, 125 - 144.
- [14] Sharpe, William F., “Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk”, *Journal of Finance*, 1964, 19:3, pp. 425-442.
- [15] Symantec, Report on the Underground Economy for July 07–June 08, November 2008. Varian, Hal R., “System reliability and free riding”, University of California, Berkeley, November 2004.

Appendix

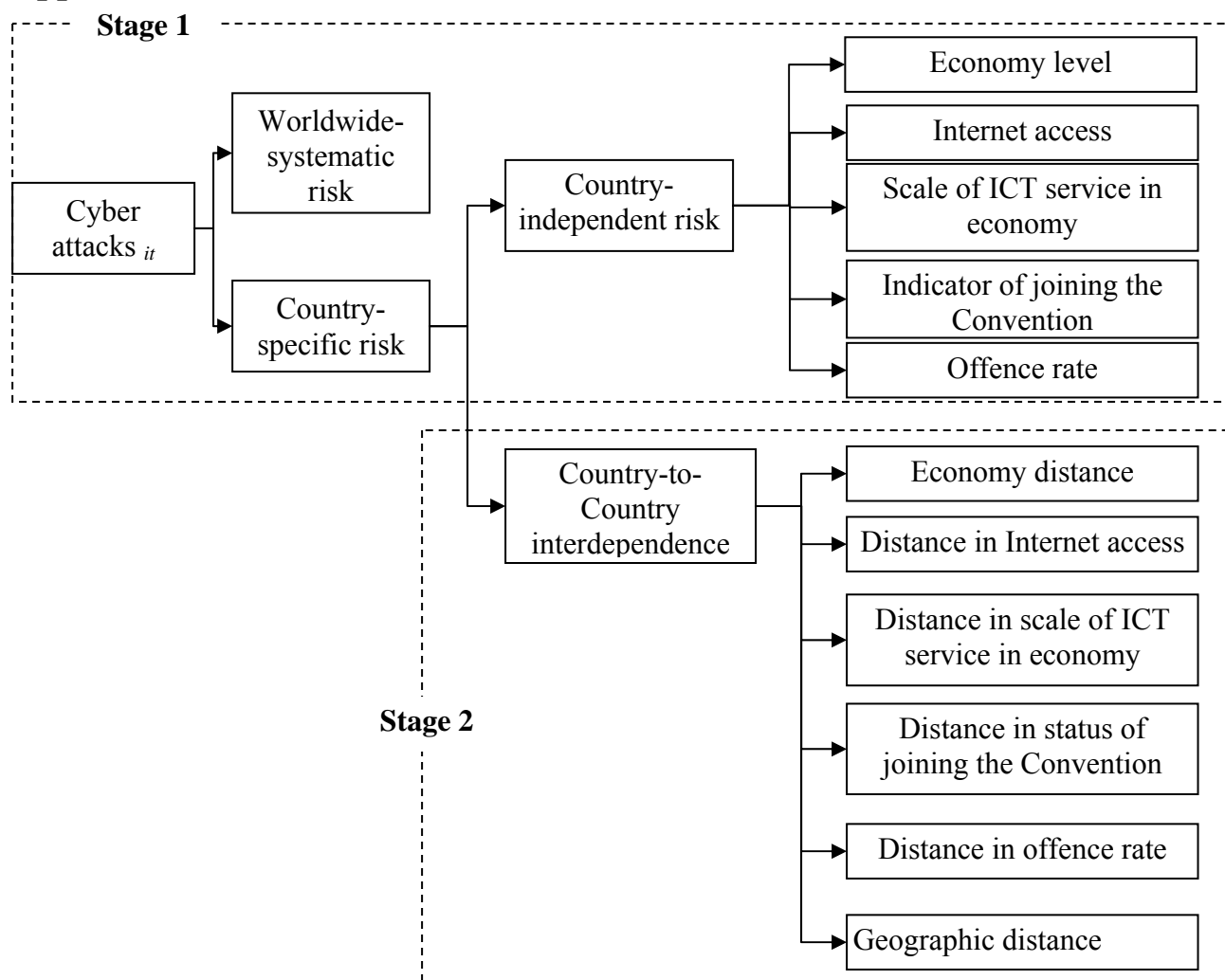


Figure 1. Cyber attack interdependence model

Table 1. Independent variables and their measurement.

Factors as independent variables	Measurements
Economy level	GDP per capita, GDP_{iw} . Unemployment with tertiary education, UMP_{iw} .
Internet access	Internet user base, $IUSER_i$. Price basket for Internet monthly subscription, $IPRICE_{iw}$.
Scale of ICT service in economy	Computer, communications and other services (% of commercial service imports) ⁶ , IMP_{iw} Computer, communications and other services (% of commercial service exports), EXP_{iw} Computer, communications and other services (% of commercial service imports and exports), $IMPEXP_{iw}$

⁶ Computer, communications and other services (% of commercial service imports) include such activities as international telecommunications, and postal and courier services; computer data; news-related service transactions between residents and nonresidents; construction services; royalties and license fees; miscellaneous business, professional, and technical services; and personal, cultural, and recreational services (Source: World Development Indicators Database).

Indicator of joining the Convention	Status in joining the Convention: signature (=1), $CONSIGN_{iw}$.
Offence rate	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.
Distance in Internet access	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.
Distance in scale of ICT services in economy	Maximum(IMP_{iw}/IMP_{jw} , IMP_{jw}/IMP_{iw}), the value is constant within a year, same for EXP_{iw} and $IMPEXP_{iw}$.
Distance in status of joining the Convention	Absolute value ($\Sigma CONSIGN_{iw} - \Sigma CONSIGN_{jw}$), $\Sigma CONSIGN_{iw}$ is the aggregation within one year.
Common longitudinal status in International cooperation in enforcement against cybercrimes	No. of weeks as of year t since both countries have joined the Convention
Distance in offence rate	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.

Table 2. Status of countries that have joined the Convention on Cybercrimes.⁷

States	Signature
Albania	2001-11-23
Armenia	2001-11-23
Austria	2001-11-23
Azerbaijan	2008-6-30
Bosnia and Herzegovina	2005-2-9
Belgium	2001-11-23
Bulgaria	2001-11-23
Canada	2001-11-23
Switzerland	2001-11-23
Montenegro	2005-4-7
Serbia	2005-4-7
Cyprus	2001-11-23
Czech Republic	2005-2-9
Germany	2001-11-23
Denmark	2003-4-22
Estonia	2001-11-23
Spain	2001-11-23
Finland	2001-11-23
France	2001-11-23

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

United Kingdom	2001-11-23
Georgia	2008-4-1
Greece	2001-11-23
Croatia	2001-11-23
Hungary	2001-11-23
Ireland	2002-2-28
Iceland	2001-11-30
Italy	2001-11-23
Japan	2001-11-23
Liechtenstein	2008-11-17
Lithuania	2003-6-23
Luxembourg	2003-1-28
Latvia	2004-5-5
Moldova	2001-11-23
Former Yugoslav Republic of Macedonia	2001-11-23
Malta	2002-1-17
Netherlands	2001-11-23
Norway	2001-11-23
Poland	2001-11-23
Portugal	2001-11-23
Romania	2001-11-23
Sweden	2001-11-23
Slovenia	2002-7-24
Slovakia	2005-2-4
Ukraine	2001-11-23
United States	2001-11-23
South Africa	2001-11-23

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	USD Thousands at PPP	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
Convention on security	‘1’ as signature	Council of Europe	0.48	0.5	0	1
Computer, communications and other services over commercial service imports	(% 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. Correlations of independent variables in stage 1.

	GDP per capita	Internet access	Indicator of joining the Convention	Computer, communications and other services over commercial service imports
GDP per capita	1			
Internet access	0.0642	1		
Indicator of joining the Convention	0.5458	0.0906	1	
Computer, communications and other services over commercial service imports	0.1278	0.2153	0.292	1
Offence rate	0.698	-0.0496	0.5811	0.2512

Table 5. Systemic interdependence and country-specific effects (both dependent variable and independent variables are in natural logarithm forms except the indicator of the Convention on Cybercrimes)

Independent variables	Dependent variable: ratio over the total weekly attacks			Dependent variable: ratio over the average weekly attacks	
	(a) OLS: panel-corrected standard error	(b) OLS: panel-corrected standard error & Robust check	(c) Two-way fixed effects	(d) OLS: panel-corrected standard error	(e) OLS: panel-corrected standard error & Robust check
GDP per capita	3.26012*** (0.23407)	1.94850*** (0.53124)	3.30877*** (0.24777)	3.2333*** (0.2341)	1.9543*** (0.5316)
Internet access	-0.17192** (0.07122)	-0.05363 (0.10756)	-0.15048*** (0.05665)	-0.1747** (0.0712)	-0.0538 (0.1076)
Ratio of internet security servers	—	-0.16361 (0.13563)	—	—	-0.1648 (0.1357)
Internet price	—	-0.13385*** (0.03868)	—	—	-0.1326*** (0.0387)
Indicator of joining the Convention	-0.22705*** (0.05500)	-0.32295*** (0.07211)	-0.19907** (0.08486)	-0.2242*** (0.0550)	-0.3215*** (0.0722)
Ratio of computer, communications and other services over commercial service imports	-0.46337*** (0.06726)	-0.30853*** (0.08951)	-0.46247*** (0.07189)	-0.4638*** (0.0673)	-0.3091*** (0.0895)
Offence rate	-1.63491*** (0.13455)	-1.94766*** (0.39016)	-1.63712*** (0.13774)	-1.6216*** (0.1348)	-1.9470*** (0.3907)
Unemployed with territory education	—	0.96297*** (0.11578)	—	—	0.9653*** (0.1159)

year 2004	-0.02687 (0.02971)	0.17004** (0.07385)	—	-0.0184 (0.0298)	0.1749** (0.0740)
year 2005	-0.04334 (0.03513)	0.17436* (0.10545)	—	-0.0258 (0.0352)	0.1876* (0.1057)
year 2006	-0.24073*** (0.04521)	0.18427 (0.17874)	—	-0.2207*** (0.0453)	0.1955 (0.1790)
year 2007	-0.26730*** (0.05800)	0.00000 (0.00000)	—	-0.2507*** (0.0581)	0.0000 (0.0000)
Constant	0.00000 (0.00000)	7.67413* (4.37496)	6.52878*** (1.02868)	0.0000 (0.0000)	11.9081*** (4.3830)
R-squared	0.820	0.840	0.823	0.820	0.840
Convention impact ¹	-24.77% ~ -16.03%	-33.00% ~ -22.60%	-25.22% ~ -11.38%	-24.59% ~ -15.81%	-32.92% ~ -22.48%
Number of countries	62	55	62	62	55
Observations	11870	5845	11870	11870	5845

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

Note:

1. Impact of the Convention on Cybercrimes was calculated using Kennedy (1981, equation 1.4) and the standard error using Garderen and Shah (2002, equation 2.4).

Table 6. Correlations of independent variables in stage 2.

	Distance in GDP per cap	Distance in internet access	Relative status in joining the Convention	Common longitudinal status in joining the Convention	Distance in the ratio of computer, communications and other services import	Distance in offences per 100,000 inhabitants	Physical distance
Distance in internet access	0.0457	1					
Relative status in joining the Convention	0.1996	0.016	1				
Common longitudinal status in joining the Convention	-0.1312	0.0093	-0.3546	1			
Distance in the ratio of computer, communications and other services import	0.0185	0.0743	0.0119	-0.059	1		
Distance in offences per 100,000 inhabitants	0.4008	-0.0413	0.1606	-0.1052	-0.0162	1	
Physical distance	0.0393	0.1057	0.1404	-0.262	-0.0454	0.0891	1
Neighboring country	-0.1063	-0.0364	-0.1277	0.0848	-0.0145	-0.063	-0.2633

Table 7. Country-specific interdependence (Dependent variable: the correlation of residuals by country and year from stage 1)¹

Independent variables	(a) Whole samples	(b) Whole samples	(c) Excluding pairs of countries neither of which have yet joined the Convention	(d) Including only pairs of country in which one joined but the other not yet	(e) Including only pairs that have completely the same status in joining the Convention

Distance in GDP per cap	-0.00347535*** (0.00115542)	-0.00415788*** (0.00115789)	-0.00551884*** (0.00143342)	-0.00519412*** (0.00150427)	-0.00136174 (0.00199326)
Distance in Internet access	-0.00027528*** (0.00009972)	-0.00028435*** (0.00010027)	-0.00026329** (0.00010755)	-0.00015179 (0.00011212)	-0.00035809** (0.00016745)
Relative status in joining the Convention	-0.00090154*** (0.00014182)	-0.00087330*** (0.00014022)	-0.00085766*** (0.00021352)	-0.00085969* (0.00044829)	—
Common longitudinal status in joining the Convention	-0.00024956*** (0.00008266)	-0.00022660*** (0.00008164)	-0.00026257*** (0.00009081)	—	-0.00022405*** (0.00008658)
Distance in the ratio of IT service import	-0.00057223 (0.00044976)	-0.00048894 (0.00045761)	-0.00057864 (0.00051036)	-0.00061144 (0.00051653)	-0.00058888 (0.00082583)
Distance in offences	-0.00027603 (0.00026880)	-0.00023424 (0.00027309)	-0.00020076 (0.00032043)	-0.00027586 (0.00032704)	-0.00016649 (0.00045222)
Physical distance	-0.00001076*** (0.00000116)	-0.00001050*** (0.00000115)	-0.00001171*** (0.00000148)	-0.00000803*** (0.00000181)	-0.00001165*** (0.00000171)
Neighboring country	0.02203826 (0.01902016)	0.02337230 (0.01878447)	0.00722394 (0.02207645)	-0.01194192 (0.03710020)	0.02903158 (0.02465120)
Year 2004	—	0.10041813*** (0.01067932)	0.12687656*** (0.01240109)	0.13822572*** (0.01539986)	0.05984832*** (0.01660718)
Year 2005	—	-0.06294175*** (0.00979046)	-0.04308761*** (0.01095072)	-0.02707223** (0.01373626)	-0.10364107*** (0.01577035)
Year 2006	—	-0.04127503*** (0.00877351)	-0.02728220*** (0.00975762)	-0.01259651 (0.01230144)	-0.07245914*** (0.01438531)
Year 2007	—	-0.06559872*** (0.01154470)	-0.06649162*** (0.01291353)	-0.14485471*** (0.01564099)	0.01437430 (0.01700941)
Constant	0.17716007*** (0.00946612)	0.18260768*** (0.01076698)	0.18003837*** (0.01223954)	0.15630075*** (0.02454114)	0.19994724*** (0.01634173)
Observations	7725	7725	5729	3922	3386
Number of panels	1830	1830	1365	930	765
R-square ¹	0.0235	0.0656	0.0569	0.0400	0.0277

Robust standard errors in parentheses ; *** p<0.01, ** p<0.05, * p<0.1

Note:

1. R-square is the normal OLS R-square.