6-2017

Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks

Kai-Lung HUI
Hong Kong University of Science and Technology

Seung Hyun KIM
Yonsei University

Qiu-Hong WANG
Singapore Management University, qiuhongwang@smu.edu.sg

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

Kai-Lung Hui

Department of Information Systems, Business Statistics, and Operations Management
School of Business and Management
Hong Kong University of Science and Technology
Clear Water Bay, Hong Kong
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

Authors list in alphabetical order. We thank the seminar participants at the Erasmus University, ESSEC Business School (Asia Pacific campus), Hong Kong University of Science and Technology, Jyväskylä University, National University of Singapore, Seoul National University, Singapore Management University, University of Georgia, and Xi'an Jiaotong University, and the Workshop on Economics of Information Security and Workshop on Analytics for Business, Consumer and Social Insights for their helpful comments. We also thank Ross Anderson, Yuanyuan Chen, Richard Clayton, Avi Goldfarb, Ivan Png, Catherine Tucker, Wei T. Yue, and Alejandro Zentner, and the senior editor, associate editor, and reviewers for their constructive advice and guidance. A substantial part of this research project was completed when the third author was with the School of Management, Huazhong University of Science and Technology, China. This research was supported in part by the National Science Foundation of China project 71371082, the Hong Kong SAR General Research Fund project 16500715, and the Yonsei Business Research Institute. Corresponding author: Qiu-Hong Wang, qiuhongwang@smu.edu.sg.

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

Abstract

We estimate the impact of enforcing the Convention on Cybercrime (COC) on deterring distributed denial of service (DDOS) attack. Our data set comprises a sample of real random spoof-source DDOS attacks recorded in 106 countries in 177 days in 2004–2008. We find that enforcing the COC decreases DDOS attack by at least 11.8%, but a similar deterrence effect does not exist if the enforcing countries make a reservation on international co-operation. We also find evidence of network and displacement effects in COC enforcement. Our findings imply attackers in the cyberspace are rational, motivated by economic incentives and strategic in choosing attack targets. We draw related implications.

Key words: Cybercrime, deterrence, legislation, law enforcement, convention on cybercrime, distributed denial of service attack

1. Introduction

Cybercrimes cause a sizable loss to the world economy (Hayman 2013; McAfee 2014). One way to deter a socially undesirable behavior is to criminalize it. In many countries, policy makers and security specialists have been trying to fight cybercrime by establishing the corresponding legal frameworks and law enforcement agencies. However, compared with crimes in the physical world, cybercrime is less constrained by monetary and physical resources and can cause significant harms remotely. It is often difficult to identify and trace cyber criminals, assess the extents and impacts

of their offenses, and collect and analyze related digital evidence. Such global and virtual nature of cybercrime calls for collaborative international enforcement (Png et al. 2008).

Recognizing the importance of international co-operation, the Council of Europe drafted a new initiative, the Convention on Cybercrime (COC; Europe Treaty Series No. 185), which was adopted by the Committee of Ministers in 2001. The COC was the first international legislation against cybercrime. It provides a substantive legal framework to address any infringement against the confidentiality, integrity, and availability of computer data and systems, including common offenses such as distributed denial of service (DDOS) or malware attacks (Keyser 2003; Li 2007).

More importantly, the COC promotes mutual assistance across participating countries in handling traffic and stored computer data, which are the main traces of cybercrime. Supposedly, such international co-operation heightens the certainty and celerity of apprehending and convicting global cyber criminals and so should help deter cybercrime. However, some experts are skeptical about the COC because it reached consensus on what cybercrime is by making a vague definition, and it does not specify concrete enforcement mechanisms (Owens et al. 2009; Goldsmith 2011). Empirical evidence on the effectiveness of similar international legislations is scant. Accordingly, the key question remains: *Does the COC help deter cybercrime?*

The answer to this question is not trivial. The profile of cyber criminals is quite unique and different from conventional criminals in the physical world (Kshetri 2010). Cyber criminals tend to discount their chance of being punished. Skillful hackers often perceive only careless hackers are caught (Barnes 2004). Many cyber attackers are minors who face lighter sanctions than adults because most countries have separate legal systems for juvenile delinquency (Pipkin 2002). Minors may assess risks differently from adults. They tend to place a heavier weight on reward and short term consequence than risk and long term consequence (Steinberg 2003). Indeed, it has been

shown that a higher risk of penalty on young offenders does not reduce juvenile crimes (Singer and McDowall 1988; Steiner and Wright 2006). Many cybercrimes involve professional crime syndicates, which are less sensitive to apprehension and conviction than individual offenders (Kshetri 2010). Such crime syndicates are mostly dispersed geographically, meaning concerted international enforcement is necessary in confronting them.

Even if cyber criminals were similar to conventional criminals, the extant evidence has not unequivocally substantiated the effectiveness of law enforcement. The prior empirical literature has found contradictory evidence on the deterrence effects of criminal sanctions (Nagin 1998). Law enforcement may not deter crime because it can stigmatize people and stimulate defiant behaviors (Sherman 1993; Bouffard and Piquero 2010). This seems to be consistent with the emergence of radical online hacktivist groups such as Anonymous and Darkode.

With this backdrop, and the fact that the COC allows participating countries to selectively make reservations on certain provisions, it is important to investigate *empirically* if the COC can help deter cybercrime. In this study, we empirically estimate the impact of COC enforcement on deterring DDOS attack. We study DDOS attack because it is a popular cybercrime that can be carried out by a wide range of attackers, from script kiddies to professional hackers, and it poses a significant threat to the society (e.g., the estimated loss of revenue to DDOS attacks was $240,000 per day among business organizations and could be more than $100,000 per hour for retailers; see Neustar 2012). It is also well covered by various articles in the COC, such as those concerning data and system interference (Council of Europe 2013).

Our data set comprises records of real DDOS attacks targeting victims (computers) in 106 countries in 177 days in 2004–2008. We identify the impact of COC by exploiting its staggered enforcement over time and the nuanced differences in its adoption across countries. Unlike prior

studies which mostly analyzed processed data by law enforcement agencies or self-reported data by victims, our data were captured in real time by an independent third party. Therefore, we can offer a reliable assessment of crime deterrence from the field.

By conducting a battery of statistical tests, we find evidence of successful deterrence by COC enforcement. The number of IP addresses victimized by DDOS attacks decreases by at least 11.8% in the enforcing countries. This deterrence effect does not exist, however, if the enforcing countries make a reservation on international co-operation. We also find evidence of network and displacement effects. The enforcement is particularly effective when other countries also enforce the COC, but it may divert attacks to non-enforcing countries.

We make three important contributions. First, we provide pioneering evidence on whether international legislation helps curb cybercrime, which poses a significant challenge to the criminal justice system (Brenner 2006; Calderoni 2010). To tackle such emerging crime, we need quality empirical evidence to guide government policy. This study provides such quality evidence from an international panel of real offenses. Second, we provide a formal test of enforcement spill overs and find that cybercrime enforcement can be complementary and drives cyber attacks to non-enforcing countries. To our knowledge, such spillover effects across countries have not been systematically documented. Finally, we contribute to the understanding of hacker motivation. Analyzing "black hat" motivation is paramount to curbing the rampant increase in malicious cyber activities, but the lack of field data on hacker behavior has been a big obstacle (Mahmood et al. 2010). By analyzing the responses of real cyber attacks to COC enforcement, we indirectly infer that cyber attackers can be motivated by economics incentives and strategic in choosing attack targets, implying they are rational.

This remainder of this paper is organized as follows. Section 2 surveys the related literature and reviews the characteristics of the COC and DDOS attack. Section 3 develops the hypotheses. Section 4 describes our empirical model and data. Section 5 presents the statistical results. Section 6 discusses the implications. Section 7 concludes the paper.

2. Background

2.1. Related Literature

Our study is related to three streams of research. The first stream studies the deterrence effect of perceived threat and punishment (D'Arcy et al. 2009; Johnston and Warkentin 2010; Xue et al. 2011; Chen et al. 2012; Liang et al. 2013; Sojer et al. 2014; Chatterjee et al. 2015; Johnston et al. 2015). People who fear the threat and punishment against an improper behavior, such as IT misuse or non-compliance, are less likely to commit such behavior. This deterrence effect is observed mostly at the individual level in an organizational setting. It is unclear whether similar threat and punishment can deter cyber criminals, the identification of whom is difficult on the Internet (Ransbotham and Mitra 2009; Mahmood et al. 2010). Cyber criminals also tend to be more determined and less sensitive to near-term punishment (Kshetri 2010). Therefore, their responses to threat and punishment may differ from employees in a work setting.

The second related stream of research studies the strategic interaction between end-user protection and enforcement, and their benefits and trade-offs, against attackers (Cavusoglu et al. 2005; Cremonini and Nizovtsev 2009; Png and Wang 2009). Signalling protection at the end-user level can enhance deterrence, but attackers will strategically reallocate resources to attack users with less protection (Cremonini and Nizovtsev 2009). Enforcement may cause end-users to spend less effort in precaution, which can lead to less effective protection in equilibrium (Png and Wang

2009). The implication is that enforcement need not decrease the number of attacks and victims. This theoretical analysis is largely untested in a field setting.

The third related stream of research empirically examines the deterrence of conventional crimes in the physical world. Supportive evidence of crime deterrence exists in capital sanction and execution (Ehrlich 1973, 1977; Shepherd 2005; Yang and Lester 2008), gun-carrying laws (Lott and Mustard 1997; Bronars and Lott 1998), and enforcement against rape and other sexual offenses (Vaillant and Wolff 2009). However, counter evidence has also been recorded for similar enforcement, such as gun control and death penalty (Black and Nagins 1998; Ayres and Donohue 2003; Donohue 2004; Kirchgässner 2011). Besides the inconclusive findings, these studies focus on single-country enforcements. Such domestic enforcements may not be sufficient in deterring global cyber attacks involving multiple countries. Our research departs from this literature in that we empirically examine the effectiveness of enforcement against cybercrime with international co-operation (Li 2007; Kim et al. 2012).

In the specific domain of cybercrime, Png et al. (2008) find limited evidence of deterrence by domestic law enforcement. However, they find cybercrime displacement – U.S. enforcement against security violations could have caused attackers to initiate attacks from other countries. Their research calls for international co-operation against cybercrime. Our study examines whether such concerted international enforcement is effective and whether it generates any spillover effects on other countries (Kim et al. 2012).

To conclude, prior research suggests that enforcement and punishment should deter crime at the individual level, but the effect at the country level is unclear. The prior empirical evidence is mixed. Accordingly, the effectiveness of international enforcement against cybercrime is a non-

trivial empirical question. We address this question in a focused context, viz. COC enforcement, by scrutinizing real cyber attack data from a panel of 106 countries.

2.2. The Convention on Cybercrime

The COC is the first international legislation against criminal behavior in the cyberspace. It adopts a loose definition of cybercrime and so covers almost any malicious activities on the Internet, including DDOS attack. Besides the Council of Europe member states, four non-member states, viz. Canada, Japan, USA, and South Africa, participated in drafting it. The COC has been open for signature since 23 November 2001 and was first entered into force by Albania, Croatia, Estonia, Hungary, and Lithuania on 1 July 2014. As of December 2015, 49 countries have signed and 47 countries have enforced the COC. Figure 1 summarizes its signature and enforcement.

[Insert Figure 1 here]

The COC comprises four chapters.[1] The first chapter defines the terms. The second chapter specifies measures that need to be adopted at the national (domestic) level, including establishment of substantive criminal laws on offenses such as illegal access and interception, data and system interference, etc., the procedural laws, and jurisdictions over offenses. The third chapter contains principles of international co-operation such as extradition and mutual assistance. The last chapter allows participating countries to set the scope in terms of territorial application and reservation. In particular, Article 42 allows participating countries to reserve selected articles. These include, for national enforcement, selected provisions in criminalizing data interference (Article 4), misuse of devices (Article 6), child pornography (Article 9), infringement of copyright (Article 10), attempt and aiding or abetting (Article 11), power and procedures in criminal investigations and

[1] The full version of the COC and its explanatory report are available on the Council of Europe's Web site, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. [Accessed January 18, 2016]

proceedings (Article 14), and jurisdiction (Article 22) and, for international co-operation, mutual assistance in expedited preservation of stored computer data (Article 29). Article 42 also allows a federal state to reserve the right to assume the obligations under Chapter 2 (Article 41). Table 1 lists the countries with reservations. Among the 47 enforcing countries, 25 have made at least one reservation.

[Insert Table 1 here]

To enforce the COC, a signatory country has to bring its domestic laws into accord with COC's penal and procedural requirements. This is a significant undertaking and could delay the enforcement process. For example, the Finnish legislature had to add new provisions concerning information processing systems and possession of instruments used for cybercrime and establish the corresponding liability. The Swedish government had to harmonize laws regarding punishment of forgery, data interference, child pornography, unlawful use of computers and monitoring of computer information, and violation of copyright and related rights. The Japanese government had to change its laws to address the COC's data retention and provision requirements and general requests for co-operation in investigation (Li 2007).

The signatory countries may not have consensus on the definition of criminal offense either. For example, data interference as stated in Article 4 of the COC is considered a criminal offense in Denmark and France, but Azerbaijan, Lithuania, Slovakia, and USA have reserved the right to criminalize it only when it causes serious harms. This divergence in crime definition could impede the provision of mutual assistance across countries, which may cause further delay for a country to move from signature to enforcement. For example, Lithuania and Norway have reserved the right to refuse the request of any participating country for preserving stored computer data if the offense is not criminalized in both countries at the time of investigation.

In the empirical analysis, we include related developments in domestic law enforcement as a covariate. This helps increase the precision in identifying the impact of COC's unique provision of international co-operation in enforcement.

2.3. Distributed Denial of Service Attack

DDOS attack has been pervasive on the Internet. For example, a survey of IT professionals from 38 countries suggests 50% of the respondents have experienced business disruptions due to DDOS attacks (Kaspersky Lab 2015). The main reasons cited for the attacks were criminals seeking to disrupt operations (28%), disrupt or distract the business while another attack took place (18%), and use the attack to hold the company to ransom (17%). Competitors seeking to benefit from the attacks (12%) and political motivations (11%) were also commonly mentioned. In fact, many of these DDOS attacks targeted banks (24%), telecommunications companies (23%), and financial services organizations (20%), indicating they were possibly motivated financially.

It is notoriously difficult for individual organizations to defend against DDOS attack. The attacks are often launched from botnets in dispersed regions, making it challenging for victims to block the attack traffic. The attack tools are increasingly available too. It is now easy to launch a DDOS attack using just mobile devices, and DDOS attacks are available as online services amid the diversification of attack techniques (Symantec 2014). Today, we can "purchase" a DDOS attack online by simply specifying the target, duration, and magnitude. Hence, large-scale DDOS attacks have become an affordable tool for cyber criminals but a costly security issue for network operators (Zuckerman et al. 2010; Mansfield-Devine 2011).

The pervasiveness and global nature of DDOS attack make it an ideal candidate to study the effectiveness of international law enforcement. Our data set spans the second quarter of 2004

to last quarter of 2008. Hence, it pre-dates several prominent political disputes and cyber warfare, such as those between North Korea and South Korea and USA in 2009, between China and USA in 2013, and between Taiwan and Philippines in 2013.

3. Theory and Hypotheses

Our theoretical analysis is guided by two important theories in criminology, the general deterrence theory (GDT) (Gibbs 1975) and routine activity theory (RAT) (Cohen and Felson 1979). Both GDT and RAT view potential criminals as rational actors who would weigh the benefits and costs before committing a crime. GDT posits we can deter improper behaviors by raising the certainty and severity of punishment (Gibbs 1975). Previous research has shown that certainty and severity of punishment can help predict individual decisions on information systems misuse (D'Arcy et al. 2009), information security policy compliance (Chen et al. 2012), unethical IT use (Chatterjee et al. 2015), and unethical code reuse from the Internet (Sojer et al. 2014).

In general, the certainty and severity of punishment depend on the chance to apprehend and convict the criminal and the expected sanction. Chapter 2 of the COC requires participating countries to establish legislative and other measures against cybercrime, facilitate collection of evidence in electronic forms, and ensure any criminal offenses specified in the COC are punishable by effective sanctions. Chapter 3 also facilitates international co-operation and mutual assistance in cybercrime investigation. These provisions should strengthen the apprehension, conviction, and sanction of cyber criminals. Hence, at the individual level, GDT predicts the COC should decrease attackers' inclination to launch DDOS attacks against other people.

However, one essential assumption of GDT is that the punishment is salient, meaning we must be able to identify and track the criminals. This may be the case for conventional crimes such

as homicide, arson, or burglary for which forensic investigation can often help trace the criminals. The identification of criminals in the cyberspace is less trivial. Most DDOS attacks (and a broad range of cybercrimes) are launched from botnets or spoofed IP addresses which do not link to attackers' identities or physical locations. Hence, cyber criminals need not feel threatened by COC enforcement, which may undermine the applicability of GDT.

In any case, GDT omits structural elements in the environment that influence overall crime opportunities. By contrast, RAT, adopting a macro view of crime victimization, posits that crime is shaped by environmental factors, particularly the presence of a motivated offender and suitable target and the absence of a capable guardian (Cohen and Felson 1979). A crime is more likely to occur when these environmental factors converge in time and space. Unlike GDT, RAT does not focus on the criminal or punishment, or attempt to explain what motivates a person to commit a crime. Instead, it analyzes why some people are more likely victimized. RAT has been applied to explain improper IT use such as employee computer abuse, online identity theft, and unauthorized attempts on information systems (Willison and Warkentin 2013; Wang et al. 2015).

One core insight of RAT is that even if there is no structural change in crime motivation, the convergence of suitable targets and absence of capable guardians can lead to increased crime rates. The definition of guardians in RAT is broad. It may include "*someone whose mere presence serves as a gentle reminder that someone is looking*" and "*ordinary citizens going about their daily lives but providing by their presence some degree of security*" (Felson and Boba 2010, pages 28 and 37; see, also, Hollis-Peel et al. 2011). In our context, Articles 16–21 of the COC require participating countries to establish legal power to collect, preserve, search, seize, and intercept stored computer, traffic, and general content data. This implies any cybercrime related activities may be passively monitored in the enforcing countries, and network administrators, security staff,

or law enforcement agencies may serve as "social guardians" (Wang et al. 2015). RAT then implies COC enforcement should lead to fewer DDOS attacks in the country.

Overall, GDT and RAT are complementary in predicting crime occurrence (Tillyer 2011). GDT suggests heightened punishment can demotivate potential criminals at the individual level. RAT suggests the presence of guardianship from a macro view can help protect potential victims by discouraging motivated criminals. Together, they imply the COC will help deter DDOS attack if potential criminals are rational and aware of the heightened punishment and guardianship in the enforcing countries. How do we know these latter conditions are present?

We offer the following anecdotal observations. First, recent surveys find that cybercrime is mostly motivated by financial incentives (Kshetri 2010; McAfee 2014; Kaspersky Lab 2015), meaning attackers consider the potential benefits before committing a crime. This implies they are rational and may consider the cost in launching an attack (Kshetri 2006). Sporadic examples have indeed shown that hackers respond to enforcement (Rufo 2013).

Second, we have secondary observations that some attackers or would-be attackers do pay attention to the heightened punishment and guardianship due to COC enforcement. The following excerpts are extracted from one of the most popular hacker forums on the Internet. Apparently, the enforcement of the COC is well noted in the hacker community.[2]

- "*...Until 1 months ago I thought is no danger in hacking...I've got only a warning because I was under 18...then I realized...that was because we just joined...European Union and*

[2] The forum was the top-ranked site in the category "Hacking—Chats and Forums" in Alexa, which publishes comprehensive web traffic analysis on the Internet. In the month of October 2011, the forum had 58,332 unique active users, 9,320 new topics, and 74,590 new replies. Its global traffic rank was 4,647 in May 2013. Some posts in the forum mention law enforcement but took the opposite stance to argue why it may not be threatening. We list some of these posts in the Online Supplement.

there are new laws in IT...from now I take care because...it never knows when the cops catch you..." (posted by user "the_insane_eye" on July 2008).

- "*...the law follows the same guidelines for all countries in the european union and they're very strict about that,*" (posted by user "h4ck.in" on April 2010).
- "*There are conventions...within European Union borders he can be transported due to the crime, because of the European Unions conventions about partnership in law*," (posted by user "Aeternum" on March 2011).
- "*...I would rethink your theory on Croatia not having cybercrime laws: The cybercrime convention is a European directive to which Croatia is a member state...All of the offences proscribed in the Cybercrime Convention…are incorporated into the domestic legal framework,*" (posted by user "matemisic" on November 2011).

Third, enforcement against cybercrime is often publicized after COC enforcement. For example, a Russian was convicted for launching DDOS attacks against Estonia's government services in 2007 (Vamosi 2008). Estonia enforced the COC in 2004. A programmer was tried and convicted in USA in 2010 for crippling rollingstone.com with a DDOS attack involving 100,000 computers worldwide in 2008 (Goodin 2010). USA enforced the COC in 2007. A German was convicted for cyber extortion with threats of DDOS attacks against six online bookmakers in 2011. A similar DDOS attack was not against Germany's law in 2006 (Zorz 2011). Germany enforced the COC in 2009. The widespread reporting of these incidents should increase the salience of the punishment and guardianship brought by COC enforcement.

Taken together, our theoretical analysis, supplemented by anecdotal observations, points to a deterrence effect of the COC. This deterrence effect should lead to fewer victims observed at the country level. Our first hypothesis follows.

H1a: *COC enforcement reduces the number of DDOS attack victims in the enforcing countries*.

H1a results from a broad, conceptual application of GDT and RAT. As discussed above, the unique characteristics of cybercrime, particularly the difficulty in identifying and tracking attackers, may potentially inundate the COC's purpose. Accordingly, its empirical effectiveness may depend on the resources devoted to the enforcement (Stigler 1970). Effective enforcement calls for designated agents that take charge of investigation, apprehension, and conviction. Such agents are especially important for cybercrime because it often crosses jurisdictional boundaries and thus requires highly available and prompt investigations and proceedings, such as real-time interception and preservation of evidence. The deployment of designated agents also strengthens the guardianship which is an essential environmental factor in RAT.

In view of the importance of designated agents, the COC requires each enforcing country to establish an authority to take charge of all cybercrime-related investigations and proceedings on a 24/7 basis. Article 24 states "*each Party shall…communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty*." Article 27 states "*each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution*." Article 35 states "*each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence*." Article 25 allows requests for mutual assistance to be made by "*expedited means of communications, including fax or e-mail*."

In USA, the Computer Crime and Intellectual Property Section of the U.S. Department of Justice acts as the point of contact. France has established the Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication to implement Article 35 (Verdelho 2008). These authorities should increase the expected punishment and guardianship against cyber criminals. Therefore, if COC enforcement does reduce DDOS attack, then any delay in establishing the authority in charge should make the enforcement less effective, meaning there should be less reduction in DDOS attack. This begs the question: Why would any country delay establishing such an authority given its sanguine purpose?

The answer might lie in incentive and perceived effectiveness. A country may not want to respond to other countries' requests because it can take substantial effort to address the requests. For example, preserving and transporting a large volume of stored computer and traffic data (as stipulated in Chapter 3 of the COC) can be costly, and the cost may scale up rapidly as the number of enforcing countries increases. International co-operation may also be hampered by time zone difference. Even if a designated authority is in place, it may fail to provide the rapid responses needed for collecting and preserving the data and traffic involved in cybercrime. Disagreements on crime definition or differences in legal systems could further discourage a country from fully complying with the COC (Weber 2003; Li 2007; Verdelho 2008).

Perhaps anticipating such complications in adoption, the COC does not mandate when a participating country should establish the authority. It is unclear what will happen if a country does not respond to external requests. We observe staggered establishments of the authorities among the enforcing countries over time. This provides another testbed to study the relevance of COC enforcement to DDOS attack. Our second hypothesis is:

H1b: *Among enforcing countries, establishing the authority responsible for reacting to external requests for international co-operation reduces the number of DDOS attack victims more than those that have not established such an authority.*

The testing of H1b informs enforcing countries about the benefit of having a responsible authority. If the authority does contribute to decreasing DDOS attack, then it may be helpful for the enforcing countries to establish it in a timely manner.

One main challenge in enforcing the COC lies in harmonizing domestic legal frameworks with the COC's provisions. Because domestic legislative systems are often driven by complex interplays between culture, ethical standard, and political ideology, complying with all terms and conditions in the COC may not be viable for all countries. Hence, as discussed in Section 2.2, the COC allows participating countries to reserve the right in applying selected articles. This helps ease the burden of countries interested in joining the COC.

However, such reservations may threaten the COC's integrity. In particular, Chapter 3 of the COC mandates international co-operation, which is one of COC's most important objectives as it transcends the enforcement beyond domestic measures. Article 23 states "*the Parties shall co-operate with each other…through the application of relevant international instruments on international co-operation in criminal matters, … to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense*." More importantly, Article 29 mandates expedited preservation of stored computer data for mutual assistance. It states "*A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the*

search or similar access, seizure or similar securing or disclosure of the data," and "*Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law*."

Article 29 is "*probably one of the most widely used tools of the Convention*" (Verdelho 2008, page 30). For USA, the provision of such international co-operation is "*less clearly traceable to existing U.S. law*" (Weber 2003, page 437). Making a reservation on Article 29 will likely increase the difficulty of apprehending and convicting criminals located in other countries. As an example, with Article 29 in force, it will be easier to follow DDOS attacks involving botnets from multiple countries because all enforcing countries have an obligation to preserve, store, disclose, and facilitate the access of attack-related traffic in their countries. For attackers, making a reservation on Article 29 probably signals a lack of guardianship in the enforcing countries (cf. other enforcing countries that do not make the reservation). Hence, broadly speaking, we expect more victims in countries that have made the reservation.

Yet, the power of Article 29 could be limited because, by paragraph 7 of Article 29, any preservation request has to be made within a period of not less than 60 days. This could be too short for other countries to issue a formal request for mutual assistance (e.g., the procedure can take one year in France; see Verdelho 2008). If Article 29 has not been effectively utilized, then its reservation may not produce a material impact on cyber attack. In fact, complying with Article 29 can be costly for a country because it may require substantial revisions of related domestic laws. Hence, identifying the empirical impact of the reservation on Article 29 can inform policy makers about whether the international co-operation and mutual assistance as stipulated in the COC are important. Our next hypothesis follows.

H1c: *Reservation on Article 29 (expedited preservation of stored computer data) increases the number of DDOS attack victims in the enforcing countries.*

The testing of H1c provides a meaningful *indirect* assessment of the merit of international co-operation. As discussed in Section 2.2, COC enforcement is often preceded by adaptations of domestic laws. Accordingly, enforcement of the COC alone may not lend a powerful test to tease out its benefit due to international co-operation from the benefit due to domestic law enforcement. In addition to controlling for domestic law changes in the empirical model, the reservation on Article 29 provides another apparatus to identify the effect of international enforcement. Empirical support to H1c implies, specifically, the COC's promotion of international co-operation can help deter cybercrime.

Our last hypotheses concern enforcement spillover effects. A large body of research has shown that private investments in security can help reduce crime rates (Gonzalez-Navarro 2013; Zimmerman 2014), and such crime reduction effect may exhibit positive externalities (Ayres and Levitt 1998) and displacement (Png et al. 2008; Yang 2008; Kim et al. 2012). Technically, DDOS attacks, and a wide range of cybercrimes such as malicious code exploits and man-in-the-middle attacks, are routed through multiple Internet hops. For a target country to trace the attacks, we need to collect as much traffic as possible to reconstruct the attack sessions. It may be difficult to identify, locate, apprehend, and convict attackers without adequate collection of evidence. This, however, can be a challenging task if few countries enforce the COC.

As a hypothetical example, suppose an attacker from country A has conquered a botnet in countries B and C to launch an attack against a target in country D. Suppose further that countries B and D have enforced the COC but not countries A and C. Then, once the investigative agency in country D receives the attack report, it will have to first contact the counter-parties in countries

B and C to identify and locate the botnet. Country B will work with country D because the COC mandates international co-operation and mutual assistance. However, country C does not need to cooperate with country D. Country D may still be able to pin down the attack from country A based on the traffic provided by country B alone, but the quality of investigation will improve if country C also participates. Finally, country A's assistance will be necessary to convict the attacker, but it need not offer such assistance to countries B, C and D.

In this example, the probability of locating, apprehending, and convicting the attacker will increase if countries A and/or C also enforce the COC. Hence, similar to many technologies and standards that exhibit network effects, the COC should be more effective in deterring cybercrime when more countries adopt it (cf. each country relying on its own domestic legislations). The more countries enforcing the COC, the broader its coverage, and the higher the perceived risk faced by attackers. Following the spirits of GDT and RAT, the perceptions of punishment and guardianship should be stronger as more countries enforce the COC.

H2a: *The effect of COC enforcement on the number of DDOS attack victims in the enforcing countries is stronger as the enforcement in other countries increases.*

If the COC indeed raises the perceived punishment to attackers or perceived guardianship around potential victims, then two outcomes may occur. The first outcome is attackers scaling back their attacks. The second outcome, which may apply more to undeterred people, is attackers choosing targets so that their chance of being caught and punished is lower. In our setting, with international co-operation in enforcement against cybercrime, *ceteris paribus*, the risk to attackers will be lower if they attack targets in countries not enforcing the COC. The attackers may still be apprehended and punished if the target countries have domestic enforcement against cybercrime, but their risks of facing cross-border investigation, extradition, and offshore trials will be lower in

non-enforcing countries. Hence, we expect undeterred attackers will shift some of their attacks from COC to non-COC countries.

Realistically, both outcomes will likely occur. The first outcome, viz. attackers lessening their offenses, will cause a decrease in attack rate in the empirical data, leading to support of H1a–H1c. The second outcome, viz. attackers strategically shifting attacks from enforcing countries to non-enforcing countries, gives rise to our last hypothesis:

H2b: *Enforcement of the COC will cause cybercrime displacement; non-enforcing countries will receive more DDOS attacks as the enforcement in other countries increases*.

H2a and H2b are important because they formally assess the externalities in international cybercrime enforcement. Such externalities need to be noted and addressed for any international treaties or enforcement to achieve their best purposes.

4. Model and Data

To empirically test the hypotheses, we use a panel fixed-effects model:

$$r_{it} = f(\cdot) + \beta_1 L_{it} + \beta_2' x_{it} + \beta_3' \mu_i + \beta_4' \tau_t + \beta_5' \gamma_{it} + \varepsilon_{it}, \quad (1)$$

where r_{it} denotes the cyber attack rate in country i in day t, $f(\cdot)$ captures COC enforcement in country i in day t (see below), L_{it} is the cumulative number of domestic cybercrime legislations, x_{it} are control variables, μ_i are country fixed effects, τ_t are time (day) fixed effects, γ_{it} are country-specific time trends, and ε_{it} are idiosyncratic random errors.

The country fixed effects, μ_i, account for unobserved time-invariant heterogeneity, such as culture and political systems. The time fixed effects, τ_t, account for time-related shocks that apply to all countries, such as seasonality in DDOS attack or advances in hacking or defense techniques. We include country-specific time trends, γ_{it}, to allow for different trends of DDOS attack across

countries. We construct the trend as the number of calendar days starting from the first day in the sample, so, day = 1 for 26 May 2004, day = 2 for 27 May 2004, and so on. Altogether, we include 106 such time trend variables, one for each country in the sample.

To test H1a, i.e., the direct effect of the enforcement, we parameterize $f(\cdot)$ by an indicator, K_{it}, that equals 1 if the COC entered into force in country *i* in day *t*, and 0 otherwise. To test H1b, i.e., the effect of the responsible authority, we parameterize $f(\cdot)$ by two indicators, each denoting the enforcement status with or without the responsible authority. To test H1c, i.e., the effect of the reservation on international co-operation, we parameterize $f(\cdot)$ by multiple indicators that denote whether a country has made different reservations, including Article 29 on expedited preservation of stored computer data. To test H2a and H2b, i.e., the spillover effects in COC enforcement, we parameterize $f(\cdot)$ by the following two-way interaction function:

$$f(\cdot) = \alpha_1 K_{it} + \alpha_2 \omega_{-i,t} + \alpha_3 K_{it} \omega_{-i,t}, \quad (2)$$

where $\omega_{-i,t}$ measures the extent of COC enforcement in other countries. With this specification, α_1 captures the direct enforcement effect. α_2 captures whether the enforcement in other countries affects the attacks recorded in country *i*, and so provides an estimate of the displacement effect (H2b). α_3 captures whether this effect due to others' enforcement would differ if country *i* has also enforced the COC. Therefore, $\alpha_2+\alpha_3$ provides an estimate of network effect (H2a).

We compiled our data from multiple sources. To measure the cyber-attack rate, r_{it}, we obtained backscatter data sent by DDOS attack *victims* from the Cooperative Association for Internet Data Analysis (CAIDA 2005–2008a). CAIDA administers a global network comprising roughly 1/256th of all IP addresses in the world to record unsolicited Internet traffic, including spoof-source DDOS attacks. Each of these backscatter packets contains the victim's IP address,

which allows us to identify its country. By tracking the backscatter packets and their origins, we can study the change in DDOS attack victims over time and across countries.

The CAIDA data set is a random sample of unsolicited Internet traffic and captures only attacks that randomly spoofed the source IP addresses. Hence, it allows us to identify DDOS attack victims, not attackers, and does not include the full details of each attack, such as the total number of packets involved or size of payload data used. Further, due to the excessive volume, CAIDA releases only several days of data in each quarter. Figure 2 provides a graphical illustration of the backscatter data.[3] Table 2 reports the periods when the CAIDA data are available.

[Insert Figure 2 and Table 2 here]

Despite these limitations, Mao et al. (2006) shows that backscatter data match the patterns of general large-scale DDOS attacks well. The use of backscatter data to measure DDOS attack is common in computing studies (Moore et al. 2001; Balkanli et al. 2015). From the backscatter data, we compute the number of victim IP addresses per Internet host by country and day as the dependent variable in all statistical estimations.

Next, from Council of Europe's (COE) website, we compiled the signing and enforcement status of the COC and, also, the reservation of any articles therein by all countries in our data set. We compiled the enforcement of Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms (CPHRFF) and use it as the instrumental variable in one of our identification strategies. To measure domestic enforcement, L_{it}, we compiled developments in domestic cybercrime legislations from Asian School of Cyber Laws (ASCL), COE, International

[3] For more details of the CAIDA data set, see http://www.caida.org/projects/network_telescope/. An animated illustration of backscatter data is available at http://www.caida.org/publications/animations/passive_monitoring/backscatter.mov. [Accessed January 18, 2016]

Telecommunications Union (ITU), and United Nations Office on Drugs and Crime (UNODC). We report the details in compiling the domestic legislations in the Online Supplement.

For control variables, x_{it}, we compiled demographic data from Global Market Information Database (GMID) and Central Intelligence Agency (CIA). For socio-economic development, we have unemployment rate, gross domestic product in purchasing power parity rate, and the number of higher education students (Korgaonkar and Wolin 1999). For Internet landscape, we have the numbers of Internet hosts, Internet users, and integrated services digital network subscribers and the percentage of digital main lines. We include the countries' land areas as a proxy for the need for communications networks between people. Except for unemployment rate and percentage of digital main lines, we convert all demographic variables to per-capita term.

To measure the effectiveness of jurisdictional systems and quality of enforcement agencies, we obtained six indicators from Worldwide Governance Indicators (WGI): control of corruption, government effectiveness, political stability and absence of violence/terrorism, regulatory quality, rule of law, and voice and accountability (Kaufmann et al. 2010). Each of these six indicators is normalized over all countries in the world and varies on a yearly basis.

Finally, referring to equation (2), to measure $\omega_{-i,t}$, i.e., the extent of other countries' COC enforcement, we obtained autonomous connection (AS) data from CAIDA (2008b). AS connection is commonly used in the computing literature to capture the routes for launching DDOS attacks (Moore et al. 2006; Chen et al. 2007; Soundar Rajam et al. 2013). By tracking AS connections, we can capture the scope of other countries' COC enforcement. We provide more details about AS connection and the estimation of equation (2) in Section 5.

Taken together, our data set contains information on DDOS attack victims in 106 countries over 177 days in 2004–2008 and the corresponding countries' characteristics (COC enforcement

status, domestic cybercrime legislations, demographics, and governance quality indicators). Table 3 lists the 106 countries in our sample. Table 4 presents the descriptive statistics, which are further grouped by COC enforcement status in Table 5. For example, in Bosnia and Herzegovina, France, Norway, and Ukraine which enforced the COC in 2006, the number of victims per 1,000 Internet hosts has decreased by 92%, from 0.829 (pre-2006) to 0.064 (post-2006). By contrast, the decrease was only 76%, from 5.047 (pre-2006) to 1.210 (post-2006), among the non-enforcing countries. Generally, the decrease in number of victims was sharper in the 23 enforcing countries than the 83 non-enforcing countries. Table 6 reports the variable correlations.

[Insert Tables 3–6 here]

Referring to Table 4, on average, there were 2.216 unique victim IP addresses per day for every 1,000 Internet hosts in each country, but the variation was substantial. Senegal had the most significant attack on 24 May 2006, with 256 victim IP addresses out of a total of 412 Internet hosts. 23 countries have enforced the COC in 2004–2008 and, among them, 12 have made reservations and 10 have delayed establishing the authority after the dates of entry into force.

Figure 3 plots the average log numbers of victim IP addresses per 1,000 Internet hosts per country per day in each quarter in countries that have enforced and not enforced the COC by 31 December 2008, and their differences, over time. In general, the attack trends are similar, but the enforcing countries had mostly fewer victims than the non-enforcing countries. The difference in number of victims was increasing over time, which is consistent with the presence of network and displacement effects as posited in H2a and H2b. Together with Table 5 which shows that the number of victims has decreased more sharply in the enforcing countries than non-enforcing countries after the year of enforcement, we have cross-sectional and longitudinal model-free evidence that COC enforcement is negatively correlated with DDOS victimization.

[Insert Figure 3 here]

Except for index and percentage variables, we log-transform all continuous variables as the double-log specification often fits the data better (Wooldridge 2006, p. 197-200). We add one as necessary to avoid logarithm of zero. Further, DDOS attacks may exhibit cross-sectional or spatial interdependency due to their global nature (Kim et al. 2012). So, in all regressions, we incorporate spatial correlation-consistent standard errors, which can accommodate general heteroskedasticity and spatial autocorrelations (Driscoll and Kraay 1998).

5. Results

Table 7, column (1) reports a panel fixed-effects regression which allows for spatial correlation-consistent standard errors and includes the COC enforcement ($K_{it} = 1$ if country i has enforced the COC in day t, and = 0 otherwise) and all domestic legislation and demographic variables. The cumulative number of domestic cybercrime legislations helps reduce the number of DDOS attack victims in the country. On top of it, the coefficient of COC enforcement is –0.125 (s.e. 0.028) and statistically significant. Because we use a double-log specification, the coefficient corresponds to the elasticity. Accordingly, in our sample of 106 countries (see Table 3) and 177 days in 2004–2008 (see Table 2), enforcement of the COC has led to a $-(e^{-0.125} - 1) = 11.8\%$ *decrease* in DDOS attack victims. Given the potential losses of organizations to DDOS attacks, this is economically significant. Referring to Table 4, it implies the enforcement could have reduced $2.216 \times 11.8\% = 0.261$ victims per 1,000 Internet hosts, or 96 victims, per country per day.

[Insert Table 7 here]

The coefficients of the demographic variables exhibit various signs and significance. As reported in Table 6, many of these variables, particularly the six governance quality indicators, are

highly correlated. Therefore, their coefficients should be interpreted with caution. In any case, we include them to capture variations in DDOS attacks due to observable national characteristics which, if omitted, may confound the effect of COC enforcement. Their own signs and significance are of less importance.

The estimate in Table 7, column (1) accounts for domestic law enforcement measured by the cumulative number of domestic cybercrime legislations over time. Evidently, each domestic legislation may serve a different purpose. Simply adding them up may not accurately measure the progress in domestic enforcement. In Table 7, column (2), we report another estimate that replaces the cumulative number of domestic cybercrime legislations by an indicator that equals one on or after the date when a country enforced the *first* domestic cybercrime legislation, and zero otherwise. Essentially, this indicator separates the time for each country into two periods, one without any domestic cybercrime legislation and the other with at least one domestic cybercrime legislation. As shown in the Online Supplement, the mean of this indicator variable is 0.509, meaning close to half of our sample observations were not covered by any domestic cybercrime legislation in 2004–2008.

The statistical results are largely similar. The coefficient of COC enforcement continues to be negative and significant. However, its magnitude has increased (–0.133 vs. –0.125) whereas the magnitude of the coefficient of first domestic cybercrime legislation is considerably smaller than that of the cumulative number of domestic cybercrime legislations (–0.084 vs. –0.231) in Table 7, column (1). This suggests, using an imprecise variable to measure domestic enforcement, the COC enforcement variable, K_{it}, could have picked up some effects due to the domestic enforcement. In view of this potential bias, in the remaining analysis we revert to using the cumulative number of domestic cybercrime legislations, which provides a finer differentiation in domestic enforcement.

Technically, the COC enforcement variable, K_{it}, captures the changes in number of DDOS attack victims after the enforcement among the enforcing countries. Accordingly, our specification shares a similar spirit as a difference-in-differences (DID) model. However, our "treatment," i.e., COC enforcement, is applied to the enforcing countries at different time, whereas in a typical DID model the treatment is applied to multiple cross-sectional units at the same time.

We next buttress our estimation with several robustness tests. COC enforcement could be endogenous. A country could have chosen to enforce the COC because it experienced more attacks (Ehrlich and Brower 1987). This endogeneity (due to reverse causality), if present, should bias the coefficient of COC enforcement *upward*, i.e., the coefficient should become more *positive* than its true value. Because we find a negative coefficient for COC enforcement in Table 7, column (1), H1a is supported even if COC enforcement is subject to this endogeneity.

To formally address this endogeneity (and other unknown sources of bias), we conduct an instrumental variable (IV) estimation using the enforcement of Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, which was also drafted by COE and opened for signature at around the same time as the COC, as the instrument. The identification assumption is that the country characteristics leading to the enforcement of COC and CPHRFF are likely similar, but the enforcement of the latter should be related to general developments in human rights and freedom and so should not relate to DDOS attack. Hence, CPHRFF enforcement should help us prune the endogenous variations and establish the causal influence of COC enforcement on DDOS attack. This IV estimator, using CPHRFF as the instrument, should also help address the potential bias, if any, due to imprecise measurement of domestic enforcement.

We perform the IV estimation using two-stage least squares (2SLS) regression. The first-stage regression with the COC enforcement indicator as dependent variable has a high R-square,

0.609. The coefficient of CPHRFF enforcement is 0.100 (s.e. 0.014) and statistically significant ($p < 0.01$). Hence, CPHRFF enforcement is a relevant instrument. For brevity, we do not report the first-stage regression results. Table 7, column (3) reports the second-stage regression. As expected, the coefficient of COC enforcement becomes *more negative*, –1.160 (s.e. 0.473), and continues to be statistically significant. This indicates the true effect of COC enforcement could be considerably larger than that reported in Table 7, column (1).[4]

Despite the 2SLS results are consistent with our expectation, we hesitate in using it as our main specification. The effect, $-(e^{-1.160} - 1) = 68.7\%$ decrease in number of DDOS attack victims, is substantially bigger than our earlier estimate of 11.8%. Given this is the first estimation of the COC enforcement effect, we prefer to use a more conservative estimate in drawing the conclusions and insights. Further, we cannot find suitable instruments for some of our subsequent estimations. Hence, to ensure the results are comparable across estimates, we use the specification in Table 7, column (1) as the "preferred" estimate in the remaining discussion. We emphasize our estimated impact is conservative as it is subject to endogeneity and so is biased upward.

We next conduct a falsification test. A country can sign without enforcing the COC. Such signature is symbolic and hence should have a weaker effect on DDOS attack. If, however, the COC effect found above is spurious and caused by unobserved country characteristics related to the participating countries' political systems or their general attitude to law enforcement, then the coefficient of COC signature may also be statistically significant.

Table 7, column (4) reports an estimate replacing COC enforcement by COC signature (= 1 if country *i* has signed the COC in day *t*, and = 0 otherwise). The coefficient of COC signature

[4] The Hausman test gives unstable results, possibly caused by non-positive semi-definite estimated parameter differences (Schreiber 2008). Accordingly, we conduct the Davidson-McKinnon test, which is a common alternative procedure to test for endogeneity when the Hausman test does not behave. The Davidson-McKinnon test statistic is 5.12 ($p < 0.05$), indicating that the ordinary least squares estimator may not be consistent.

is negative but much smaller, –0.014 (s.e. 0.070) and, most importantly, not statistically significant. Hence, using the same data set and specification, we do not obtain a significant negative impact if we simply replace COC enforcement by COC signature. This confirms our finding is specific to the COC enforcement "treatment".[5]

Taken together, the results in Table 7, columns (1) to (4) provide robust evidence to support H1a, i.e., the direct impact of COC enforcement on the number of DDOS attack victims. We next assess H1b and H1c. Table 7, column (5) reports an estimate similar to the preferred estimate in Table 7, column (1), except two changes: i) we split the COC enforcement variable into two, one with the responsible authority to react to external requests for international co-operation and the other without, and ii) we include the number of articles reserved by the enforcing countries as an additional covariate. Consistent with H1a, COC enforcement always has a negative impact after controlling for domestic enforcement. Consistent with H1b, the enforcement with the responsible authority has a more negative impact, –0.160 (s.e. 0.040), than the one without, –0.131 (s.e. 0.044), but their difference is not statistically significant ($F = 0.47$, $p = 0.49$). The coefficient of the number of reservations is positive, 0.019 (s.e. 0.021), but not statistically significant.

To more precisely test H1c, we split the reservations into four sets. The first set, "domestic enforcement," comprising reservations on Articles 4, 6, 11, 14, and 22, concerns definitions of offenses in accordance with domestic laws, the procedural provisions, and the establishment of jurisdictions. The second set, "mutual assistance," comprising reservation on Article 29, concerns the preservation of stored computer data for other countries, which can be helpful for cross-border

[5] So far, all the tests rely on cross-sectional variations across countries and, also, longitudinal within-country variations in COC enforcement. In one unreported test, we limit the sample to only countries that have enforced the COC in 2004–2008 and so focus on within-country variations in the treatment. The coefficient of COC enforcement continues to be negative, –0.171 (s.e. 0.031), and statistically significant. In another unreported test, we limit the sample to only countries in Council of Europe (which initiated the convention) and obtain similar findings. The coefficient of COC enforcement is –0.140 (s.e. 0.030).

crime investigation. The third set, "DDOS irrelevant," comprising reservations on Articles 9 and 10, concerns non-DDOS attack offenses, viz. child pornography and infringement of copyrights. The fourth set, "federal clause," comprising reservation on Article 41, concerns the obligations among federal and member states.

Table 7, column (6) reports the estimate. Only "mutual assistance" (i.e., Article 29) has a statistically significant impact on the number of DDOS attack victims. In fact, its coefficient, 0.301 (s.e. 0.071), corresponding to an elasticity of $e^{0.301} - 1 = 35.1\%$, is considerably bigger than the impact of COC enforcement itself (–0.142 and –0.185, corresponding to elasticities of –13.2% and –16.9%). This implies COC enforcement deters DDOS attack mostly by facilitating international co-operation in expedited preservation of stored computer data.

Note that the last set of reservation, "federal clause," is applicable only to countries with a federal system. In our data set, only USA has made this reservation. USA is also a frequent target for cyber attacks. Hence, we check if our results are robust to excluding USA from the sample. Table 7, column (7) repeats the estimate without USA. The result is similar. Only the reservation on "mutual assistance" has a statistically significant positive impact.

We now test our second set of hypotheses concerning how COC enforcement affects other countries. H2a posits that the deterrence effect of COC enforcement on DDOS attack is stronger as the other countries' enforcement increases. H2b posits COC enforcement will divert attacks to non-enforcing countries. As shown in Figure 1, the global enforcement of the COC is staggered over time. Hence, if H2a and H2b are correct, we expect the difference in the number of DDOS attack victims between enforcing and non-enforcing countries to widen over time. This is indeed the case as shown in Figure 3.

A simple way to statistically test H2a and H2b is to incorporate a more flexible structure that allows for varying enforcement effect. In the next specification, we split the COC enforcement variable into five according to the time since the enforcement became effective. For example, if country A has enforced the COC on 1 April 2005, then "first year of enforcement" equals one only on the days from 1 April to 31 December 2005 and 0 otherwise, "second year of enforcement" equals one on all the days in 2006, and so on. Similarly, if country B has enforced the COC on 1 July 2007, then "first year of enforcement" equals one only on the days from 1 July to 31 December 2007 and 0 otherwise, "second year of enforcement" equals one on all the days in 2008. All other "year of enforcement" variables equal 0 for country B.

The advantage of splitting the COC enforcement variable this way is that it allows for the changing enforcement impact due to network (H2a) and displacement (H2b) effects. At the same time, it accommodates the possibility that the participating countries may need time to impose the enforcement measures. As reported in Table 8, column (1), the coefficient of COC enforcement is consistently negative and increasing in magnitude over time. A Wald test indicates the five "year of enforcement" coefficients are statistically different ($F = 14.07$, $p < 0.01$). Hence, consistent with the predictions of H2a and H2b, as more countries enforce the COC over time, the difference in the number of DDOS attack victims widens between the enforcing and non-enforcing countries.[6]

We next exploit the topology of the Internet to devise a direct test of H2a and H2b. The Internet is organized into thousands of autonomous systems, each of which is a connected network with a unique AS number and belongs to one country. In general, an Internet host can connect to

[6] In an unreported test, we split the COC enforcement variable in Table 7, column (1) into five, each corresponding to the enforcement effect in one year. The result once again points to a more salient enforcement effect over time. For brevity, we report the detailed statistical results in the Online Supplement. Note that this test is less precise than the one reported in Table 8, column (1) because it does not account for the possibility that it may take time for a country to fully enforce all the measures mandated by the COC. The individual enforcement may be badly measured in the early years because of the few number of enforcing countries, contributing to the weaker results.

another Internet host from a different AS provided the two AS have a direct business relationship. Hence, the number of business relationships between a country's AS with other countries' AS measures the country's external Internet connectivity (Moore et al. 2006).

Conceptually, the number of AS connections from a country to other countries is analogous to the number of "windows" that it has to the external world. If COC enforcement exhibits network (displacement) effect, then having more AS connections to other enforcing countries should lead to *fewer* (*more*) attacks in an enforcing (a non-enforcing) country. This is because, owing to the COC's promotion of international co-operation, the risk of being tracked and punished in attacking an enforcing (a non-enforcing) country will be higher (lower) if the attack originates from or is routed through another directly connected enforcing country.

Essentially, AS connections serve as "windows" from which attackers can break in. The better these windows are guarded, the less likely a country will be targeted, and the more likely undeterred attacks will be redirected to countries with less guarded windows. This consideration of the role of AS connection is consistent with RAT, which suggests guardianship is one important environmental factor for crime victimization.

We compute the percentage of AS connections to *other* enforcing countries as the number of AS connections to other enforcing countries divided by the number of AS connections to all other countries. Referring to equation (2), with this specification, the percentage of AS connections to other enforcing countries allows us to test the displacement effect (H2b). By interacting it with COC enforcement, we can test whether the impact of enforcement in a country varies with others' enforcement, i.e., whether network effect exists (H2a).

Table 8, column (2) reports an estimate including the percentage of AS connections to other enforcing countries and its interaction with COC enforcement. COC enforcement continues to

have a statistically significant negative impact on the number of DDOS attack victims. Importantly, the coefficient of the percentage of AS connections to other enforcing countries is positive, 0.171 (s.e. 0.063), and statistically significant. Its interaction with COC enforcement is negative, –0.427 (s.e. 0.089), and statistically significant. These estimates imply an increase in AS connections to other enforcing countries by one per cent point could have *increased* the number of DDOS attack victims by 0.17% in a non-enforcing country, and *decreased* the number of DDOS attack victims by –(0.171 – 0.427) ÷ 100 = 0.26% in an enforcing country. They support the presence of both network (H2a) and displacement (H2b) effects in COC enforcement.

To further scrutinize these spillover effects from other countries' enforcement, we split the countries into two sets, those that have and have not enforced the COC in 2004–2008. Table 8, columns (3) and (4) show that, indeed, the effect of other countries' enforcement (measured by the percentage of AS connections to other enforcing countries) is *negative* in the enforcing countries and *positive* in the non-enforcing countries. Therefore, by applying the same specification to two different sets of countries, we find completely opposite effects of other countries' enforcement. Such spillover effects in COC enforcement are remarkable.[7]

Table 9 summarizes the hypothesis testing results. We find significant deterrence effect of COC enforcement on DDOS attack, but this deterrence effect does not exist if an enforcing country makes a reservation on international co-operation. COC enforcement generates spillover effects. It decreases attacks as the enforcement in other countries increases, but increases attacks to non-enforcing countries. H1a, H1c, H2a, and H2b are supported, but not H1b.

[7] For completeness, we consider if these spillover effects are affected by domestic enforcement. In another estimation, we add the percentage of AS connections to other countries with domestic cybercrime legislation and its interaction with COC enforcement as additional covariates to the specification in Table 8, column (2). The results are consistent. the coefficient of the percentage of AS connections to other enforcing countries is positive, 0.221 (s.e. 0.067), and statistically significant. Its interaction with COC enforcement is negative, –0.592 (s.e. 0.090), and statistically significant. For brevity, we report this estimate in the Online Supplement.

6. Discussion

Our statistical evidence points to the conclusion that attackers in the cyberspace are rational. They respond to heightened law enforcement by either forgoing their attacks or shifting attacks to non-enforcing countries. This rationality suggests that we can restraint cybercrime by economic means (cf. technical means such as using advanced security intelligence systems). If cyber criminals care about the expected punishment, then they may also consider the direct costs involved in launching an attack (Katyal 1997). Such direct costs may include, for example, the costs in acquiring related software (e.g., traffic generators for DDOS attacks), subscribing Internet access with dynamic IP addresses, or concealing their physical whereabouts (e.g., by using computers in an Internet café to launch attacks). Increasing these direct costs, such as taxing software that can potentially be used in cyber attacks or Internet services with dynamic IP addresses, or mandating the registration of visitors to Internet cafés, may help dissuade people from attacking others.

Practically, how significant is COC enforcement? Our various estimates imply an elasticity of around 11.8% to 68.7%. In the USA, there were around two million unique victim IP addresses in our data set. Hence, for USA alone, these estimates could mean hundreds of thousands or even a million fewer victims. A research commissioned by Verisign indicates that among 19 companies with annual revenues exceeding one billion dollars, the loss in revenue due to DDOS attacks ranges from 0.2 to 10 million dollars per hour (Forrester Consulting 2009). A survey by HP Enterprise Security shows that the annualized cost of DDOS attacks was around $172,238 per incident (Ponemon Institute 2012). Many victims in our data set are probably non-commercial and have smaller scales of operations than the companies included in these surveys. Even with this proviso, however, the potential benefit from COC enforcement seems large.

More importantly, cybercrime generates opportunity costs. The government and business organizations need to spend resources into securing themselves. These resources can be put into better use if there is no cybercrime. The total addressable market for cyber security products and services added up to 58 billion dollars in 2013, and cybercrime causes a total loss of up to 1.5% of a country's gross domestic product (McAfee 2014). Many cybercrime-related opportunity costs, such as the procurement and operation of protection technologies and mandate of security audits and contingency planning, are incurred on an ongoing basis. Hence, they can scale up in the long run. Besides, any technical or preventive measures against cybercrime will only contain the *ex post* damage but not *ex ante* opportunity costs. Given the significant deterrence effect identified in this study, we propose law enforcement as a more economical *ex ante* solution to cybercrime. Law enforcement also enjoys significant economies of scale. The same law should apply to any number of organizations or individuals in the country.

The pursuance of deterrence instead of preventive measures is particularly timely because conventional preventive measures against cyber attacks, such as bandwidth over-provisioning or perimeter controls (which are often used to defend against DDOS attack), seem to be gradually losing the battle because of the rapid development in hacking technologies (Forrester Consulting 2009). Deterrence by law enforcement is less sensitive to this development. As the COC illustrates, the terms and offenses can be defined broadly to cover a wide range of behaviors instead of the use of hacking technologies *per se*. Deterrence by law enforcement has another advantage – in addition to tackling threats from external parties, it curbs malicious insider threats which are often difficult to anticipate and preempt, and which are on the rise globally (Vormetric 2013).

The significant positive effect of reservation on preserving stored computer data for other countries, i.e., "mutual assistance" (H1c), on DDOS attack is illuminating. It implies attackers are

concerned about international co-operation. Any divergence in concepts or attitude towards crime or political ideology across countries could be exploited by criminals to evade prosecution. Hence, it would help if the countries can work closer together. As of 31 December 2015, only 47 countries have enforced the COC, and 13 of them have made a reservation on Article 29 mandating mutual assistance in expedited preservation of stored computer data for other parties. Obviously, there is room to enhance deterrence through international co-operation.

In fact, if concerted global enforcement cannot be reached, then selected enforcement by a subset of countries may produce ambiguous effectiveness on cybercrime deterrence. Our analysis of H2a and H2b implies attackers, other than being rational, are also strategic. They may redirect attacks to countries with less enforcement when facing higher risks of being held accountable for their attacks. Such diversion of attacks to other countries is particularly feasible for cybercrime (cf. conventional crimes in the physical world) because of its primary use of electronic means for aggression. Table 8, columns (2)–(4) show that COC enforcement is all the more beneficial when other countries have enforced it because the enforcement is complementarity. Evidently, we face a coordination problem *a la* Prisoners' Dilemma. Facilitating countries to come into agreement in criminalizing malicious user behaviors and international co-operation is key to achieving global deterrence of cybercrime.

Our research also echoes the importance of studying strategic hacker behavior (Png et al. 2008; Cremonini and Nizovtsev 2009; Hui et al. 2012). The defender has choices on how to deter cyber attacks, but attackers also have choices on which targets to attack. Estimating the elasticity of substitution or "cross-enforcement" elasticity of cybercrime will be an important step towards devising an effective program against cybercrime. We defer such estimation to future research.

Finally, although we study only DDOS attack, our insights apply to other cybercrimes. It is difficult to track the identities of random spoof-source DDOS attackers. If the COC can deter DDOS attack despite this difficulty, then it should deter other cybercrimes that are more readily traceable, such as cyber extortion or international syndicates of cash mules.

6.1. Limitations

There are a few limitations in this study. First, we can identify victims but not attackers, and so we can infer the effectiveness of crime deterrence only from victim-side data. Future research should establish direct, complementary evidence from attacker-side data. Second, our data set contains only packet headers but not the payload data. Hence, we cannot ascertain the methods used for the attacks, or whether the attacks aimed at depleting the victims' bandwidths or computing resources. Third, we study one kind of cyber attack, viz. random spoof-source DDOS attack. Future research should triangulate our findings with other cybercrimes. Finally, we consider only the first step of enforcement, i.e., legislation. Future research should consider whether other enforcement factors such as the actual manpower deployed to police malicious online activities or facilitate criminal trials would moderate the impact of such legislation at the global scale.

7. Conclusions

We find that COC enforcement is effective in deterring random spoof-source DDOS attack. We find evidence that this deterrence comes primarily from the COC's provision on international co-operation, and there is network effect in the enforcement. The enforcement has led to an average reduction of at least 11.8%, and could be up to 68.7% of DDOS attacks in the enforcing countries.

However, it could have diverted attacks to non-enforcing countries. Our findings provide strong indication that cyber criminals are rational and strategic.

Our work can be extended in several meaningful ways. It is helpful to explore if the COC effect is moderated by country characteristics, such as technical infrastructure or political systems. It would also be interesting to see if there is any lag in the enforcement effect. Directly observing attacker behavior may help devise new means of deterrence that can complement law enforcement. Within the COC framework, it is meaningful to explore if facilitating victim precaution (Png and Wang 2009) could complement law enforcement to reduce cyber attacks in an empirical setting. Finally, given only 47 out of nearly 200 countries in the world have enforced the COC, it would be interesting to study what affects its adoption. Such a study may provide valuable guidance to future developments of international legislation.

The growth of cybercrime is staggering and causes significant loss to the global economy (McAfee 2014), but the solution so far seems to be passive. Many technical counter-measures such as advanced detection or security perimeters are devised or tuned after new attacks have emerged (Kim and Kim 2014). To preempt new cybercrimes, the government can be more proactive in dis-incentivizing potential attackers from entering a hacking career. Unfortunately, a single country's effort is far from being sufficient especially when cybercrime is increasingly launched offshore. We hope this study can strengthen the confidence in the COC's effectiveness and crystalize its merit due to international co-operation, and spurs closer co-operation at the global scale.

References

Ayres, I. and Donohue, J.J. 2003. "Shooting Down the More Guns, Less Crime Hypothesis," *Stanford Law Review* (55:4), pp. 1193-1312.

Ayres, I. and Levitt, S.D. 1998. "Measuring Positive Externalities from Observable Victim Precaution: An Empirical Analysis of Lojack," *Quarterly Journal of Economics* (113:1), pp. 43-77.

Balkanli E., Zincir-Heywood, A.N., and Heywood, M.I. "Feature selection for robust backscatter DDoS detection," *40th Local Computer Networks Conference Workshops (LCN Workshops)*, 2015, pp. 611-618.

Barnes, D.A. 2004. "Note, Deworming the Internet," *IEEE Security & Privacy* (83:1), pp. 279-329.

Black, D.A. and Nagin, D.S. 1998. "Do Right-To-Carry Laws Deter Violent Crime," *Journal of Legal Studies* (27:1), pp. 209-219.

Bouffard, L.A. and Piquero, N.L. 2010. "Defiance Theory and Life Course Explanations of Persistent Offending," *Crime & Delinquency* (56:2), pp. 227-252.

Brenner, S.W. 2006. "Cybercrime Jurisdiction," *Crime, Law and Social Change* (46:4-5), pp. 189-206.

Bronars, S.G., and Lott, J.R. 1998. "Criminal Deterrence, Geographic Spillovers, and the Right to Carry Concealed Handguns," *American Economic Review* (88:2), pp. 475-479.

CAIDA. 2005. *UCSD Backscatter 2004-2005 Dataset, May 2004 - November 2005*. Available at https://www.caida.org/data/passive/backscatter_dataset.xml. [Accessed January 18, 2016]

CAIDA. 2006. *UCSD Backscatter 2006 Dataset, February 2006 - November 2006*. Available at https://www.caida.org/data/passive/backscatter_dataset.xml. [Accessed January 18, 2016]

CAIDA. 2007. *UCSD Backscatter 2007 Dataset, January 2007 - November 2007*. Available at https://www.caida.org/data/passive/backscatter_dataset.xml. [Accessed January 18, 2016]

CAIDA. 2008a. *UCSD Backscatter 2008 Dataset, February 2008 - November 2008*. Available at https://www.caida.org/data/passive/backscatter_dataset.xml. [Accessed January 18, 2016]

CAIDA. 2008b. *AS Relationships Dataset, January 2004 - December 2008*. Available at http://www.caida.org/data/active/as-relationships/. [Accessed January 18, 2016]

Calderoni, F. 2010. "The European Legal Framework on Cybercrime: Striving for an Effective Implementation," *Crime, Law and Social Change* (54:5), pp. 339-357.

Cavusoglu, H., Mishra, B. and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16:1), pp. 28-46.

Chatterjee, S., Sarker, S. and Valacich, J.S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use," *Journal of Management Information Systems* (31:4), pp. 49-87.

Chen, Y., Hwang, K. and Ku, W.S. 2007. "Collaborative Detection of DDoS Attacks over Multiple Network Domains," *IEEE Transactions on Parallel and Distributed Systems* (18:12), pp. 1649-1662.

Chen Y., Ramamurthy, K. and Wen, K.W. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?" *Journal of Management Information Systems* (29:3), pp. 157-188.

Cohen, L.E. and Felson, M. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* (44:4), pp. 588-608.

Council of Europe. 2013. *T-CY Guidance Note #5: DDOS attacks*, Cybercrime Convention Committee (T-CY).

Cremonini, M. and Nizovtsev, D. 2009. "Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers," *Journal of Management Information Systems* (26:3), pp. 241-274.

D'Arcy, J., Hovav, A. and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Donohue, J.J. 2004. "Guns, Crime, and the Impact of State Right-To-Carry Laws," *Fordham Law Review* (73:2), pp. 623-652.

Driscoll, J.C. and Kraay, A.C. 1998. "Consistent Covariance Matrix Estimation with Spatially Dependent Panel Data," *Review of Economics and Statistics* (80:4), pp. 549-560.

Ehrlich, I. 1973. "The Deterrent Effect of Capital Punishment: A Question of Life and Death," *American Economic Review* (65:3), pp. 397-417.

Ehrlich, I. 1977. "Capital Punishment and Deterrence: Some Further Thoughts and Additional Evidence," *Journal of Political Economy* (85:4), pp. 741-788.

Ehrlich, I. and Brower, G.D. 1987. "On the Issue of Causality in the Economic Model of Crime and Law Enforcement: Some Theoretical Considerations and Experimental Evidence," *American Economic Review* (77:2), pp. 99-106.

Felson, M. and Boba, R. 2010. *Crime and Everyday Life: Insight and Implications for Society.* Thousand Oaks: Pine Forge.

Forrester Consulting. 2009. *DDoS: A Threat You Can't Afford to Ignore*, January 21, 2009. Available at https://www.nl-ix.net/docs/verisign/whitepaper-ddos-threat-forrester.pdf. [Accessed January 18, 2016]

Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence*. Elsevier, New York.

Goldsmith, J. 2011. *Cybersecurity Treaties: A Skeptical View*, Hoover Institution, Stanford University. http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf. [Accessed January 18, 2016]

Gonzalez-Navarro, M. 2013. "Deterrence and Geographical Externalities in Auto Theft," *American Economic Journal--Applied Economics* (5:4), pp. 92-110.

Hayman, P. 2013. "Cybercrime: It's Serious, But Exactly How Serious?" *Communications of the ACM* (56:3), pp. 18-20.

Hollis-Peel, M.E., Reynald, D.M., van Bavel, M., Elffers, H. and Welsh, B.C. 2011. "Guardianship for Crime Prevention: A Critical Review of the Literature," *Crime, Law and Social Change* (56:1), pp. 53-71.

Hui, K.L., Hui, W. and Yue, W.T. 2012. "Information Security Outsourcing with System Interdependency and Mandatory Security Requirement," *Journal of Management Information Systems* (29:3), pp. 117-155.

Goodin, D. 2010. "Sex, Lies, and Botnets: The Saga of Perverted Justice -- Ex-Vigilante Vents DDoS Fury over Sham Affair," *The Register*, September 23, 2010.

Johnston, A.C. and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Johnston, A.C., Warkentin, M. and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Kaspersky Lab. 2015. *Global IT Security Risks Survey*. Available at http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf. [Accessed January 18, 2016]

Katyal, N.K. 1997. "Deterrence's Difficulty," *Michigan Law Review* (95:8), pp. 2385-2476.

Kaufmann, D., Kraay, A. and Mastruzzi, M. 2010. "The worldwide governance indicators: methodology and analytical issues," *Unpublished Report*. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1682130. [Accessed January 18, 2016]

Keyser, M. 2003. "The Council of Europe Convention on Cybercrime," *Journal of Transnational Law and Policy* (12:2), 2003, pp. 287-326.

Kim, S.H. and Kim, B.C. 2014. "Differential Effects of Prior Experience on the Malware Resolution Process," *MIS Quarterly* (38:3), pp. 655-678.

Kim, S.H., Wang, Q.H. and Ullrich, J.B. 2012. "A Comparative Study of Cyberattacks," *Communications of the ACM* (55:3), pp. 66-73.

Kirchgässner, G. 2011. "Econometric Estimates of Deterrence of the Death Penalty: Facts or Ideology?" *Kyklos* (64:3), pp. 448-478.

Korgaonkar, P.K. and Wolin, L.D. 1999. "A Multivariate Analysis of Web Usage," *Journal of Advertising Research* (39:2), pp. 53-68.

Kshetri, N. 2006. "The Simple Economics of Cybercrimes," *IEEE Security & Privacy* (4:1), pp. 33–39.

Kshetri, N. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Springer.

Li, X. 2007. "International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene," *Webology* (4:3). Available at http://www.webology.org/2007/v4n3/a45.html. [Accessed January 18, 2016]

Liang, H., Xue, Y. and Wu, L. 2013. "Ensuring Employees' IT Compliance: Carrot or Stick?" *Information Systems Research* (24:2), pp. 279-294.

Lott, J.R. and Mustard, D.B. 1997. "Crime, Deterrence, and Right-to-Carry Concealed Handguns," *Journal of Legal Studies* (26:1), pp. 1-68.

Mahmood, M.A., Siponen, M., Straub, D. and Rao, H.R. 2010. "Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue," *MIS Quarterly* (34:3), pp. 431-434.

Mansfield-Devine, S. 2011. "DDoS: Threats and Mitigation," *Network Security* (2011:12), pp. 5-12.

Mao, Z. M., Sekar, V., Spatscheck, O., Van Der Merwe, J. and Vasudevan, R. 2006. "Analyzing Large DDoS Attacks Using Multiple Data Sources," *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*.

McAfee. 2014. *Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II*, Center for Strategic and International Studies.

Moore, D., Voelker, G. and Savage, S. 2001. "Inferring Internet Denial of Service Activity," *Proceedings of the 2001 USENIX Security Symposium*.

Moore, D., Shannon, C., Brown, D., Voelker, G. and Savage, S. 2006. "Inferring Internet Denial-of-Service Activity," *ACM Transactions on Computer Systems* (24:2), pp. 115-139.

Nagin, D.S. 1998. "Criminal Deterrence Research at the Outset of the Twenty-First Century," *Crime and Justice* (23), pp. 1-42.

Neustar. 2012. *DDoS Survey: Q1 2012 – When Businesses Go Dark*, Neustar Insights.

Owens, W.A., Dam, K.W. and Lin, H.S. 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Academies Press, Washington D.C., pp. 7-24.

Pipkin, D. L. 2002. *Halting the Hacker: A Practical Guide to Computer Security*, 2nd ed., Prentice Hall.

Ponemon Institute. 2012. *2012 Cost of Cyber Crime Study: United States*. Available at http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf. [Accessed January 18, 2016]

Png, I.P.L., Wang, C.Y. and Wang, Q.H. 2008. "The Deterrent and Displacement Effects of Information Security Enforcement: International Evidence," *Journal of Management Information Systems* (25:2), pp. 125-144.

Png, I.P.L. and Wang, Q.H. 2009. "Information Security: Facilitating User Precautions Vis-a-Vis Enforcement against Attackers," *Journal of Management Information Systems* (26:2), pp. 97-121.

Ransbotham, S. and Mitra, S. 2009. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research* (20:1), pp. 121-139.

Rufo, A. 2013. *Frozen Cybercrime Law: Deterrence or Nuisance?* Available at http://www.rappler.com/newsbreak/21223-frozen-cybercrime-law-deterrent-or-nuisance. [Accessed January 18, 2016]

Schreiber, S. 2008. "The Hausman Test Statistic can be Negative Even Asymptotically," *Journal of Economics and Statistics* (228:4), pp. 394-405.

Shepherd, J.M. 2005. “Deterrence Versus Brutalization: Capital Punishment’s Differing Impacts Among States,” *Michigan Law Review* (104:2), pp. 203-256.

Sherman, L.W. 1993. “Defiance, Deterrence, and Irrelevance: A Theory of the Criminal Sanction,” *Journal of Research in Crime and Delinquency* (30:4), pp. 445-473.

Singer, S. I. and McDowall, D. 1988. “Criminalizing Delinquency: The Deterrent Effects of the New York Juvenile Offender Law,” *Law & Society Review* (22:3), pp. 521-535.

Sojer, M., Alexy, O., Kleinknecht, S. and Henkel, J. 2014. “Understanding the Drivers of Unethical Programming Behavior: The Inappropriate Reuse of Internet-Accessible Code,” *Journal of Management Information Systems* (31:3), pp. 287-325.

Soundar Rajam, V.K., Selvaram, G., PradeepKumar, M. and Mercy Shalinie, S. 2013. “Autonomous System Based Traceback Mechanism for DDoS Attack,” *Fifth International Conference on Advanced Computing* (ICoAC), pp. 164-171.

Steinberg, L. and Scott, E.S. 2003. “Less Guilty by Reason of Adolescence: Developmental Immaturity, Diminished Responsibility, and the Juvenile Death Penalty,” *American Psychologist* (58:12), pp. 1009-1018.

Steiner, B. and Wright, E. 2006. “Assessing the Relative Effects of State Direct File Waiver Laws on Violent Juvenile Crime: Deterrence or Irrelevance?” *Journal of Criminal Law and Criminology* (96:4), pp. 1451-1477.

Stigler, G.J. 1970. “The Optimum Enforcement of Laws,” *Journal of Political Economy* (78:3), pp. 526–536.

Symantec. 2014. *Internet Security Threat Report 2014: Volume 19*. Available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. [Accessed January 18, 2016]

Tillyer, M.S. 2011. “Routine Activities Theory and Rational Choice Theory,” *Routledge Handbook of Deviant Behavior*, ed. by Clifton D. Bryant, Routledge, New York, NY, pp. 143-149.

Vaillant, N.G. and Wolff, F.C. 2009. “Does Punishment of Minor Sexual Offences Deter Rapes? Longitudinal Evidence from France,” *European Journal of Law and Economics* (30:1), pp. 59-71.

Vamosi, R. 2008. “First Conviction for Estonia’s ‘Cyberwar’,” *CNET News*, January 24, 2008. Available at http://www.cnet.com/news/first-conviction-for-estonias-cyberwar/. [Accessed January 18, 2016]

Verdelho, P. 2008. *The Effectiveness of International Co-operation against Cybercrime: Examples of Good Practice.* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f69c3 [Accessed December 23, 2015]

Vormetric. 2013. *2013 Vormetric/ESG Insider Threats Survey: The Ominous State of Insider Threats*. Available at http://www.vormetric.com/sites/default/files/ap_Vormetric-Insider_Threat_ESG_Research_Brief.pdf. [Accessed January 18, 2016]

Wang, J., Gupta, M. and Rao, H.R. 2015. “Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications,” *MIS Quarterly* (39:1), 91-112.
Weber, A.M. 2003. “The Council of Europe’s Convention on Cybercrime,” *Berkeley Technology Law Journal* (18:1), pp. 425-446.
Willison, R. and Warkentin, M. 2013. “Beyond Deterrence: An Expanded View of Employee Computer Abuse,” *MIS Quarterly* (37:1), pp. 1-20.
Wooldridge, J.M. 2006. *Introductory Econometrics: A Modern Approach*, Southwestern, Mason, OH: Thomson.
Xue, Y., Liang, H. and Wu, L. 2011. “Punishment, Justice, and Compliance in Mandatory IT Settings,” *Information Systems Research* (22:2), pp. 400-414.
Yang, D. 2008. “Can Enforcement Backfire? Crime Displacement in the Context of Custom Reforms in Philippines,” *Review of Economics and Statistics* (90:1), pp. 1-14.
Yang, B., and Lester, D. 2008. “The Deterrent Effect of Executions: A Meta-Analysis Thirty Years after Ehrlich,” *Journal of Criminal Justice* (36:5), pp. 453–460.
Zimmerman, P.R. 2014. “The deterrence of crime through private security efforts: Theory and evidence,” *International Review of Law and Economics* (37), pp. 66-75.
Zorz, Z. 2011. “Man Convicted for Using DDoS Attacks in Extortion Scheme,” *Net Security*, June 15, 2011.
Zuckerman, E., Roberts, H., Mcgrady, R., York, J. and Palfrey, J. 2010. *Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites*, The Berkman Center for Internet & Society at Harvard University, pp. 1-66.

Figure 1. Signature and Enforcement of the Convention on Cybercrime

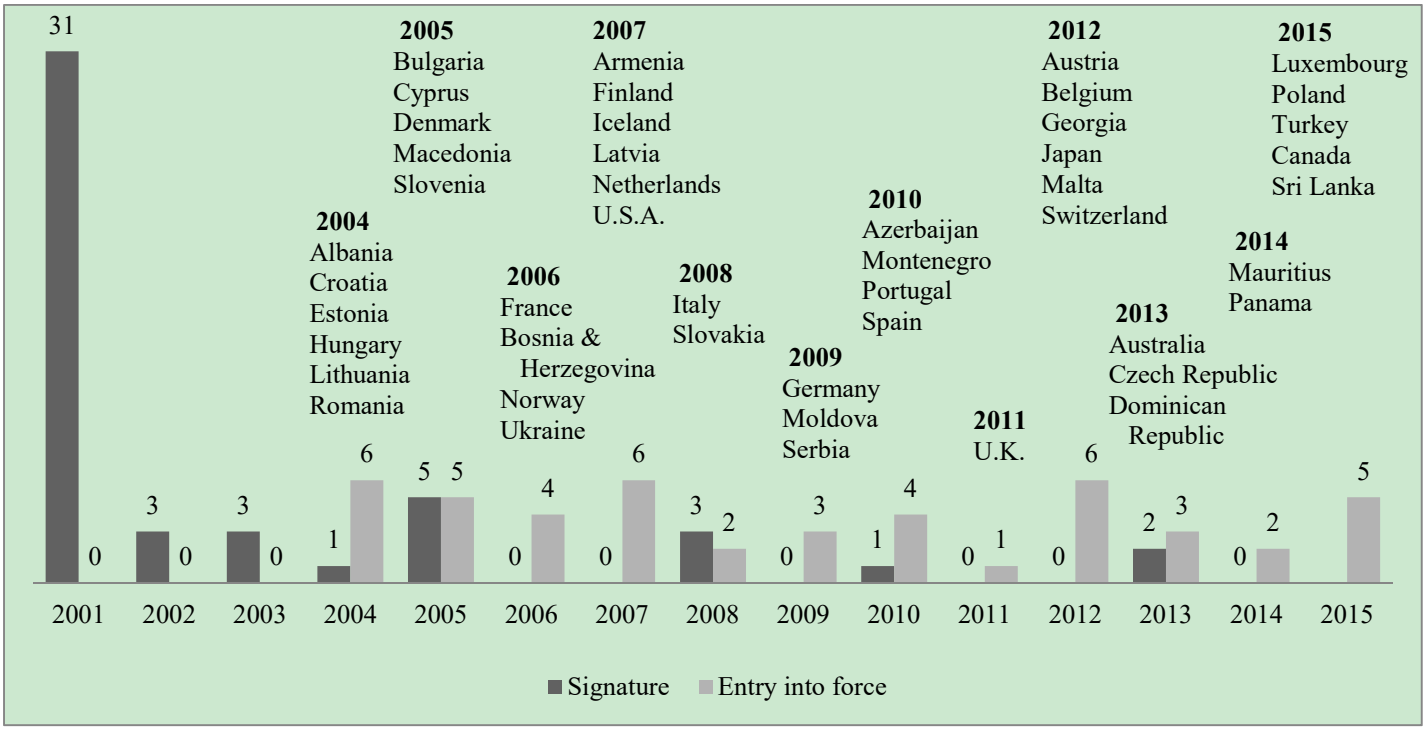
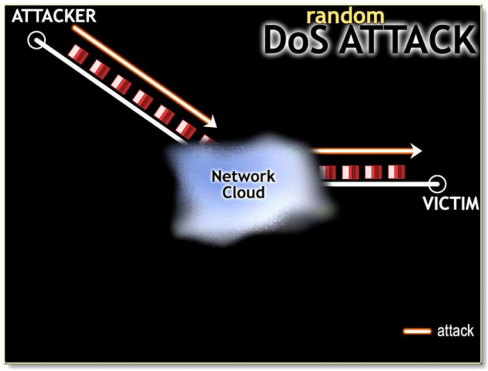
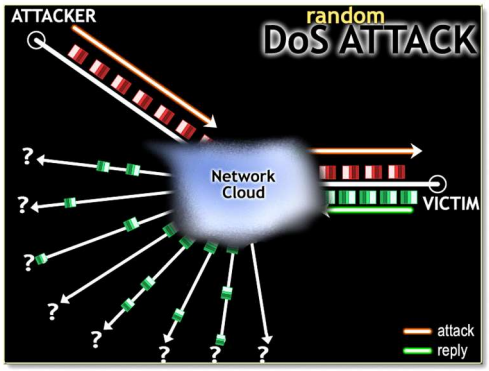


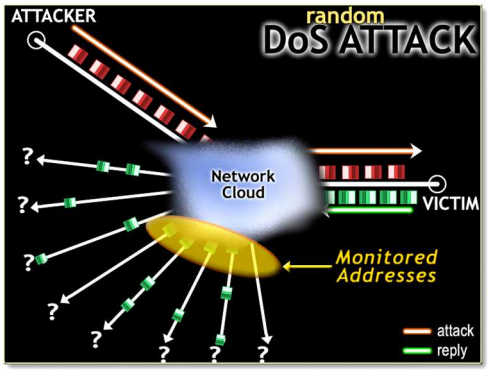
Figure 2. The Backscatter Data



(a) Attacker sends packets with spoofed source addresses to the victim.



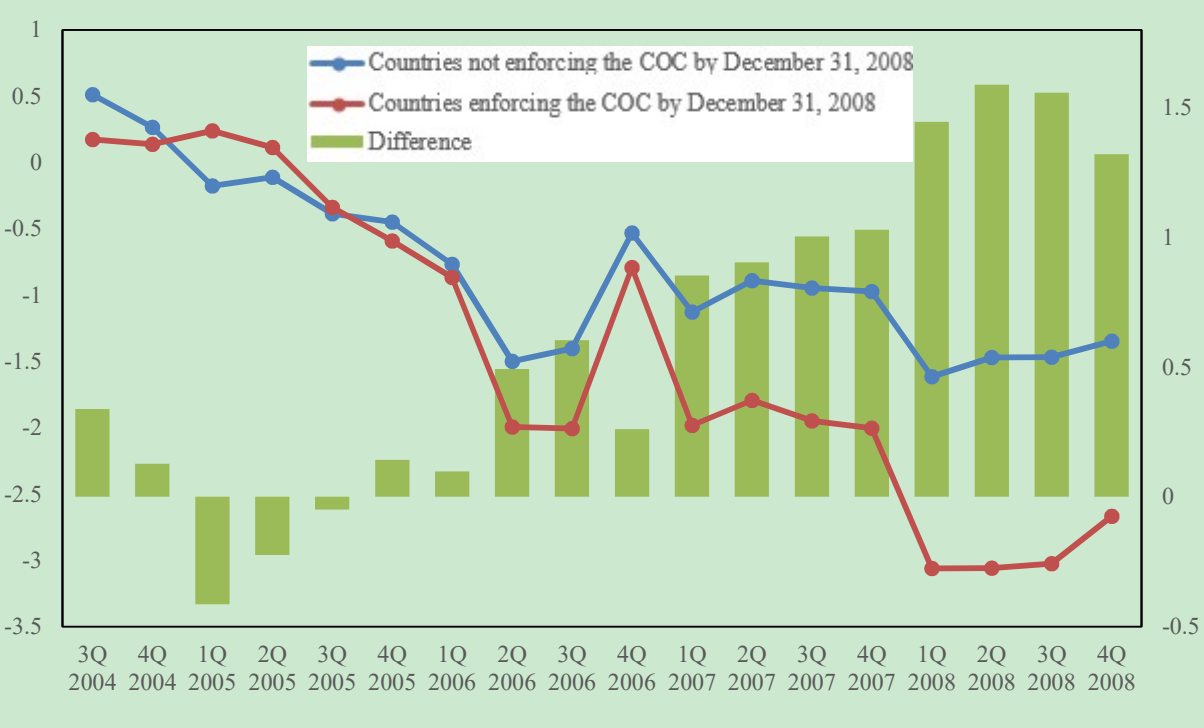
(b) The victim responds to the attack packets.



(c) The 1/256th IP addresses monitored by CAIDA receive roughly 1/256th of the response packets sent by the victim.

Image source: CAIDA (http://www.caida.org/projects/network_telescope/). An animated illustration of the backscatter data is available at http://www.caida.org/publications/animations/passive_monitoring/backscatter.mov.

Figure 3. DDOS Attacks Over Time



Note: The figure plots the average log numbers of victim IP addresses per 1,000 Internet hosts per country per day in each quarter in 2004–2008 across countries that have enforced and not enforced the COC by 31 December 2008. The first enforcement of the COC started in 3Q 2004.

Table 1. Reservations

Country	Article 4	Article 6	Article 9	Article 10	Article 11	Article 14	Article 22	Article 29	Article 41
Australia*			22	22		○	○		
Austria*								○	
Azerbaijan*	○	○						○	
Belgium*							○		
Bulgaria						○			
Canada*				○			○		
Czech Republic*								○	
Denmark			○			○			
Finland					○	○			
France			○				○		
Germany*		○						○	
Hungary			○						
Iceland**			○						
Japan*	11	○	○ 11		○		○	○	
Latvia**							○	○	
Lithuania	○							○	
Montenegro*			○			○			
Norway		○				○		○	
Poland*								○	
Slovakia	○							○	
Switzerland*		○	○			○		○	
Turkey*					○	○		○	
Ukraine		○	○						
U.K. *			○				○	○	
U.S.A.	○	○	○	○			○		○

Notes:

1. ○: Reservation declared on the specific article; 11: Reservation declared under the provision of Article 11; 22: Reservation declared under the provision of Article 22.
2. * Countries that enforced the Convention on Cybercrime after 2008, the end of the sample for this study.
3. ** Iceland withdrew the reservation of Article 9 on December 12, 2012; Latvia withdrew the reservation of Article 22 on December 9, 2011.
4. Article 4 – Data interference; Article 6 – Misuse of devices; Article 9 – Offences related to child pornography; Article 10 – Infringements of copyright and related rights; Article 11 – Attempt and aiding or abetting; Article 14 – Scope of procedural provisions; Article 22 – Jurisdiction; Article 29 – Expedited preservation of stored computer data; Article 41 – Federal clause.

Table 2. Time Periods Covered

Year	First quarter	Second quarter	Third quarter	Fourth quarter	Number of Days
2004	n.a.	May 26–Jun 3	Aug 26–Sep 3	Nov 24–Dec 2	27
2005	Feb 23–Mar 3	May 25–Jun 2	Aug 24–Sep 1	Nov 23–Dec 1	36
2006	Feb 22–Mar 2	May 24–Jun 1	Aug 23–31	Nov 22–30	36
2007	Jan 8–11, Feb 21–Mar 1	May 23–31	Aug 22–30	Nov 20–29	41
2008	Feb 20-28, Mar 18-19	May 21–29	Aug 20–28	Nov 12–19	37
Total					177

Table 3. List of Studied Countries

Countries enforcing the COC by December 31, 2008			
Albania	Denmark	Italy	Romania
Armenia	Estonia	Latvia	Slovakia
Bosnia and Herzegovina	Finland	Lithuania	Slovenia
Bulgaria	France	Macedonia	Ukraine
Croatia	Hungary	Netherlands	United States
Cyprus	Iceland	Norway	
			Total: 23

Countries *not* enforcing the COC by December 31, 2008			
Afghanistan	Egypt	Lebanon	Qatar
Australia	El Salvador	Luxembourg	Russian Federation
Austria	Ethiopia	Madagascar	Saint Lucia
Azerbaijan	Fiji	Malaysia	Senegal
Bahrain	Germany	Maldives	Serbia
Barbados	Greece	Malta	Singapore
Belarus	Guatemala	Mauritius	South Africa
Belgium	Hong Kong	Mexico	Spain
Bolivia	India	Republic of Moldova	Sweden
Botswana	Indonesia	Mongolia	Switzerland
Brunei Darussalam	Iran	Morocco	Taiwan
Cameroon	Ireland	New Zealand	Tanzania
Canada	Israel	Nigeria	Thailand
Cape Verde	Jamaica	Oman	Trinidad and Tobago
Chile	Japan	Pakistan	Tunisia
China	Jordan	Panama	Turkey
Colombia	Kazakhstan	Paraguay	United Arab Emirates
Costa Rica	Kenya	Peru	United Kingdom
Czech Republic	Republic of Korea	Philippines	Uruguay
Dominican Republic	Kuwait	Poland	Yemen
Ecuador	Lao	Portugal	
			Total: 83

Table 4. Descriptive statistics

Variable	n	No. of countries	Unit	Mean	Std. dev.	Min	Max	Source
COC enforcement	16,429	106	1 = enforce; 0 = not enforced	0.152	0.359	0	1	COE
COC signature	16,429	106	1 = signed; 0 = not signed	0.414	0.493	0	1	COE
Reservations	16,429	106	Number of reservations	0.142	0.610	0	6	COE
CPHRFF enforcement	16,429	106	1 = enforce; 0 = not enforced	0.085	0.279	0	1	COE
Cumulative domestic legislation	16,429	106	Number of legislations/revisions	1.283	2.550	0	36	COE, UNODC, ITU, GCLD
Victim IP addresses	16,429	106		817.137	5,013.390	0	91,755	CAIDA
…per 1,000 Internet hosts	16,429	106		2.216	13.975	0	621.359	Self-computed
Internet hosts	16,429	106	Per 1,000 inhabitants	87.923	157.019	0.001	1,039.270	CIA
Unemployment rate	16,429	106	% economically active people	8.173	5.760	0.400	37.300	GMID
GDP in PPP	16,429	106	Thousand dollars per capita	18.878	16.034	0.620	84.249	GMID
Higher education students	16,429	106	Per 100 inhabitants	3.213	1.635	0.033	6.713	GMID
Internet users	16,429	106	Per 1,000 inhabitants	356.875	259.855	2.197	911.319	GMID
% digital main lines	16,429	106	% of telephone main lines	95.996	10.529	34.000	100	GMID
ISDN subscribers	16,429	106	Per 1,000 inhabitants	16.822	32.434	0	177.903	GMID
Land area	16,429	106	sq. km per 1,000 inhabitants	34.899	83.610	0.142	617.118	GMID
Control of corruption	16,429	106	Normalized index	0.373	1.034	-1.459	2.591	WGI
Government effectiveness	16,429	106	Normalized index	0.481	0.927	-1.236	2.374	WGI
Political stability and absence of violence/terrorism	16,429	106	Normalized index	0.142	0.901	-2.550	1.586	WGI
Regulatory quality	16,429	106	Normalized index	0.495	0.863	-1.647	1.983	WGI
Rule of law	16,429	106	Normalized index	0.361	0.970	-1.734	2.014	WGI
Voice and accountability	16,429	106	Normalized index	0.299	0.9390	-1.770	1.826	WGI
% Internet users covered by others' enforcement	16,429	106		0.120	0.101	0	0.285	Self-computed
% AS connections to other enforcing countries	16,429	106		0.162	0.199	0	0.889	CAIDA

Table 5. Descriptive statistics: Before/after enforcement

	Countries enforcing the COC in 2005		Countries not enforcing the COC by December 31, 2008		Countries enforcing the COC in 2006		Countries not enforcing the COC by December 31, 2008		Countries enforcing the COC in 2007		Countries not enforcing the COC by December 31, 2008	
	Pre-2005 (n = 135)	Post-2005 (n = 570)	Pre-2005 (n = 837)	Post-2005 (n = 8893)	Pre-2006 (n = 189)	Post-2006 (n = 312)	Pre-2006 (n = 3528)	Post-2006 (n = 6121)	Pre-2007 (n = 594)	Post-2007 (n = 222)	Pre-2007 (n = 6300)	Post-2007 (n = 2923)
Variable	Mean	Mean	Mean	Mean	Mean	Mean	Mean	Mean	Mean	Mean	Mean	Mean
Cumulative domestic legislation	0.733	2.216	0.443	1.246	1.523	2.625	0.517	1.422	1.327	3.595	0.667	1.627
Victim IP addresses	102.378	74.433	724.194	342.302	1154.910	365.619	574.088	331.235	8889	2674.838	482.854	227.783
…per 1,000 Internet hosts	1.566	0.291	6.681	1.752	0.829	0.064	5.047	1.210	0.318	0.087	4.123	1.187
Internet hosts	52.925	150.712	23.872	64.854	89.828	192.783	38.996	70.813	311.546	564.067	44.584	82.429
Unemployment rate	13.180	10.969	9.171	7.320	7.200	10.852	8.362	7.107	9.891	9.000	8.110	7.109
GDP in PPP	18.008	22.114	18.526	18.251	27.452	25.437	16.541	19.029	27.127	31.557	16.537	19.339
Higher education students	3.412	3.778	3.318	2.904	4.636	4.047	2.920	2.965	4.716	4.904	2.854	2.981
Internet users	396.472	503.542	298.011	329.746	418.751	491.531	275.088	351.885	604.759	680.333	277.627	372.276
% digital main lines	86.600	94.250	94.045	97.531	90.838	94.238	95.502	97.697	89.826	93.733	96.233	97.946
ISDN subscribers	36.793	37.799	19.752	11.182	74.857	43.008	13.518	11.159	30.238	22.817	12.513	10.956
Land area	11.119	11.036	35.159	36.374	29.175	24.860	35.037	36.444	77.579	73.993	35.557	37.924
Control of corruption	0.801	0.817	0.453	0.253	0.864	0.553	0.306	0.262	1.323	1.321	0.273	0.274
Government effectiveness	0.932	0.928	0.568	0.358	1.052	0.507	0.397	0.375	1.380	1.220	0.363	0.367
Political stability and absence of violence/terrorism	0.315	0.521	0.104	0.004	0.419	0.327	0.052	0.018	0.748	0.693	0.018	0.015
Regulatory quality	0.904	0.943	0.422	0.360	0.746	0.502	0.359	0.379	1.296	1.232	0.342	0.384
Rule of law	0.691	0.667	0.482	0.231	0.859	0.541	0.316	0.243	1.225	1.265	0.266	0.249
Voice and accountability	0.873	0.891	0.333	0.086	0.902	0.720	0.206	0.090	1.053	0.917	0.149	0.095
% Internet users covered by others' enforcement	0.006	0.165	0.006	0.168	0.011	0.217	0.013	0.226	0.023	0.193	0.025	0.219
% AS connections to other enforcing countries	0.022	0.307	0.003	0.218	0.038	0.289	0.007	0.306	0.034	0.234	0.015	0.306

Note: The table compares the variables in the enforcing countries before/after the year of enforcement vis-à-vis the other 83 non-enforcing countries. The first column reports the comparison for the five countries (Bulgaria, Cyprus, Denmark, Macedonia, and Slovenia) enforcing the COC in 2005, the third column reports the comparison for the four countries (Bosnia and Herzegovina, France, Norway, and Ukraine) enforcing the COC in 2006, the fifth column reports the comparison for the six countries (Armenia, Finland, Iceland, Latvia, Netherlands, USA) enforcing the COC in 2007. The second, fourth, and sixth columns report the corresponding comparisons in the 83 non-enforcing countries by excluding, respectively, the 2005, 2006, and 2007 data.

Table 6. Correlations

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1.	COC enforcement	1																						
2.	COC signature	0.50	1																					
3.	Reservations	0.55	0.28	1																				
4	CPHRFF enforcement	0.49	0.36	0.03	1																			
5.	Cumulative domestic legislation	0.20	0.21	0.21	0.07	1																		
6.	Victim IP addresses	0.01	0.14	0.20	-0.04	0.03	1																	
7.	…per 1,000 Internet hosts	-0.04	-0.10	-0.02	-0.03	-0.04	0.01	1																
8.	Internet hosts	0.24	0.43	0.35	0.12	0.18	0.24	-0.08	1															
9.	Unemployment rate	0.13	0.13	-0.10	0.31	-0.04	-0.07	0.01	-0.28	1														
10.	GDP in PPP	0.05	0.34	0.18	0.05	0.10	0.17	-0.04	0.56	-0.40	1													
11.	Higher education students	0.23	0.34	0.27	0.01	0.33	0.14	-0.11	0.37	-0.20	0.22	1												
12.	Internet users	0.19	0.51	0.24	0.06	0.19	0.16	-0.12	0.72	-0.30	0.76	0.47	1											
13.	% digital main lines	-0.10	-0.06	-0.02	-0.11	-0.27	0.05	-0.01	0.17	-0.15	0.25	-0.11	0.27	1										
14.	ISDN subscribers	0.17	0.54	0.10	0.12	0.02	0.03	-0.07	0.42	-0.15	0.53	0.13	0.55	0.17	1									
15.	Land area	-0.05	-0.06	-0.01	-0.07	0.08	-0.01	0.01	0.20	-0.15	0.02	0.26	0.06	0.00	-0.05	1								
16.	Control of corruption	0.07	0.43	0.15	0.03	0.06	0.14	-0.09	0.66	-0.26	0.77	0.33	0.85	0.36	0.54	0.09	1							
17.	Government effectiveness	0.09	0.47	0.18	0.01	0.08	0.16	-0.09	0.64	-0.26	0.75	0.37	0.87	0.37	0.54	0.04	0.95	1						
18.	Political stability and absence of violence/terrorism	0.15	0.45	0.14	0.06	0.05	0.00	-0.06	0.45	-0.24	0.64	0.32	0.68	0.19	0.44	0.17	0.74	0.72	1					
19.	Regulatory quality	0.16	0.53	0.18	0.06	0.12	0.16	-0.12	0.59	-0.21	0.72	0.37	0.84	0.32	0.50	0.02	0.89	0.94	0.72	1				
20.	Rule of law	0.09	0.47	0.18	0.00	0.06	0.15	-0.08	0.63	-0.26	0.76	0.36	0.85	0.38	0.55	0.07	0.96	0.96	0.77	0.92	1			
21.	Voice and accountability	0.21	0.60	0.19	0.09	0.08	0.12	-0.13	0.55	-0.09	0.49	0.40	0.72	0.30	0.54	0.08	0.76	0.77	0.63	0.81	0.78	1		
22.	% Internet users covered by others' enforcement	0.11	-0.05	0.06	0.09	0.16	-0.08	-0.09	0.12	-0.10	0.06	0.01	0.12	0.10	-0.05	0.00	-0.03	-0.03	-0.01	-0.01	-0.03	-0.06	1	
23.	% AS connections to other enforcing countries	0.15	0.05	0.08	0.07	0.19	-0.05	-0.07	0.11	-0.09	0.06	0.07	0.14	0.07	-0.01	-0.04	0.01	0.02	-0.06	0.07	-0.02	0.08	0.70	1

Table 7. Test of H1: COC deterrence effect

VARIABLES	(1) Main estimate (preferred)	(2) Binary domestic legislation	(3) 2SLS: CPHRFF enforcement as instrument	(4) COC signature instead of enforcement	(5) Include responsible authorities and reservations	(6) Separate reservations into four sets	(7) Exclude USA
COC enforcement	-0.125***	-0.133***	-1.160**				
	(0.028)	(0.030)	(0.473)				
COC signature				-0.014			
				(0.070)			
COC enforcement without the responsible authority					-0.131***	-0.142***	-0.137***
					(0.044)	(0.045)	(0.046)
COC enforcement with the responsible authority					-0.160***	-0.185***	-0.181***
					(0.040)	(0.057)	(0.057)
Number of reservations					0.019		
					(0.021)		
Reservations – domestic enforcement						-0.023	-0.021
						(0.043)	(0.043)
Reservations – mutual assistance						0.301***	0.290***
						(0.071)	(0.072)
Reservations – DDOS irrelevant						-0.005	-0.010
						(0.062)	(0.062)
Reservations – federal clause						0.094	
						(0.146)	
Indicator of first domestic legislation		-0.084**					
		(0.034)					
Cumulative domestic legislation (log)	-0.231***		-0.227***	-0.231***	-0.228***	-0.219***	-0.244***
	(0.042)		(0.029)	(0.042)	(0.042)	(0.042)	(0.043)
Internet hosts (log)	-0.978***	-0.981***	-1.002***	-0.976***	-0.978***	-0.979***	-0.963***
	(0.010)	(0.009)	(0.014)	(0.010)	(0.009)	(0.010)	(0.011)
Unemployment rate	-0.044***	-0.043***	-0.006	-0.048***	-0.043***	-0.043***	-0.040***
	(0.009)	(0.009)	(0.020)	(0.009)	(0.009)	(0.009)	(0.009)
GDP in PPP (log)	-0.608**	-0.597**	-0.570*	-0.618**	-0.625**	-0.556**	-0.599**
	(0.273)	(0.274)	(0.317)	(0.265)	(0.278)	(0.280)	(0.280)

Higher education students (log)	0.556***	0.548***	0.234	0.595***	0.558***	0.556***	0.593***
	(0.154)	(0.156)	(0.234)	(0.152)	(0.156)	(0.155)	(0.155)
Internet users (log)	-0.124***	-0.124***	-0.116**	-0.125***	-0.123***	-0.124***	-0.110**
	(0.045)	(0.045)	(0.050)	(0.046)	(0.045)	(0.045)	(0.045)
% digital main lines	0.007	0.005	0.008*	0.007	0.007	0.007	0.008
	(0.005)	(0.006)	(0.005)	(0.006)	(0.006)	(0.006)	(0.006)
ISDN subscribers (log)	0.703***	0.709***	0.713***	0.702***	0.702***	0.696***	0.679***
	(0.088)	(0.089)	(0.063)	(0.088)	(0.087)	(0.085)	(0.085)
Land area (log)	0.226	0.191	0.592	0.187	0.217	0.229	0.226
	(1.083)	(1.111)	(0.831)	(1.084)	(1.083)	(1.082)	(1.075)
Control of corruption	-0.195***	-0.215***	-0.211**	-0.193***	-0.199***	-0.174**	-0.087
	(0.066)	(0.067)	(0.084)	(0.066)	(0.068)	(0.069)	(0.071)
Government effectiveness	-0.244***	-0.245***	-0.225***	-0.245***	-0.247***	-0.266***	-0.270***
	(0.064)	(0.065)	(0.076)	(0.063)	(0.063)	(0.064)	(0.065)
Political stability and absence of violence/terrorism	-0.326***	-0.352***	-0.364***	-0.321***	-0.324***	-0.313***	-0.339***
	(0.059)	(0.060)	(0.057)	(0.058)	(0.060)	(0.060)	(0.062)
Regulatory quality	0.363***	0.347***	0.304***	0.370***	0.367***	0.361***	0.377***
	(0.072)	(0.072)	(0.090)	(0.072)	(0.071)	(0.071)	(0.072)
Rule of law	0.732***	0.780***	0.664***	0.741***	0.733***	0.719***	0.646***
	(0.087)	(0.088)	(0.109)	(0.087)	(0.087)	(0.087)	(0.087)
Voice accountability	-0.235***	-0.246***	-0.217***	-0.237***	-0.234***	-0.224***	-0.195**
	(0.082)	(0.084)	(0.079)	(0.083)	(0.082)	(0.080)	(0.080)
Country fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Day fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Country time trends	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	16,429	16,429	16,429	16,429	16,429	16,429	16,252
Number of countries	106	106	106	106	106	106	105
R-squared within model	0.811	0.810	0.799	0.811	0.811	0.811	0.807

Notes: Log number of victim IP addresses per Internet host as dependent variable. Column (1): Preferred estimate with COC enforcement, domestic enforcement, and all demographic variables as regressors; Column (2): Domestic enforcement represented by indicator of dates since first legislation in the country; Column (3): 2SLS estimate with the enforcement of Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms as instrument; Column (4): COC signature in place of COC enforcement; Column (5): Split the COC enforcement variable into two based on whether the responsible authority was established and include the number of reservations as a covariate; Column (6): Separate the reservations into four sets; Column (7): Exclude USA. Spatial correlation-consistent standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1.

Table 8. Test of H2: Network and displacement effects

VARIABLES	(1) Split enforcement variable into five	(2) Measure others' enforcement by AS connection	(3) Only non-enforcing countries with AS connection	(4) Only enforcing countries with AS connection
1st year of enforcement	-0.177***			
	(0.030)			
2nd year of enforcement	-0.276***			
	(0.037)			
3rd year of enforcement	-0.601***			
	(0.078)			
4th year of enforcement	-0.783***			
	(0.107)			
5th year of enforcement	-0.841***			
	(0.156)			
COC enforcement		-0.074**		
		(0.030)		
% AS connections to other enforcing countries		0.171***	0.206***	-0.419***
		(0.063)	(0.074)	(0.098)
COC enforcement × % AS connections to other enforcing countries		-0.427***		
		(0.089)		
Cumulative domestic legislation (log)	-0.267***	-0.235***	-0.140***	-0.344***
	(0.043)	(0.042)	(0.041)	(0.069)
Internet hosts (log)	-0.978***	-0.972***	-0.998***	-0.935***
	(0.008)	(0.009)	(0.009)	(0.020)
Unemployment rate	-0.052***	-0.044***	-0.061***	-0.136***
	(0.009)	(0.009)	(0.014)	(0.017)
GDP in PPP (log)	-0.839***	-0.594**	-1.186***	-2.963***
	(0.266)	(0.271)	(0.349)	(0.626)
Higher education students (log)	0.696***	0.533***	1.463***	-3.218***
	(0.159)	(0.154)	(0.182)	(0.419)
Internet users (log)	-0.110**	-0.120***	-0.283***	0.485***
	(0.045)	(0.045)	(0.044)	(0.118)

% digital main lines	0.014**	0.008	0.043***	-0.009
	(0.006)	(0.005)	(0.008)	(0.006)
ISDN subscribers (log)	0.683***	0.699***	0.655***	0.636***
	(0.086)	(0.089)	(0.085)	(0.159)
Land area (log)	0.771	0.303	-0.501	19.600***
	(1.056)	(1.097)	(1.052)	(7.015)
Control of corruption	-0.280***	-0.197***	-0.448***	0.791***
	(0.068)	(0.066)	(0.084)	(0.141)
Government effectiveness	-0.204***	-0.260***	-0.186***	-0.694***
	(0.065)	(0.062)	(0.069)	(0.131)
Political stability and absence of violence/terrorism	-0.336***	-0.314***	-0.264***	-0.216**
	(0.059)	(0.058)	(0.055)	(0.107)
Regulatory quality	0.390***	0.373***	0.410***	0.106
	(0.073)	(0.071)	(0.085)	(0.175)
Rule of law	0.828***	0.751***	0.649***	1.878***
	(0.091)	(0.087)	(0.105)	(0.232)
Voice accountability	-0.265***	-0.257***	0.035	-1.157***
	(0.085)	(0.083)	(0.112)	(0.185)
Country fixed effects	Yes	Yes	Yes	Yes
Day fixed effects	Yes	Yes	Yes	Yes
Country time trends	Yes	Yes	Yes	Yes
Observations	16,429	16,429	12,421	4,008
Number of countries	106	106	83	23
R-squared within model	0.811	0.811	0.785	0.890

Notes: Log number of victim IP addresses per Internet host as dependent variable. Column (1): Split the COC enforcement variable into five according to the number of years since the enforcement took place; Column (2): Include the percentage of direct AS connections to other enforcing countries and its interaction with COC enforcement; Column (3): Only countries not enforcing the COC in 2004–2008 and include the percentage of direct AS connections to other enforcing countries; Column (4): Only countries enforcing the COC in 2004–2008 and include the percentage of direct AS connections to other enforcing countries. Spatial correlation-consistent standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1.

Table 9. Summary of hypothesis testing

Effect of enforcement within the enforcing countries		
H1a	*COC enforcement reduces the number of DDOS attack victims in the enforcing countries*.	Supported
H1b	*Among enforcing countries, establishing the authority responsible for reacting to external requests for international co-operation reduces the number of DDOS attack victims more than those that have not established such an authority.*	Not supported
H1c	*Reservation on Article 29 (expedited preservation of stored computer data) increases the number of DDOS attack victims in the enforcing countries.*	Supported
Effect of enforcement on other countries (externalities)		
H2a	*The effect of COC enforcement on the number of DDOS attack victims in the enforcing countries is stronger as the enforcement in other countries increases.*	Supported
H2b	*Enforcement of the COC will cause cybercrime displacement; non-enforcing countries will receive more DDOS attacks as the enforcement in other countries increases*.	Supported

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

ONLINE SUPPLEMENT

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)...They 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... heheheheehe... :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 legislations. 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 legislations against cybercrime in each country from multiple sources, including Asian School of Cyber Laws (ASCL), Council of Europe (COE), International Telecommunications 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 legislations (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 legislations. 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 Laws (ASCL)	Global Cyber Law Database: "*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/

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

From these repositories, for each of the 106 countries in our sample, we first identified legislations 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 legislations irrelevant to DDOS attack, such as copyright, child pornography, spam, money laundering, fraudulent use of credit or debit cards, etc. However, we included legislations 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 legislations 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 legislations against cybercrime.

For each country in our sample, we constructed two variables to measure the extent of domestic legislations 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 legislations enforced over time. The following table reports the descriptive statistics of the domestic legislations.

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 legislations	Number of domestic legislations (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

VARIABLES	(1) Only enforcing countries	(2) Only COE countries	(3) Split enforcement effect over time	(4) 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)
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) DID for countries enforcing in 2006
VARIABLES	
Post-2006 (=1 if year > 2006)	-0.281**
	(0.138)
Countries enforcing COC in 2006	-0.573***
× Post-2006	(0.036)
Cumulative domestic	-0.078
legislation (log)	(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	-0.686***
of violence/terrorism	(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

VARIABLES	(1) 1st year of enforcement vs. no enforcement	(2) 2nd year of enforcement vs. no enforcement	(3) 3rd year of enforcement vs. no enforcement	(4) 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.