MIS Quarterly

RESEARCH ARTICLE

CYBERCRIME DETERRENCE AND INTERNATIONAL LEGISLATION: EVIDENCE FROM DISTRIBUTED DENIAL OF SERVICE ATTACKS

Kai-Lung Hui
School of Business and Management, Hong Kong University of Science and Technology,
Clear Water Bay, Hong Kong, CHINA {klhui@ust.hk}

Seung Hyun Kim
School of Business, Yonsei University, Seoul 120-749 KOREA {seungkim@yonsei.ac.kr}

Qiu-Hong Wang
School of Information Systems, Singapore Management University, SINGAPORE {qiuhongwang@smu.edu.sg}

Appendix A

Other Excerpts from the Hacker Forum

V e X (2008-08-12 04:33): Simon Parker Wrote (2008-07-14 22:16) :|*Yep. Never hack without knowing the laws (Sometimes they can even work for you!) "The man speaks the truth. Learn them. Don't live them Use them to your advantage."*

- Hackers or potential hackers having concerns related to the issues addressed in COC Articles 11, 22, 29, and 41.

Articles	Hacker Forum Posts
Article 11	bckc (03-13-2011 05:34 PM): *"...and dont worry about the police, there are no "international laws within states governed by independancy"meaning that if shes in a different country the police cant do shit unless its a major offence which it isn't There are conventions. Also, he can be judged in absentia where the crime has happend. And within European Union borders he can be transported due to the crime, because of the European Unions conventions about partnership in law."*
Article 22	flute123 (2010/7/23 20:05): *"By Law...ISP's are not allowed to hand out any information about any IP Number unless it is of a serious crime such as cyber crime. Depends which country your from. They usualy need a court order before they can obtain an ip address."*
Article 29	michaeljay (06-11-2011 08:07): "*This is a confusing issue. Usually there needs to be "double criminality," that is, an act must be illegal in both the country harboring a suspect and the country seeking extradition. That's why the US government couldn't prosecute some dude in the Philippines several years back for distributing a worm, as that act was not illegal in the Philippines at the time. As for what country claims jurisdiction, there are many factors to consider, such as territoriality (where the suspect and the slave are located, where the servers are located, etc) and nationality. The countries involved work this out themselves.…So basically there's not really a clearcut way to avoid prosecution....Damnit.Thanks for the help."*

Article 29	Paradigma (2011/2/19 17:17): *"If he proxied from country X to country Y and country Y isn't cooperative with country X, they won't be able to subpoena the IP records."*
Article 29	#FFFFFF (2009/8/14 21:01): *"Try to use a proxy from a different country. If some feds or something find your proxy hacking, the proxy company doesn't have to give them the ip since they have different laws and do not have to obey. If you have proxies in your countries I wouldn't suggest it."*
Article 41	I5??/span> (2011/6/30 22:08): *"Not sure where you live, but in California, extortion is punishable by up to four years in the California State Prison and by a maximum 10,000 fine. Every state and country is different."*
Article 41	Naye (2009/8/23 19:27): *"The laws vary depending on your state (or country for that matter). In Texas if you just hack a site or a computer with no damage done, its a class A misdemeanor."*

- Hackers or potential hackers having concerns on the enforcement against cybercrime.

Carb0n F1ber (2010/1/13 6:25): *"Buying a premium VPN service with port-forwarding service could help you out. But again, check their TOS (Terms of Service)....hey would constantly be monitoring the forwarded ports, and if they found traffic similar to connecting to a RAT or such, then your contract might get terminated without notice and you'll loose your money... Worst case scenario, depending on the kind of activity done, you might even get into trouble with the law (again depending on your current state/country cyber laws)."*
Gallant (2010/10/6 15:42): *"Well I like my house and don't like jail….Keylogging and RATs are both illegal (not to mention immoral) and are punishable by law in various countries."*
stdape2011 (2011/8/22 16:03): *"very illegal. depending on country may have different rules, but UK 5 years in a Holiday camp oooops i mean Prison lol."*
monologue (2010/6/26 8:47): *"I live in a 3rd world country in Asia, the police here are not smart like in the States. I will be opening a website, which is likely illegal...How will they track me down? and what are the steps I need to take in order to protect myself? Isn't it easy for them to find me once they contact my ISP? I am actually kind of scared but I know this is gonna be worth it once I success.I know it is bad to ask stuffs like this but this is a freaking "hack" forum. I bet other people hack stuffs and do even worse stuffs than me lol. anyways cheers folk, help me with this. Recommend me some kick ass programs. Like really really safe one, which cant be tracked by a freaking 3rd world country in Asia, the Phili...ok, thanks a lot!"*
PCAnarchist (2008/5/15 11:18): *"I m unsure how irish law works but if i get caught hacking in my country of the UK, i will just say im an irish citizen, as i am, and also a british citizenbut some risky buisness, as some ISP spy on you"*
user_floor 1 (2010/4/24 12:04): *"Woah buddy, you better lay low a bit, the Greek Internet Police may be after you after that vicious hacking attack you pulled on your friends Gmail. I'm sure Gmail already warned your ISP, get out of the country, you're fucked!"*
Jadencide (2010/2/24 6:38): *"I've been screwing with some from diffrent countries and there threatening me with cops and law enforcement. Should i uninstall the server and run?"*
Qwazz (2010/11/7 17:29): *"It is neither easier nor harder, its all about your personal skill as a SE.The thing about Europe is some countries have more lenient laws so the consequences will be less severe."*
polabear345 (2011/7/11 12:16): *"Whats usually happens if you get caught RATting by the authorities? And if your slave is in a diferent country, can interpol get involved? I don't want my dad to go to jail lol. Replies appreciated. Thanks."*
metzrock (2011/5/9 16:39): *"So recently I took one of my slaves xbox live gamertags and he threatened to call the police. I'm only slightly worried because he is in a different country and I'm behind a VPN. What I'm wondering is, should I be worried? Thanks :)"*
hexon (2009/11/30 5:45): *"unless you're in a no cyber law country (which is a no no for you) , then you have the possibility of being caught (if the admin is really pissed off and decides to trace you back)"*
DA-SYPhA (2009/1/12 9:27): *"Well, i don't know about your countries, but in Australia, Cybercrimes is one of the most seriously treated crimes, trust me, it is, got me expelled, i almost had Federal Police involved in it...just for gaining admin... but it mostly depends on who is affected by what you do. But for most of the cases ive read about, they usually just get a year probation, a fine and like a year with no computer, which would KILL me. But all of the serious hackers got jail time- Infamous hackers."*
RJSv2.5beta (2009/4/13 13:11) *"Uh, yeah, they do have a better program. It's called the record of your IP in question, presenting the record to a judge as evidence of the alleged crime in question, a subpoena or warrant from said judge for the seizure of account info from the ISP/registrant of said IP. Then depending on country, severity of crime, assholeness and authority of law enforcement involved, the possible seizure of some/all equipment at said location as evidence and/or followed/accompanied by possible arrest of individuals associated with said location/equipment.1. Don't commit computer crimes.2. Don't get caught."*

- Hackers or potential hackers challenging the effectiveness of the enforcement.

bobsagetfullhouse (2009/12/21 20:11): *"Your ISP does not have some magical "rat detector" that checks all of its users for rat usage and then call the police. … Have you ever heard of a case where any internet service provider actually took the initiative to call the police? No. They have a lot more things to worry about, and don't monitor the websites and programs their users are using. What CAN happen though, if one of your victims is tech-savy is he can scan for IP addresses that are currently connected to him. If he manages to get your IP address he can then contact his local police, and from there the police can contact your ISP. Your ISP will most likely tell the police that it is not in their service contract to monitor the online activity of their subscribers, and it will end there. Even this scenario is unlikely, considering if they are stupid enough to download the RAT in the first place, they most likely won't have the knowledge to scan for connected IP addresses either. So the point is, you DON'T have to worry about your ISP spying on you using your RAT, and calling the police."*
Venomxboss (2009/12/4 18:45): *"Lmfao no, its across countries and if you just deny it you can get out of almost everything. Just if you get swatted which 99.9% chance it won't happen just don't say anything till you speak to a lawyer"*
teluwat (2009/12/5 14:54): *"You're fine. It's impossible for the police to do anything about it so far overseas."*
xPloit (2010/10/09 22:12): *"that's true...even if somebody did report (unlikely) it is also unlikely that the cops would be willing to help. They have much bigger things to deal with that a conned pedo."* bejogila (2010/12/7 10:08): *"nice comment ro.. :p ;)specially if you're in a 3rd country... hehehehehe... :peven for a 1000 dollar, i'm not sure there will be a police coming by to your door... huahahahahahaha"*
don_ddu (2009/8/10 8:27): *"it also depands on which country you live in i.e cyber laws of country for example in most of asian countries no 1 cares"*
nak15 (2011/8/30 20:02): *"Police is not going to get involved unless they have solid evidence. For all they know your computer could be a decoy for another hacker, meaning they'll need to confiscate your computer, and doing that would result in needing a warrant. If you did this overseas than forget it your A-ok."*
Plitvix (2010/10/1 15:09): *"None when I injected this site =).I don't worry about that because you didn't do anything that is 'illegal'. In my country, law is not developed enough for them to charge me."*
Subliminally (2010/08/31 13:16): *"Is Dosing / DDosing illegal in Switzerland? I have tried google couldn't find anything on it."* Kicker (2010/08/31 13:22): *"No one ever gets caught so it doesn't matter."* crim (2010/08/31 13:24): *"you can probably answer it yourselfis it allowed to destroy someone elses property in switzerland?"*
ibrahim0346 (2011/2/19 18:34): *"okay i am from pakistan and if i hack a website of anyother country then pakistan will pakistan cyber police arrest me ? ?"* alibaba5 (2011/2/19 19:56): *"I guess Pakistan has other things to worry about, i don't think they have any laws about cybercrime, and if they have, a simple deface won't hurt you."*
crash0verride (2009/1/12 15:26): *"pffft ive ddosed so many sites....Its called hacking a site in another country, OR just not giving a shit and doing it anyway like me haha I have never ever been caught here in Canada...maybe they are catching on slowly? Maybe canada dosnt care?"*
Baz (2009/8/23 7:40): *"melbourne here , you know lets say a hacker from the other side of the world does deface the LAPD , what are they going to do ? send the fbi ? you know it costs tens and thousands of dollars to deal with crimes committed in another country , its why if you stole a few hundred bucks from a overseas bank account there is very little they can do , its not worth there time and money and effort. go steal a few millions dollars and watch how fast your local law enforcement and your goverment finds out lol"*
333 (2010/7/11 2:15): *"Cyber Police Department is active in many states of India. For eg: Some will have sites for the purpose of defamation,abuse etc.Videocon files police complaint on fake websites - Hindustan Timesbut ,these people can't do anything on someone sitting in another country :(Target all Pakistani websites!Let the reign of script kiddies begin!"*

- Hackers or potential hackers intending to minimize risks.

FullyAutomatic (2011/8/20 3:36): *"Depends how big the botnet is, what you use it for and what country you live in. On average, how long would be the prison sentence be in the 1st world for owning a 1000 bot botnet?"*
digigoth (2010/8/15 5:43): *"yeah germany got some strict laws, i heard too :)Canada is a good choice, since the laws are very friendly ;]or any undeveloped/native country :P"*
gunnit (2009/4/15 15:45): *"nice tutorial ; brute forcing is not a good idea unless you live in a third world cuntry or in Italy. People in US and Canada ; Swizzerland; France and Israel Should be most carefull ; thise countries have the strongest onternet police and the largest number of cybercriminals brought to justice"*

SomeoneWithAPurpose (2009/4/23 5:09): *"Depends on what country your from. If you're from the US, there's a 10-20% chance that they'll come for you. My friend from New York had the feds in his house earlier this week. … If you live in Europe, you have a 40-50% chance they'll come for you. If you live in Russia, it is the same as Europe. But if you live in China for example, they WILL find you... And hacking is punishable by the death penalty there. Anyway, in your case; If you login someones private account without permission, you have broken the computer criminal law of "unauthorized access", where you can end up having to pay a fine of a minimum 200, depending on the damage you have done + you will have a stamp on your criminal records, making you unable to get work at some places EDIT: Btw, the reason the cops came to my friends place was because 2 weeks ago, he had been attacking only 2 websites with SQL injection. But he had not used protection (i.e. proxies). So anyone who thinks that nothing will happen; Well it will..."*
Endebrito (2009/12/3 10:41): *"If you are going to host anything in any country you must first know their laws about internet.For example, you must better do not try to host anything in any datacenter in Spain. The law makes the admins to save all the connection logs for a year, but sometimes they save them for even more. And not only in DC, but also the librarys, universities and so on gather all kind of connection logs. The idea of this post is to know the national laws that rules the net in every country. Which is the best to host illegal stuff? Which one is the worst?"*
endebrito (2009/12/3 10:41): *"If you are going to host anything in any country you must first know their laws about internet.For example, you must better do not try to host anything in any datacenter in Spain. The law makes the admins to save all the connection logs for a year, but sometimes they save them for even more. And not only in DC, but also the librarys, universities and so on gather all kind of connection logs.The idea of this post is to know the national laws that rules the net in every country. Which is the best to host illegal stuff? Which one is the worst?"*

- Hackers or potential hackers raising concerns on the enforcement before committing DDOS attacks.

S?MNIUM.EXE (2009/7/17 10:36): *"In what trouble can I get if I DOS one WOW private server site?* *--youll get banned and arrest bro* *--So what if I'll get banned, I don't play that game..* *--look up the laws in your country, i know here in the uk a dos or ddos attack now carries a heavy sentance. do it from a public wifi and you should be ok* *--How to check that?Where?* *--lol fuck this country.Where can i find details?* *--google us ddos laws ect, in the uk you can be jailed for up to 10 years for a dos attack."*
Cooljack (2009/2/23 03:19): *"Hi, In Poland DOS attack is NOT an illegal activity (the law here does not forbid you to "invite friends' to another website). I wonder how it works in other countries?* *--I think in most of the countries...DOS attack is illegal...But unfortunately, simple DOS attack such as "Ping Of Death" does not work anymore...* *--in italy it's illegal. also netstrikes are not completely legitimate...* *--Illegal in Australia as well.* *--In Lithuania it's inlegal, but cyberpolice is very lazy.* *--in MF turkey is everyting legal so fear if you suppoert the patroitism and militery, th MF militery spend millions of dollar to build their own bandit.* *--at greece is illegal !* *--It's illegal in every country that has a government with an iq above 75. The best cyber polic, however, are in Japan, Canada, US and the UK* *-it's illegal also in tunisia* *--you sure its legal in poland? its illegal in the uk and most MEDC's* *--illegal Sweden, Finland, Norway, Russia, Usa(The Mexico Touchers), England, Scottland, Wales, Ireland, Iceland, Japan, Canada(USA's hat)Denmark, Italy, Spain, Australia, Germany, Austria, Schweiz, Holland, Hungary, I guess China and India as well legal poland, Turkey, I guess Hole Africa, maybe southamerica, centralamerica, Cuba and Jamaica idk lolDon't rely on this, it probably has sme faults* *--in croatia is illegal* *-- (True, although my ISP (T-Com xD) never even warned me about it (yes, I've been DoSing a bit).* *--The law on net protection is pretty weak in Poland. There was a case last year, when a group of hackers took down the main police website for a day, just to show that it is a legal thing to do. The law interprets DDOS attack, as "inviting friends to visit another website". I'm not sure, though, if building a botnet is legal. Probably not, if by using trojans.* *--I've heard that DoS is legal on Moon, atleast there isn't anyone who said it ain't. So if you fly to the Moon and have a satellite connection from there, you sure can DoS anyone you like."*

- Hackers or potential hackers using DDOS attacks to earn money.

vladmir (2010/9/19 13:46): *"Has anyone here ever successfully extorted money from a business or organization by performing DDoS attacks on their website? I know it's illegal in most Western countries but I live in Eastern Europe where cybercrime laws are very lax. It seems like a good way to monetize a botnet. Has anyone tried or done this?*
--Not anybody on HF, but yes, a lot of people do that.
--I don't know anyone who has done such a thing.It must be used as a way to earn in some eastern countries actually.
--ibebootin on de eboxlifes an getter randomies two paid me two stop deddawesing dem
-- dam br0 h0w miny ms p0intz??
--Well, last year with my public rf...I mean fully r00ted unix, I made 4000 in extortion money from DDoSing ebay.
--i do this in some private server games=p1 payment of 120dllsor 20 dlls monthly for 1 yearjojo
--try casino and betting websites
--dollars?If they pay you 20 a month to have you stay away from you DDoS button, they are ripping you off.
--oh! sorry it was weekly jojo not monthly ;p sorrry"

Appendix B

Compilation of Domestic Cybercrime Legislation Data

Various international organizations maintain country profiles on cybersecurity development and cybercrime legislation. For example, the International Telecommunication Union (ITU) publishes a cyberwellness profile which provides an overview of a country's cybersecurity development, including the legal measures. However, as the ITU acknowledges, "*No single publication can adequately cover all aspects in depth*."[1] Accordingly, we compiled domestic legislation against cybercrime in each country from multiple sources, including Asian School of Cyber Laws (ASCL), Council of Europe (COE), International Telecommunication Union (ITU), and United Nations Office on Drugs and Crime (UNODC). Each of these organizations maintains a cybercrime legislation repository covering 42–195 countries. The repositories contain up-to-date legislation codes and country reports. However, they do not document historical changes of the legislation (except when the changes are officially recorded as part of the legislation itself). In some cases, the enforcement dates are missing, so we conducted an Internet search to locate more detailed information on the legislation. The following table lists the repositories used in this study and their publishers.

Publisher	Report
Council of Europe (COE)	Country Profile (Domestic Legislation): "*The country profiles have been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation*." Source: http://www.coe.int/web/cybercrime/country-profiles
United Nations Office on Drugs and Crime (UNODC)	Repository Cybercrime (Database of Legislation): "*The cybercrime repository is a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance*." Source: https://www.unodc.org/cld/index-sherloc-leg.jspx?tmpl=cyb
International Telecommunication Union (ITU)	Cyberwellness Profiles: "…*the cyberwellness profiles provide an overview of the countries' levels of cybersecurity development based on the five pillars of the Global Cybersecurity Agenda namely Legal Measures, Technical Measures, Organisation Measures, Capacity Building and Cooperation. Information on Child Online Protection, a key ITU initiative, is also covered*." Source: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx
Asian School of Cyber	Global Cyber Law Database:

[1]See International Telecommunication Union, *Cyberwellness Profiles*, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx (accessed December 5, 2015).

Laws (ASCL)	"*Global Cyber Law Database (GCLD) aims to become the most comprehensive and authoritative source of cyber laws for all countries*." Source: http://www.cyberlawdb.com/gcld/

From these repositories, for each of the 106 countries in our sample, we first identified legislation that were enacted between 2004 and 2008. If we could not locate the date in which a legislation was enforced, then, depending on availability, we used either the assented date or the date in which the legislation was published. If none of these dates are available, then we excluded that particular legislation. We assume that the enforcement date is the first day of the month if only year and month information is available.

We further removed all legislation irrelevant to DDOS attack, such as copyright, child pornography, spam, money laundering, fraudulent use of credit or debit cards, etc. However, we included legislation on extradition as it is related to international co-operation, which is covered by the Convention on Cybercrime (COC).

This compilation leads to a set of domestic legislation data organized by country and date. Among the 106 countries in our sample, in 2004–2008, 37 countries neither ratified the COC nor introduced any domestic legislation against cybercrime. 46 countries introduced domestic legislation against cybercrime but did not ratify the COC. 3 countries ratified the COC without introducing domestic legislation against cybercrime. 20 countries have ratified the COC and introduced domestic legislation against cybercrime.

For each country in our sample, we constructed two variables to measure the extent of domestic legislation against cybercrime. One is a dummy variable that equals 1 starting from the date when the *first* domestic legislation entered into force. The second is a continuous variable that counts the cumulative number of domestic legislation enforced over time. The following table reports the descriptive statistics of the domestic legislation.

Variable	Unit	Mean	Std. dev.	Min	Max	Source
First domestic legislation or after	1 = At least one domestic legislation against cybercrime was in place; 0 = No domestic legislation against cybercrime	0.509	0.500	0	1	COE, UNODC, ITU, ASCL
Number of domestic legislation	Number of domestic legislation (including revisions)	1.283	2.550	0	36	COE, UNODC, ITU, ASCL

Note: n = 16,429, number of countries = 106

Appendix C

Unreported Tests Cited in the Main Text

	(1)	(2)	(3)	(4)
VARIABLES	Only enforcing countries	Only COE countries	Split enforcement effect over time	Add % AS connections to countries with domestic legislation
COC enforcement	-0.171***	-0.140***		-0.252***
	(0.031)	(0.030)		(0.044)
COC enforcement in 2004			0.248***	
			(0.040)	
COC enforcement in 2005			0.037	
			(0.038)	
COC enforcement in 2006			-0.258***	
			(0.048)	
COC enforcement in 2007			-0.249***	
			(0.037)	
COC enforcement in 2008			-0.412***	
			(0.049)	
% AS connections to other enforcing countries				0.221***
				(0.067)
COC enforcement × % AS connections to other enforcing countries				-0.592***
				(0.090)
% AS connections to other countries with domestic legislation				-0.123**
				(0.053)
COC enforcement × % AS connections to other countries with domestic legislation				0.409***
				(0.090)
Cumulative domestic legislation (log)	-0.360***	-0.390***	-0.266***	-0.219***
	(0.068)	(0.056)	(0.043)	(0.041)
Internet hosts (log)	-0.952***	-0.847***	-0.982***	-0.969***
	(0.019)	(0.021)	(0.009)	(0.009)
Unemployment rate	-0.100***	-0.020	-0.042***	-0.044***
	(0.019)	(0.014)	(0.009)	(0.009)
GDP in PPP (log)	-2.532***	-1.664***	-0.789***	-0.596**
	(0.641)	(0.472)	(0.268)	(0.262)
Higher education students (log)	-3.365***	-0.231	0.596***	0.509***
	(0.414)	(0.359)	(0.152)	(0.154)
Internet users (log)	0.567***	0.351***	-0.111**	-0.113**
	(0.125)	(0.085)	(0.044)	(0.046)
% digital main lines	-0.009	-0.006	0.010*	0.008
	(0.006)	(0.006)	(0.006)	(0.005)

	(1)	(2)	(3)	(4)
VARIABLES	**Only enforcing countries**	**Only COE countries**	**Split enforcement effect over time**	**Add % AS connections to countries with domestic legislation**
ISDN subscribers (log)	0.602***	0.440***	0.690***	0.696***
	(0.157)	(0.132)	(0.086)	(0.089)
Land area (log)	20.907***	7.274	0.810	0.322
	(7.147)	(5.103)	(1.061)	(1.096)
Control of corruption	0.739***	0.835***	-0.233***	-0.177***
	(0.138)	(0.097)	(0.066)	(0.066)
Government effectiveness	-0.629***	0.206*	-0.157**	-0.285***
	(0.137)	(0.122)	(0.070)	(0.064)
Political stability and absence of violence/terrorism	-0.250**	-0.510***	-0.312***	-0.319***
	(0.111)	(0.100)	(0.056)	(0.059)
Regulatory quality	0.083	0.602***	0.352***	0.368***
	(0.177)	(0.114)	(0.068)	(0.073)
Rule of law	1.714***	0.059	0.756***	0.776***
	(0.235)	(0.170)	(0.087)	(0.089)
Voice accountability	-1.059***	-0.520***	-0.238***	-0.293***
	(0.174)	(0.127)	(0.089)	(0.085)
Country fixed effects	Yes	Yes	Yes	Yes
Day fixed effects	Yes	Yes	Yes	Yes
Country time trends	Yes	Yes	Yes	Yes
Observations	4,008	6,945	16,429	16,429
Number of countries	23	41	106	106
R-squared within model	0.890	0.874	0.812	0.811

Notes: Log number of victim IP addresses per Internet host as dependent variable. Column (1): Sample includes only enforcing countries; Column (2): Sample includes only COE countries; Column (3): Split enforcement effect by year; (4): Include the percentage of AS connections to other countries with domestic legislation and its interaction with COC enforcement. Spatial correlation-consistent standard errors in parentheses. ***p < 0.01, **p < 0.05, *p < 0.1.

Appendix D

Kumar and Telang's (2012) DID Test

Following Kumar and Telang (2012), we construct a DID test by excluding the data in 2006 and creating pre- and post-treatment groups that are roughly balanced in size, each containing two years of observations (2004–05 and 2007–08). We exclude countries enforcing the COC in other years because they may be different from the non-enforcing countries and so may not serve as good controls. Countries with data only before or after 2006, viz. Afghanistan, Bosnia and Herzegovina, Brunei, Botswana, Kazakhstan, Lebanon, and Serbia, are excluded as well. This DID test compares the attacks recorded in countries enforcing the COC in 2006 against the non-enforcing countries, and before and after the year of enforcement. The coefficient of COC enforcement (equivalent to the interaction between the indicator of countries enforcing the COC in 2006 and the indicator of post-2006) is negative, –0.573, and statistically significant.

	(1)
VARIABLES	**DID for countries enforcing in 2006**
Post-2006 (= 1 if year > 2006)	-0.281**
	(0.138)
Countries enforcing COC in 2006 × Post-2006	-0.573***
	(0.036)
Cumulative domestic legislation (log)	-0.078
	(0.051)
Internet hosts (log)	-0.993***
	(0.011)
Unemployment rate	-0.003
	(0.006)
GDP in PPP (log)	-0.991***
	(0.277)
Higher education students (log)	0.087
	(0.086)
Internet users (log)	-0.015
	(0.037)
% digital main lines	0.021***
	(0.004)
ISDN subscribers (log)	0.060*
	(0.030)
Land area (log)	1.509***
	(0.304)
Control of corruption	-0.053
	(0.076)
Government effectiveness	0.295***
	(0.065)
Political stability and absence of violence/terrorism	-0.686***
	(0.043)
Regulatory quality	-0.107
	(0.065)
Rule of law	0.206*
	(0.105)
Voice accountability	0.674***
	(0.070)
Observations	9,738
Number of countries	78
R-squared within model	0.671

Appendix E

COC Enforcement Effect over Time

	(1)	(2)	(3)	(4)
VARIABLES	1st year of enforcement vs. no enforcement	2nd year of enforcement vs. no enforcement	3rd year of enforcement vs. no enforcement	4th year of enforcement vs. no enforcement
First year of enforcement	-0.215***			
	(0.036)			
Second year of enforcement		-0.280***		
		(0.049)		
Third year of enforcement			-0.477***	
			(0.125)	
Fourth year of enforcement				-1.103***
				(0.183)
Cumulative domestic legislation (log)	-0.170***	-0.112***	-0.107***	-0.189***
	(0.038)	(0.039)	(0.039)	(0.044)
Internet hosts (log)	-1.009***	-1.003***	-1.006***	-1.007***
	(0.009)	(0.008)	(0.008)	(0.009)
Unemployment rate	-0.047***	-0.030***	-0.043***	-0.051***
	(0.012)	(0.010)	(0.012)	(0.013)
GDP in PPP (log)	-1.197***	-1.769***	-0.979***	-0.898**
	(0.322)	(0.315)	(0.344)	(0.348)
Higher education students (log)	1.347***	1.310***	1.360***	1.299***
	(0.181)	(0.182)	(0.179)	(0.178)
Internet users (log)	-0.279***	-0.238***	-0.265***	-0.263***
	(0.046)	(0.044)	(0.044)	(0.044)
% digital main lines	0.034***	0.039***	0.026***	0.025***
	(0.008)	(0.007)	(0.007)	(0.008)
ISDN subscribers (log)	0.578***	0.610***	0.652***	0.687***
	(0.083)	(0.084)	(0.086)	(0.082)
Land area (log)	-0.351	-0.093	-0.280	-0.497
	(1.097)	(1.054)	(1.089)	(1.036)
Control of corruption	-0.417***	-0.448***	-0.314***	-0.459***
	(0.071)	(0.069)	(0.082)	(0.084)
Government effectiveness	-0.277***	-0.103	-0.194***	-0.124*
	(0.066)	(0.065)	(0.068)	(0.069)
Political stability and absence of violence/terrorism	-0.240***	-0.271***	-0.272***	-0.264***
	(0.062)	(0.055)	(0.057)	(0.056)
Regulatory quality	0.350***	0.448***	0.396***	0.398***
	(0.078)	(0.076)	(0.081)	(0.084)
Rule of law	0.634***	0.679***	0.619***	0.644***
	(0.099)	(0.095)	(0.095)	(0.108)
Voice accountability	0.108	-0.084	-0.056	-0.002
	(0.100)	(0.099)	(0.095)	(0.111)
Country fixed effects	Yes	Yes	Yes	Yes
Day fixed effects	Yes	Yes	Yes	Yes
Country time trends	Yes	Yes	Yes	Yes
Observations	14,425	14,400	13,510	13,102
Number of countries	106	104	98	94
R-squared within model	0.794	0.793	0.793	0.794

Notes: Log number of victim IP addresses per Internet host as dependent variable. Column (1): Effect of enforcement in the first year; Column (2): Effect of enforcement in the second year; Column (3): Effect of enforcement in the third year; Column (4): Effect of enforcement in the fourth year. Spatial correlation-consistent standard errors in parentheses. ***p < 0.01, **p < 0.05, *p < 0.1.

Reference

Kumar, A., and Telang, R. 2012. "Does Web Reduce Customer Service Cost? Empirical Evidence from a Call Center," *Information Systems Research* (23:2), pp. 721-737.