8-2013

Marginal deterrence in the enforcement of law: Evidence from distributed denial of service attack

Kai-Lung HUI

Seung-Hyun KIM

QIU-HONG WANG
Singapore Management University, qiuhongwang@smu.edu.sg

Citation

HUI, Kai-Lung; KIM, Seung-Hyun; and QIU-HONG WANG. Marginal deterrence in the enforcement of law: Evidence from distributed denial of service attack. (2013). *Workshop on Analytics for Business, Consumer and Social Insights (BCSI 2013). Singapore, August 2013.*.
Available at: https://ink.library.smu.edu.sg/sis_research/3518

Marginal Deterrence in the Enforcement of Law: Evidence from Distributed Denial of Service Attack

Kai-Lung Hui, Seung Hyun Kim, and Qiu-Hong Wang[†]

May 2013

Abstract

By studying a panel dataset of distributed denial of service attack across 240 countries over 5 years, we find that enforcing the Convention on Cybercrime had increased the intensity of attack by 43 to 52 percent. It did not significantly reduce the chance for a country to be selected for the attack. We conducted a battery of identification and falsification tests to show that such increased attack intensity arose because of failure in marginal deterrence, instead of other theories such as brutalization, stigmatization, or defiance, or general forms of endogeneity. We show that raising the standard of proof of conviction is one way to facilitate marginal deterrence, but it has the undesirable effect of raising the offense rate. We discuss other possible solutions. **JEL Codes: K14, K42, M15**.

[†] Author list in alphabetical order. Corresponding author: Qiu-Hong Wang, qhwang@mail.hust.edu.cn. Hui: Hong Kong University of Science and Technology; Kim: National University of Singapore; Wang: Huazhong University of Science and Technology. We thank seminar participants at the National University of Singapore for helpful comments and suggestions. We gratefully acknowledge financial support from the Natural Science Foundation of China, project 71001042, and the Hong Kong Research Grants Council, project GRF 642411.

The effect of law enforcement on deterring harmful acts is a key question of interest to policy makers. The economic analysis of criminal behavior suggests that potential perpetrators make rational decisions when deciding whether to undertake a harmful act, and so standard economic tools to study choices can be readily extended to analyze crime and the impact of law enforcement (Becker, 1968; Ehrlich, 1973b). However, empirical research faces two challenges. First, besides deciding whether to undertake a harmful act, potential perpetrators also choose *to what extent* to carry out the act.[1] Undeterred perpetrators may increase the magnitude of their malicious acts in response to law enforcement,[2] and so, for optimal deterrence, the expected sanction of a more serious offense should exceed that of a less serious offense, i.e., there should be "marginal deterrence" (Stigler, 1970). The marginal deterrence theory suggests that any observed decrease in crime rate due to law enforcement may not imply reduced cost of the crime to the society, because undeterred perpetrators may commit more serious offenses and inflict bigger damages on victims.

Second, potential perpetrators also choose which crimes to commit. If a new law criminalizes or increases the sanction of a certain act, people may substitute that act by other related acts (Katyal, 1997). If drink-driving is criminalized, people who drive after a party may take drugs instead of drinking alcohol, which poses similar danger to other road users. The theory of crime substitution implies that the social impact of law enforcement is not confined to the crime that the law targets. To estimate such impact, we should look beyond the specific crime under study. This poses a big empirical challenge because the data of related crimes are often not available.

Here, we take advantage of a unique setting to overcome these two empirical challenges and estimate the impact of law enforcement on deterring a new class of crime, viz.,

[1] These two decisions can be referred to, respectively, as the extensive and intensive margins of crime.

[2] Re-using the examples of Stigler (1970, page 527), *"If the offender will be executed for a minor assault and for a murder, there is no marginal deterrence to murder. If the thief has his hand cut off for taking five dollars, he had just as well take $5,000."*

cybercrime. The law that we consider is the Council of Europe's Convention on Cybercrime (COC), which criminalizes a wide set of improper behaviors related to the use of computer networks and equipment. The specific cybercrime under study is distributed denial of service (DDOS) attack, which maliciously occupies the resources available to a computer so that the computer cannot serve its original purpose.[3]

We compiled a dataset of DDOS attack at the country level, including the duration and number of data packets generated in each of the offenses. We could overcome the first empirical challenge related to marginal deterrence because, other than crime (DDOS attack) rate, we also observe the intensity (magnitude) of the attacks to each country. So, we can estimate how enforcement of the COC had affected the extensive and intensive margins of DDOS attack.

Further, the COC practically criminalizes all cybercrimes, and so its scope is much broader than the law enforcement efforts studied in the prior literature. This wide coverage allows us to precisely quantify the impact of enforcing the COC in terms of deterring DDOS attack, without worrying about substitution by other cybercrimes, and so, effectively eludes the second empirical challenge described above.

Our dataset comprises records of daily DDOS attacks targeting victims (computers) in 240 countries in 177 days from 2004 to 2008.[4] By conducting a battery of identification and falsification tests, we find insignificant evidence of deterrence in the general, "crime rate reduction" sense. Specifically, enforcing the COC could have reduced the chance for

[3] In general, a denial of service attack is characterized by "an explicit attempt by attackers to prevent legitimate users of a service from using that service". Usually, to crash a victim's service, perpetrators would first take control of a large number of vulnerable hosts on the Internet and organize them into a "zombie" network (often called botnets). These "zombies" would then launch coordinated attacks against the victim (hence "distributed" denial of service, DDOS). Common DDOS attacks exhaust consumable but scarce and non-renewable resources of a service, such as network bandwidth, memory, or central processing unit (CPU) time. Therefore, from a perpetrator's perspective, the success of a DDOS attack hinges greatly on the total number of data packets that can be flooded to the target in a fixed unit of time. For a brief introduction, see Computer Emergency Readiness Team (CERT), *Denial of Service Attacks*. http://www.cert.org/tech_tips/denial_of_service.html.

[4] The data of some regions, for example, Macao and U.S. Virgin Islands, were separately recorded as different countries in our dataset. For simplicity, we refer to these regions as "countries".

a country to be selected for DDOS attack by an insignificnat 2.5%. However, in countries eventually attacked, the perpetrators committed significantly more serious offenses, in the sense of a 43-52% increase in intensity. These seemingly conflicting outcomes indicate that, consistent with predictions of the marginal deterrence theory, the COC had deterred minor but provoked more serious DDOS offenses.

Further, we find evidence that marginal deterrence can be better achieved by raising the standard of criminalization, and that perpetrators responded more sharply to COC enforcement in countries with better Internet infrastructure. Overall, although enforcing the COC may help reduce DDOS attack rate, it might stimulate more intensive attacks too. Since the loss of a country depends on both the chance and intensity of the attack, the net impact of enforcing the COC on deterring DDOS attack is ambiguous.[5]

This study is among the pioneering empirical study of crime deterrence utilizing a large, country-level panel dataset of real offenses that overcomes the challenges posed by lack of quality data to account for marginal deterrence and crime substitution. Our key strength is that our empirical framework and data allow us to demonstrate the co-existence of seemingly contradictory effects, that criminalization may deter some offenses but yet stimulate more severe violations. This supports the lack of marginal deterrence, instead of other theories such as brutalization, stigmatization, or defiance (Nagin, 1998; Kirchgässner, 2011), as one plausible explanation for the previous findings that crime rate seemed to not respond to, and sometimes even increased in, law enforcement or expected legal sanction (Shepherd, 2005; Yang and Lester, 2008).

The other strength of this research is the context. All data were collected from the field. The COC has a fortuitously wide scope, which eases the concern on substitution of DDOS attack by other cybercrimes because they are similarly criminalized and sanc-

[5] Suppose that country A will be attacked with a chance of 0.4 and the attack would comprise 10,000 packets, and that country B will be attacked with a chance of 0.2 and the attack would comprise 20,000 packets. Then, the "crime rate" will be higher in country A than country B (chance of 0.4 vis-a-vis 0.2), but the expected packets generated for the attack will be identical (both 4,000 packets).

tioned under the COC. Our data were captured across multiple countries, in real-time, by an independent third party, and so we observed direct perpetrator actions instead of processed data by law enforcement agencies or self-reported data from victims. These parties may have incentives to distort the attacks or the damages inflicted.

Finally, this study contributes to the economics of information security which faces a paucity of field data especially on real hacker attacks. Our findings suggest that effective marginal deterrence is important for cybercrimes, which have posed significant challenges to the criminal justice system because of their intrinsic difference from conventional crimes in the physical world (Brenner, 2006; Calderoni, 2010). For such an emerging class of crime, quality empirical evidence is important to informing government policy. This paper provides such evidence from a field setting.

The paper is organized as follows. The next section surveys the related literature and articulates the challenges faced by previous research. Then, we provide an overview of the COC. The following section describes our dataset, followed by the empirical framework and the variables used in the regressions. We then report the estimation results, together with a battery of identification, falsification, and robustness tests. We conclude the paper with some implications and suggestions for future research.

I. Related Literature

The prior empirical literature has found contradictory evidence on the deterrence effect of criminal sanction and general law enforcement. Support for the deterrence effect has been found for capital punishment and execution (Ehrlich, 1973a, 1977; Shepherd, 2005; Yang and Lester, 2008), gun-carrying laws (Lott and Mustard, 1997; Bronars and Lott, 1998), and in enforcement against rape and other sexual offenses (Vaillant and Wolff, 2009),[6] but counter evidence has also been observed (see, e.g., Black and Nagin, 1998; Ayres and

[6] See, also, the survey by Nagin (1998).

Donohue, 2003; Donohue, 2004; Kirchgässner, 2011). Such inconsistent findings may be due to outliers (Black and Nagin, 1998), use of alternative econometric specifications, sampling, and data (Shepherd, 2005; Yang and Lester, 2008), and psychological mechanisms such as brutalization, stigmatization, and defiance (Sherman, 1993; Nagin, 1998; Shepherd, 2005; Bouffard and Piquero, 2010; Kirchgässner, 2011).

Perhaps due to lack of delicate offense data, the empirical literature on crime deterrence is not well connected to the theoretical analyses. In particular, inspired by Stigler (1970), a large body of theoretical research analyzes how potential perpetrators decide to what extent to carry out a harmful act (Polinsky and Shavell, 2000). The general insight is that in some conditions marginal deterrence requires graduated enforcement against different extents of offenses (Mookherjee and Png, 1992, 1994; Wilde, 1992; Shavell, 1992). Lacking such graduated enforcement, an enforcement against a harmful act may incentivize perpetrators to switch to more harmful acts. Similarly, lowering the standard of proof for conviction would lead to criminalization of minor offenses but imposes no additional penalty on more serious offenses (Ognedal, 2005), and so may encourage determined perpetrators to escalate their offenses. A failure in marginal deterrence may lead to ambiguous predictions of the impact of law enforcement, because, while the number of minor offenses may decrease, the number of major offenses may increase. Hence, prior empirical studies of deterrence using single definitions of crime rate, such as murder, drink driving, or drug dealing rates (Nagin, 1998) may not reveal the holistic impact of the enforcement. This could lead to variously contradictory conclusions.

To test whether perpetrators select the severity of an offense and whether marginal deterrence is necessary, in addition to crime rate, we also need to observe the magnitude of the offenses. Studying both crime rate and magnitude could also help test psychological mechanisms, such as brutalization, stigmatization, or defiance (Nagin, 1998; Kirchgässner, 2011) as alternative explanations for changing crime rates with law enforcement because, if these psychological explanations were correct, they should apply to all minor and serious offenses (instead of only to serious offenses).

To our knowledge, the only published empirical research that separately considered crime rate and the magnitude of offense is the study of Ekelund et al. (2006). Using state-level data between 1995 and 1999, they found that single murder rate had decreased but multiple murder rate had increased with execution. However, their study had two limitations. First, their dataset contained only 255 observations across 51 states, and so it was difficult to control for state or time effects, or to conduct efficient statistical tests. Second, they studied multiple murder rate but not the actual number of murders. So, technically, they studied how executions affected different types of criminals (those who committed single vis-a-vis multiple murders) instead of the actual number of murders committed after some of the states had imposed execution.

Our unique setting allows us to track the offenses in each country, including their magnitude. So, we do not face the limitation of Ekelund et al. (2006), and could conduct elaborate statistical tests to examine the marginal deterrence theory. Further, our studied enforcement, the COC, is general and applies to all cybercrimes. We could identify how it affected DDOS attacks without worrying about substitution by other cybercrimes. This is a unique advantage over the prior literature.

II. The Convention on Cybercrime

Cybercrimes pose new challenges to law enforcement because they often are virtual and not physically grounded, evolve over time, involve perpetrators and victims from multiple countries, and use information technologies to aggravate their impacts (Katyal, 2001; Brenner, 2006; Calderoni, 2010). It is often difficult to identify, track, apprehend, and convict perpetrators in the cyberspace. Hence, new legislations that enhance investigative power and transcend territorial jurisdictions are necessary for effective enforcement against cybercrimes.

Drafted by the Council of Europe and adopted by the Committee of Ministers at its 109th Session on November 8, 2001, the Convention on Cybercrime is the first international legislation against criminal behaviors in the cyberspace. It provides participating countries with a substantive legal framework to address any actions against the confidentiality, integrity, and availability of computer data and systems (Keyser, 2003; Li, 2007).[7] The COC has been open for signature since November 23, 2001, and was first entered into force by Albania, Croatia, Estonia, Hungary, and Lithuania on July 1, 2004. As of January 2013, 47 countries have signed the COC, and 38 have ratified and enforced it. Figure 1 presents the signature and ratification of the COC over time.

Figure 1: Signature and Enforcement of the Convention on Cybercrime

The COC has three sets of provisions.[8] First, it requires ratifying countries to criminalize a wide set of activities including illegal access and interception, data and system interference, misuse of computing devices, etc. The definition of crime is loose and so it covers almost all malicious use of computer data and systems. It also requires ratifying countries to establish the corporate liability of offenses and the appropriate sanctions. Second, to facilitate detection, investigation, and prosecution, the COC requires ratifying countries to adopt procedural measures such as expedited preservation of data, and grants the legal authority to issue data production orders, search, seize, and collect real-time traffic data, and intercept other related contents. Third, the COC establishes clear jurisdiction for any cybercrime offenses and outlines the principles for international cooperation covering extradition, mutual assistance, information sharing, transborder access to data, etc. Taken together, these three sets of provisions increase the certainty and celerity of apprehension through collaborative enforcement across countries, and also the

[7] Other than 41 Council of Europe member states, four non-member states including Canada, Japan, the United States, and South Africa also participated in drafting the COC.

[8] The full version of the COC and its explanatory report are available on the Council of Europe's Web site, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

penalty through criminalizing computer-related offenses.

Despite the COC's obvious purpose, it had taken 3 to 11 years for many countries to progress from signature to ratification, and some (e.g., Canada, Greece, Sweden, and Turkey) are still in the process of ratification. This could be due to several reasons. First, to ratify the COC, a signatory country has to adopt legislations that bring its domestic laws into accord with COC's penal and procedural requirements (Li, 2007). This could be a significant undertaking.[9] Second, the signatory countries may not have consensus on the definition of criminal offenses.[10] It may take time for a signatory country to deliberate if it wants to adopt the COC in full. In fact, as of the beginning of January 2013, among the 38 countries that have ratified the COC, 21 have made reservations concerning the standard of criminalization, surveillance, mutual legal assistance, etc. Table 1 lists the countries with reservations on each specific Article of the COC.

Table 1: Reservations on the Convention on Cybercrime

There has been evidence of heightened enforcement against cybercrimes after COC enforcement. For example, in 2007, a Russian man was convicted for launching DDOS attacks against Estonia's government services (Vamosi, 2008). Estonia had enforced the COC in 2004. In 2010, a programmer in the United States was tried and convicted for his crippling of rollingstone.com in 2008 with a DDOS attack involving 100,000 computers worldwide. The United States had enforced the COC in 2007 (Goodin, 2010). In 2011,

[9] For example, to comply with the COC, the Finnish legislature had to add new provisions to its Penal Code concerning information processing systems and possession of instruments used for cybercrimes, and to establish the corresponding liability (Li, 2007). The Swedish government had to harmonize Swedish laws regarding punishment of forgery, data interference, child pornography, unlawful use of computers and monitoring of computer information, and violation of copyright and other related rights. The Japanese government had also changed its laws to address COC's data retention and provision requirements and general requests for cooperation in investigations (Library of Congress, 2009).

[10] Article 42 of the COC allows participating countries to provide additional elements and make reservations on Articles 3-4, 6, 9-11, 14, 22, 29, and 41 regarding criminalization, jurisdiction, procedural provision, and mutual assistance. For example, while data interference as stated in Article 4 of the COC is considered a criminal offense in Denmark, Germany, and many other Council of Europe member states, Azerbaijan, Lithuania, Norway, and the United States have reserved the right to criminalize this conduct only when it causes harm as determined in accordance with applicable domestic laws.

a German man was convicted for cyber-extortion with threats of DDOS attack against six online bookmakers. A similar DDOS attack was not against the German law in 2006 (Zorz, 2011). Germany had enforced the COC in 2009.

The COC has also raised concerns among the hacker community. We have traversed some posts on Hack Forums,[11] one of the most popular online forums among the hacker community. The following are some excerpts:

- "*I live in a small town in Romania. 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 why this happened: that was because we just joined...European Union and 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" in 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" in 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" in 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...As of 2007, Croatia integrated this into local laws...All of the offences proscribed in the Cybercrime Convention (to which Croatia is a State Party and which has been in force in Croatia since 1 July 2004), with the exception of offences that can generally be described as cyberterrorism, are incorporated into the domestic legal framework*," (posted by user "matemisic" in November 2011).

[11] See http://hackforums.net/. In the month of October 2011, Hack Forums had 58,332 unique active users, 9,320 new threads/topics, and 74,590 new replies. It was the top-ranked Web site in the category "Hacking–Chats and Forums" in Alexa, which publishes comprehensive Web traffic analysis on the Internet. Hack Forum's global traffic rank was 4,647 in May 2013.

Posts like the above are common on Hack Forums, which implies that the enforcement of the COC has been well recognized. In fact, it could have been instrumental in convicting perpetrators. For this study, the disparate timing of COC enforcement by different countries provides an important degree of freedom to identify its impact on cybercrime deterrence.[12] The reservations made by a subset of the countries further serve as heterogeneous treatments, which also help identify its impact.

III. Data

We obtained a set of random DDOS attack data from the Cooperative Association for Internet Data Analysis (CAIDA, 2004-2005, 2006, 2007, 2008a). The dataset contains response data packets sent by DDOS attack victims to spoofed traffic for at least a week-long period in every quarter between 2004 and 2008.[13] As stated in CAIDA (2004-2005): "*When a denial-of-service-attack victim receives attack traffic with spoofed source IP addresses, the attack victim cannot differentiate between this spoofed traffic and legitimate requests, so the victim replies to the spoofed source IP addresses. These spoofed IP addresses were not the actual sources of the attack traffic, so they receive responses to traffic they never sent. By measuring this response traffic (called backscatter data) to a large portion of IP addresses (roughly a /8 network), it is possible to estimate a lower bound for the overall volume of spoofed source denial-of-service attacks occurring on the Internet.*"[14]

[12] If all signatory countries had enforced the COC at the same time, then it is difficult to separate its impact from unobserved time-specific shocks. Other quasi-experimental techniques, such as the regression discontinuity design (Lee and Lemieux, 2010), may then be necessary. However, the use of such designs may require truncating the data and so lead to losses of statistical power.

[13] Internet traffic is mostly managed by the transmission control protocol (TCP), which uses a three-way handshake process to establish connections between different Internet hosts. This three-way handshake process necessarily requires servers (in our context, DDOS attack victims) to respond to every client (in our context, perpetrator). Most perpetrators would falsify the source Internet Protocol (IP) addresses to masquerade the origins of their attacks. Therefore, the source IP addresses of attack data packets, or, equivalently, the destination IP addresses of response data packets sent by DDOS attack victims, are usually not reliable in identifying or tracing the perpetrators.

[14] CAIDA records unsolicited traffic through the UCSD Network Telescope, a globally routed /8 network comprising approximately 1/256th of all IP addresses. Such traffic can result from a wide range of events,

For each victim IP address, CAIDA aggregates the backscatter packets by hour. By locating the country of each victim IP address, we could characterize the DDOS attacks targeting each country on a daily basis by the number of unique victim IP addresses, the total number of data packets sent by each victim (to respond to the spoofed attack packets), and the total time of the attacks. From these data, we could compute the average intensity of the attacks received by each DDOS victim in each of the studied countries. Table 2 shows the time periods covered in our dataset. Figure 2 depicts the distribution of DDOS attacks across countries.

Table 2: Time Periods Covered

Figure 2: Distribution of DDOS Attacks

In addition to the DDOS attack data from CAIDA, we also collected the status of COC enforcement from the Council of Europe's Web site, and other demographics data from the Global Market Information Database (GMID) and the database published by the Central Intelligence Agency (CIA). We collected country-level indexes of quality of governance from Worldwide Governance Indicators (WGI), and data on some conventional crimes from the United Nations Office on Drugs and Crime (UNODC) and the U.S. Department of State (USDOS). Table 3 presents the sources and descriptive statistics of our data. Table 4 presents the correlations.

Table 3: Descriptive Statistics

Table 4: Correlations

including backscatter data from randomly spoofed source DDOS attacks. Because DDOS attack victims respond to every received request, the number of response packets sent by them to the (spoofed) IP addresses under the UCSD Network Telescope should correlate highly with the extent of DDOS attacks. For details of UCSD Network Telescope, see http://www.caida.org/projects/network_telescope/. The use of backscatter data to measure DDOS attack is well established in the field of computing. See, for example, Moore et al. (2001) and Mao et al. (2006) for applications.

On average, 335 unique IP addresses in each of the 240 countries were attacked by DDOS for a combined total of 388 hours per day, but there were substantial variations across countries. The standard deviations for number of unique victim IP addresses and total hours of attack were 3,122 and 3,374, close to ten times of the respective means. Each victim IP address was attacked by an average of 1,411 packets.[15] 23 countries had enforced the COC during the sampling window. The countries were less varied in terms of demographics. In particular, there were around 0.242 Internet users per capita, and the standard deviation was around 0.245.

IV. Model and Variables

The solid lines in Figure 3 depict the average number of unique IP addresses attacked, time of attack, and number of packets generated during the attacks *per day* in each of the countries that had enforced the COC during each quarter in the sampling window (second quarter of 2004 to last quarter of 2008). The shaded areas correspond to periods when the COC was enforced. Apparently, COC enforcement had decreased DDOS attacks in Bosnia and Herzegovnia, Finland, Norway, and the United States, and had increased DDOS attacks in Armenia and Iceland. No notable effect was observed in the other countries, particularly Bulgaria, Denmark, and Netherlands.

Figure 3: DDOS Attacks Over Time

However, the patterns are quite different if we focus on attack intensity. The dotted lines in Figure 3 plot the average time of attack per victim IP address and the average number of packets generated per victim IP address over the same period. In Bosnia and Herzegovnia, Finland, Norway, and the United States, the countries wherein the total

[15] Referring to Footnote 14, the CAIDA dataset contains random spoofed source DDOS response packets recorded on roughly 1/256th of all IP addresses. Most of these 1/256th IP addresses are not allocated by providers and are widely considered as Internet “black hole” or “darkspace”. This explains the relatively small number of packets per victim recorded in our data.

time and number of packets had both decreased after COC enforcement, the average time and number of packets in fact did not decrease, or even increased slightly, after the enforcement. Similarly, the average attack rate seemed to have increased slightly in Bulgaria, Denmark, and Netherlands, and somewhat significantly in Armenia and Iceland. These trends illustrate the importance to consider multiple measures of "crime rate" when estimating the impact of law enforcement.

Statistically, the conventional approach to estimating the impact of law enforcement would be to relate crime rate with the enforcement. In our context, the crime rate can be measured by potential violation against victims, e.g., the probability of getting attacked. Hence, we could estimate the following equation:

$$\theta_{it} = \gamma_1 + \gamma_2 K_{it} + \mu_i' + \tau_t' + \epsilon_{it}, \tag{1}$$

where θ_{it} is an indicator denoting whether country i was attacked in day t, K_{it} is an indicator that equals 1 if the COC had been enforced in country i in day t, and 0 otherwise, μ_i is a vector of dummy variables capturing country-specific effects, τ_t capture time trends, and ϵ_{it} captures idiosyncratic errors.[16]

As reported in Table 5, column 1, using a random-effects probit specification, the effect of COC enforcement was negative but insignificant ($\gamma_2 = -0.135, p = 0.21$).[17] So, using probability of violation in a country to measure "crime rate", one might conclude that COC enforcement was ineffective.

Table 5: Estimations using Differnt Definitions of Crime Rate

However, we can also measure crime rate by number of victims. Let θ_{it} be the

[16] To capture time trend, for *each* data collection period in Table 2, we constructed a day index and included it and its square in the estimation. For example, day(period 1) = 1 for May 26, 2004, day(period 1) = 2 for May 27, 2004, day(period 2) = 1 for August 26, 2004, day(period 2) = 2 for August 27, 2004, and so on. Altogether, we included 21 periods × 2 = 42 time trend variables.

[17] The random-effects probit model is commonly used in the literature because a fixed-effects probit model may give biased estimates depending on panel sizes (Greene, 2002).

number of victim IP addresses, divided by number of Internet hosts to adjust for country size. By estimating a fixed-effects ordinary least squares (OLS) regression, Table 5, column 2 shows that the effect of COC became significant ($\gamma_2 = -0.639, p < 0.01$). We might now conclude that COC enforcement had successfully deterred DDOS attacks.

Yet, suppose that θ_{it} denotes the total number of packets generated per Internet host during the DDOS attacks. Then, Table 5, column 3 shows that the result was strikingly different. The effect of COC enforcement became positive and close to statistically significant ($\gamma_2 = 0.202, p < 0.1$). If we let θ_{it} be the number of packets per victim IP address, then the positive effect of COC enforcement would become even more significant ($\gamma_2 = 0.344, p < 0.01$). So, the conclusion would now be opposite – COC enforcement had increased DDOS attacks.[18]

The problem, clearly, is that linking offenses to law enforcement in a single regression could account for either the crime rate or magnitude of offense, but not both. To gain a holisitc view of how law enforcement affected criminal offenses, both the crime rate and magnitude of offense should be accounted for in the estimation. This is feasible here as we have an unambiguous measure of intensity – the number of packets generated against each DDOS attack victim.[19]

Accordingly, we modeled crime rate as the probability for a country to be attacked by DDOS on a daily basis. We modeled attack intensity by the average number of packets generated against each victim IP address.

There was one final caveat. In the CAIDA dataset, the backscatter packets were

[18] The estimations in Table 5 did not include any demographic or control variables. As we shall see later, adding demographic or control variables would not affect the conclusions. We took logarithms for all dependent variables in Table 5, columns 2 to 4.

[19] In principle, the same perpetrator could attack multiple victims at the same time, and so the number of victim IP addresses may also capture attack intensity (e.g., a single wave of DDOS attack in July 2009 had targeted 27 government agencies and commercial Web sites in Korea and the United States; see Choi and Markoff 2009). Since we could not ascertain whether the attacks recorded in our dataset came from the same perpetrators, we avoided using number of victim IP addresses as either attack rate or intensity measure in the subsequent discussion.

observed only for countries that were attacked. Some countries may be more/less likely attacked than others because of systematic factors, one of which could be enforcement of the COC. Hence, the observation of the backscatter packets maybe non-random, which implies that there could be systematic omission of observations in the regression with attack intensity as the dependent variable. It is well known that in such a regression the conditional expectation of the error term would not equal zero without considering the possible impact of how the observations were "selected" (Heckman, 1979). The estimated parameters could be biased and inconsistent, leading to invalid statistical inference (Putsis and Bayus, 2001; Ghose and Han, 2011). Essentially, the non-random inclusion of countries for DDOS attacks, plausibly due to heterogeneous country characteristics, could lead to sampling bias.

We addressed such sampling bias through a two-step estimation procedure catered for panel data proposed by Wooldridge (2001, page 564, Procedure 17.1) and adopted in previous studies (Putsis and Bayus, 2001; Ghose and Han, 2011). In step 1, we estimated a random-effects probit "selection" model to examine what affected the probability for a country to be selected for DDOS attacks. We then calculated the selection bias correction term from the estimates (Heckman, 1979).[20] In step 2, we included such correction term in a fixed-effects OLS "outcome" model to obtain unbiased estimates of the effect of COC enforcement on DDOS attack intensity.

Econometrically, we formulated the two-step model as follows:

$$\text{Selection: } s_{it} = \alpha_1 + \alpha_2 K_{it} + \alpha_3' x_{it} + \alpha_4' z_{it} + \sigma_i' + \psi_t' + u_{it}, \tag{2}$$

$$\text{Outcome: } r_{it} = \beta_1 + \beta_2 K_{it} + \beta_3' x_{it} + \rho \Phi_{it} + \mu_i' + \tau_t' + \epsilon_{it}, \tag{3}$$

where s_{it} is a binary variable that equals 1 if DDOS attack was observed in country i in

[20] The selection bias correction term equals the ratio of the population density function to the cumulative density function for the relevant choice in the selection equation.

day t, r_{it} is the average number of packets per victim IP address in country i in day t, K_{it} indicates COC enforcement, x_{it} is a matrix of demographic and control variables, z_{it} is a set of variables that satisfy the exclusion restriction for the outcome model, Φ_{it} is the selection bias correction term computed from equation (2), σ_i and μ_i denote country-level random and fixed effects, ψ_t and τ_t capture time trends (see footnote 16 for their construction), and u_{it} and ϵ_{it} are idiosyncratic random errors.

In equations (2) and (3), s_{it} and r_{it} are correlated because r_{it} is observed and exceeds 0 if and only if $s_{it} = 1$. The random effects in the selection model, σ_i, and the fixed effects in the outcome model, μ_i, control for unobservable country-level heterogeneities, which may include culture, socio-economic characteristics, state of development of information technologies, etc. The time trends, ψ_t and τ_t, capture time-related shocks that applied to all countries, such as any possible seasonality in DDOS attacks. Because Internet hosts may affect the chance of DDOS attacks but not the intensity of the attacks directed at each victim, we included in z_{it} the number of Internet hosts and its square as exclusion restrictions (Wooldridge, 2001).

If COC enforcement was effective, we would expect $\alpha_2 < 0$ and $\beta_2 < 0$. By contrast, $\alpha_2 < 0$ and $\beta_2 > 0$ would imply that the COC had failed to achieve marginal deterrence, although it might have deterred minor DDOS offenses.[21]

Following the literature (e.g., Ekelund et al., 2006; Png et al., 2008), we included relevant demographic and control variables in x_{it}. Specifically, we included gross domestic product (GDP) per capita, unemployment rate, and number of higher education students per capita to capture whether a country was attractive for DDOS attack (Korgaonkar and Wolin, 1999). We also included variables from WGI to control for the effectiveness

[21] It is instructive to note that our panel unit was country instead of individual IP address or perpetrator. We did not use IP address because the CAIDA dataset does not include any information on un-attacked IP addresses, and so we could not define a complete population if IP address was used as the unit. We did not conduct the estimation at the perpetrator level because we could not identify the real perpetrators (most of the destination IP addresses in the backscatter packets were spoofed). Also, each perpetrator could attack multiple IP addresses in multiple countries simultaneously, which may not satisfy the theoretical assumptions in most choice models.

of jurisdictional systems and quality of enforcement agencies. These included 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).[22] The six governance indicators were normalized with mean 0 and standard deviation 1. They spanned over 200 countries and varied on a yearly basis.

Specific to the context of cybercrime, we controlled for the influence of information technology infrastructure and diffusion in each country by including, on per-capita basis, the number of Internet users, number of integrated services digital network (ISDN) subscribers, and availability of digital telephone lines. We included land area per capita to approximate the average physical distance between people. These variables may affect the risk of exposure to computer crime victimization.

We constructed all demographic and control variables, except the governance indicators, in per-capita terms, and used the double-log specification as it often fits economic data better (Wooldridge, 2006, p. 197-200).[23] Other than group-wise heteroskedasticity which is commonly observed in panel data, our dataset was subject to cross-sectional or spatial interdependencies due to the global nature of cyber attacks (Kim et al., 2012).[24]

[22] According to Kaufmann et al. (2010, page 4), Control of corruption captures "perceptions of the extent to which public power is exercised for private gain, including both petty and grand forms of corruption, as well as "capture" of the state by elites and private interests". Government effectiveness captures "perceptions of the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies". Political stability and absence of violence/terrorism captures "perceptions of the likelihood that the government will be destabilized or overthrown by unconstitutional or violent means, including politically motivated violence and terrorism". Regulatory quality captures "perceptions of the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development". Rule of law captures "perceptions of the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, property rights, the police, and the courts, as well as the likelihood of crime and violence". Voice and accountability captures "perceptions of the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and a free media".

[23] Where necessary, we added 1 before any size adjustment to avoid logarithm of zeros. For brevity, we do not mention the logarithms in discussing the subsequent results.

[24] The Breusch-Pagan Lagrange Multiplier test in the outcome model rejected the null hypothesis of homoskedasticity across countries ($\chi^2 = 3,661.59$, $p < 0.01$). All three tests proposed by Frees (1995), Friedman (1937), and Pesaran (2004) rejected the null hypothesis of no cross-sectional dependency among at least 45 countries that had been attacked every day in our sampling window (all $p < 0.01$). The average

Accordingly, in all estimations of the outcome model, we used spatial correlation consistent standard errors (Driscoll and Kraay, 1998), which should be robust to general cross-sectional and temporal interdependencies.

V. Results

We first estimated the two-step model in equations (2) and (3) by excluding all explanatory variables except COC enforcement and the country and day effects. This specification allowed us to avoid pruning DDOS attack data because of missing observations on some demographic and control variables.[25] We used the average number of packets generated per victim IP address as the intensity measure in the outcome model. As reported in Table 6, column 1, the coefficient of COC enforcement was negative but not statistically significant in the selection model ($\alpha_2 = -0.135$, $p = 0.21$). It was positive and statistically significant in the outcome model ($\beta_2 = 0.715$, $p < 0.01$).

Table 6: Main Estimation Results

We next estimated another specification which replaced COC enforcement by the demographic and control variables. Because of missing data in some of these variables, the sample size decreased by more than 60%. As reported in Table 6, column 2, countries with higher GDP per capita tended to be more intensely attacked, possibly because such countries had higher incomes and so were more attractive to perpetrators (Korgaonkar and Wolin, 1999). Similarly, countries with more higher education students had a higher chance of getting attacked, and the attacks were more intensive too (in the sense of involving more packets per victim IP address). If we assume that perpetrators often launch DDOS attacks against domestic targets, then the positive effects here could be due

cross-sectional correlation of the regression residuals was 0.130.

[25] The demographic data of many countries, particularly those without an independent sovereign state, such as Cook Islands, Isle of Man, British Virgin Islands, etc., and those with less developed economies, such as Honduras, Montenegro, Vietnam, etc., were not available.

to better educated people having more knowledge about computing and cyber attacks.[26] By contrast, unemployment rate had a positive effect only in the selection model. This is consistent with unemployed people having lower opportunity cost of time but not better skills or knowledge to launch intensive attacks.[27]

The availability of digital main lines and number of ISDN subscribers had positive effects in the outcome model. This seemed plausible given that organizations were more likely to subscribe to digital main lines and ISDN, and were more prone to DDOS attacks too. Digital main lines and ISDN could also provide higher data transfer speeds and so could handle more attack packets. The average land area per capita was negatively correlated with DDOS attack intensity, possibly because it was more difficult to flood a target with many packets when the distance between the attacking and victim computers increases (and so the attacking and backscatter packets may have to go through more intermittent "hops").

Among the six governance indicators, control of corruption had a negative effect in the selection model. Political stability and absence of violence/terrorism had a negative effect in the selection model but a positive effect in the outcome model. Regulatory quality had negative effects, and rule of law had positive effects in both the selection and outcome models. While some of these results may seem counter-intuitive, perpetrators could have substituted other criminal activities in the physical world by cybercrimes, particularly when such criminal activities were more regulated or suppressed in countries with better governance quality. So, it could well be possible for some of the governance indicators to be positively correlated with DDOS attacks.

Table 6, column 3 presents the estimation results of the full model, which included the COC enforcement and all demographic and control variables. The results were largely

[26] In reality, a smart perpetrator can avoid getting caught by exploiting "zombie" computers to launch the DDOS attack from other countries.

[27] Prior research has also found a positive correlation between unemployment rate and violations. See, for example, Raphael and Winter-Ebmer (2001).

consistent with the earlier specifications. COC enforcement had an insignificant negative effect in the selection model ($\alpha_2 = -0.192$, $p = 0.15$) but a statistically significant positive effect in the outcome model ($\beta_2 = 0.511$, $p < 0.01$). By averaging the predicted probabilities across all observations, the marginal effect of COC enforcement in reducing the attack probability in the selection model was -0.025 (s.e. 0.018), which was economically small and statistically insignificant. The elasticity in the outcome model was, however, 0.511 (s.e. 0.065). So, enforcing the COC increased the average intensity of attack by 51.1%. This was statistically and economically significant.[28]

To buttress our findings, we considered alternative DDOS attack motivations. In general, perpetrators could inflict damage on a victim by two means. First, they could flood the victim with many packets persistently in the hope of causing a long downtime. Our dependent variable in the outcome model, the average number of packets generated per victim IP address, should capture such motivation. Second, perpetrators could launch focused attacks in a short period of time in the hope of successfully incapacitating the victim. To capture this motivation, we could measure attack intensity by the number of packets generated per victim IP address *per hour*. This should capture the concentration of DDOS attacks per fixed unit of time.

Table 6, column 4 reports the results of estimating the new outcome model, using the revised intensity measure as the dependent variable. The results were consistent with those in column 3. COC enforcement had a strong positive effect on attack intensity, with an elasticity of 51.9% (s.e. 5.8%).

Because some perpetrators may concurrently attack multiple IP addresses, another measure for attack intensity would be, simply, the number of packets generated by the DDOS attacks per hour (regardless of number of victims). Table 6, column 5 reports the

[28] To test the exclusion restrictions, as an experiment we included the number of Internet host and its square as independent variables in the outcome model and found that, indeed, they were not statistically significant. For brevity, we do not report the results here.

results. The elasticity of COC enforcement in the outcome model was 49.3% (s.e. 6.2%), very close to the previous estimates.

We also checked the robustness of our findings by modeling time specific effects using 176 day dummy variables instead of the 42 trend variables. Table 6, column 6 shows that the results were largely similar. The effect of COC enforcement was insignificant in the selection model, with a marginal effect of -0.015 (s.e. 0.009) on the predicted probability for a country to be attacked. Its effect continued to be significant and positive in the outcome model. The elasticity was around 43% (s.e. 6.7%).

Finally, to critically assess whether our results were related to marginal deterrence, we exploited heterogeneous treatments, that some countries had made reservations on the COC concerning the standard of criminalization, surveillance, or mutual legal assistance (see Table 1). These reservations may increase the standard of proof for conviction, which tends to increase the expected sanction of serious offenses *relative to* minor offenses, an essential requirement of marginal deterrence (Shavell, 1992; Mookherjee and Png, 1994; Ognedal, 2005). Accordingly, if the effect of COC enforcement reported above were due to lack of marginal deterrence, then we would expect its effect on DDOS attack intensity to be smaller in countries that had declared more reservations.

We added the number of reservations interacted with COC enforcement as an independent variable in both the selection and outcome models. As reported in Table 6, column 7, indeed, the coefficient of numebr of reservations interacted with COC enforcement in the outcome model was -0.137 ($p < 0.01$). For each additional reservation on the COC, the countries tended to be attacked by 13.7% (s.e. 3.3%) fewer packets. This indicated that it was the lack of marginal deterrence that caused an increased attack intensity in countries that had enforced the COC.

Overall, we preferred the ("main") specification in Table 6, column 3. It used an unambiguous measure of attack intensity and a simple structure to model country-level heterogeneities and time trends.[29]

A. Identification Tests

One concern of using observational data in deterrence research is reverse causation, that the criminal activity might have motivated the government to strengthen law enforcement (Ehrlich and Brower, 1987). In our context, the enforcement of the COC could be endogenous – a country might ratify the COC because it experienced more cyber attacks, and so there could have been an a priori positive correlation between COC enforcement and DDOS attacks at the country level.

Several reasons suggest that such endogeneity may not be of major concern here. First, if COC enforcement responded to DDOS attacks, then we would expect its correlations with both the probability and magnitude of the attacks to be positive. This was not the case in Table 6. In fact, as we shall see later, COC enforcement was negatively correlated with the number of victim IP addresses.

Second, as we reviewed in Section II, the COC does not address crime magnitude, and so there is no good reason to believe that its impact would be specifically on crime magnitude but not the rate of offenses. In fact, as the COC criminalizes an entire new class of crimes, if it were endogenous, it would more likely correlate positively with the probability or rate of offenses, instead of magnitude.

Third, if the positive correlation of COC enforcement and DDOS attack intensity was spurious and caused by reverse causation, then we should observe relatively flat DDOS attack rate and intensity patterns for each country in Figure 3 over time. The only variations in the attack rates and intensity should be along the vertical axis *across countries*. This is not the case in Figure 3. In many countries, the DDOS attack patterns

[29] The selection bias correction term was close to statistically significant ($\rho = -0.065$, $p = 0.06$), indicating that adjusting for non-random sampling may help obtain unbiased estimates of the effects of COC enforcement on DDOS attack intensity.

changed sharply before and after the COC was enforced.

Statistically, the country fixed effects were orthogonal to COC enforcement in the outcome model, and so should have extracted the country-level variations in DDOS attacks. They should suffice to address the endogeneity caused by reverse causation.

We buttress our analysis with two identification tests. First, we considered the per-capita number of professional judges or magistrates in a country. If COC enforcement was endogenous and caused by the prevailing significance of cybercrimes, then we would expect countries that were more bothered by cybercrimes to also increase resources on the criminal justice system. In particular, such countries would need more judges to convict perpetrators. So, the correlation between COC enforcement and DDOS attack intensity should be higher in countries with more judges.

By contrast, if the effect of COC enforcement was related to deterrence and so the expected marginal cost of violations, then we would expect its effect to be smaller in countries with more judges, because the chance for perpetrators to be tried and convicted would be higher in such countries.

We obtained yearly data on the number of professional judges or magistrates from UNODC,[30] and entered it and its interaction with COC enforcement as additional independent variables. As reported in Table 7, column 1, the effect of COC enforcement continued to be insignificant in the selection model and significant in the outcome model.[31] The number of professional judges or magistrates was insignificant in both models. Importantly for our identification strategy, the interaction of number of professional judges or magistrates with COC enforcement was negative, −0.778 (s.e. 0.171), and statistically

[30] According to UNODC, "professional judges or magistrates" means both full-time and part-time officials as at 31 December of every year authorized to hear civil, criminal and other cases, including in appeal courts, and to make dispositions in a court of law. It also includes authorized associate judges and magistrates.

[31] For brevity, we do not report the demographic and control variables in this and all subsequent tables. The coefficients of these variables were largely consistent in terms of signs, magnitude, and significance with those reported in Table 6.

significant. This served as a sharp test that the effect of COC enforcement was caused by its effect on deterrence instead of endogeneity.

Table 7: Identification Tests

Our second identification strategy exploited the heterogeneous Internet infrastructure across countries. As cybercrimes, particularly DDOS attack, involve transmission of packets between Internet hosts, a country's Internet connectivity with the rest of the world would directly empower or constrain international cyber attacks. We distinguished countries by (external) Internet connectivity measured by the total number of business relationships between autonomous systems (AS).[32]

We expected DDOS attacks targeting countries with more external AS relationships to respond more sharply to COC enforcement because it is easier to reach and so attack the hosts in such countries. The consideration of external Internet connectivity is particularly relevant for DDOS attack because its success and damage depend greatly on whether perpetrators could take control of a "zombie" network, which often comprises computers globally. Further, by design, the COC enhances international collaboration on enforcement against cybercrimes, and so it should apply particularly to countries whose environments favor cyber attacks from global sources (i.e., countries with good Internet connectivity with the rest of the world). As reported in Table 4, the correlations between external AS connections with the other country characteristics were mostly very small. So, it seemed reasonably exogenous in our setting.

We included the number of external AS connections and its interaction with COC

[32] We obtained AS data from CAIDA (2008b). The Internet consists of thousands of AS, each of which is a connected group of networks labeled by a unique AS number and belongs to a unique country. Although the Internet hosts within an AS uses a single and well defined routing policy for all Internet traffic, we could build a direct connection between Internet hosts in different AS only if the business relationship between the two AS has been established (the easiest way to understand AS is to treat it as a network managed by an Internet service provider). Therefore, the total number of business relationships between a country's AS with other countries' AS directly reflects the country's Internet connectivity. Starting from 2004, CAIDA provides a snapshot on the business relationship for each pair of AS on a monthly basis. By mapping each AS number to its country, we could calculate the total number of relationships between a country's AS with other countries' AS on a monthly basis.

enforcement as additional independent variables. The results are reported in Table 7, column 2. The effect of COC enforcement became insignificant, and the external AS connections had significant positive effects in both the selection and outcome models. Importantly for our identification strategy, the interaction of external AS connections with COC enforcement had a positive and significant effect, 0.110 (s.e. 0.028), only in the outcome model. This did not support the endogeneity or reverse causation explanation, and seemed inconsistent with other theories such as brutalization, stigmatization, or defiance too (all of which predict positive effects of COC enforcement in both the selection and outcome models irregardless of external AS connections). The evidence supported the lack of marginal deterrence for major offenses particularly in countries well-connected to the outside world.

B. Falsification

To validate the effect of COC enforcement, that it was specific to cybercrime deterrence instead of spurious correlations, we conducted several falsification exercises. First, from USDOS, we constructed a binary variable of whether a country was classified as a "money laundering or financial crimes country/jurisdiction" within our sampling window. We used it as the dependent variable in a random-effects probit regression. As reported in Table 8, column 1, the effect of COC enforcement was negative but insignificant.

Table 8: Falsification Tests

Next, from UNODC, we collected yearly statistics on theft, numbers of persons prosecuted and convicted, and number of untried/pre-trial persons held in each country.[33] Theft is a close physical counterpart to DDOS attack as it also deprives a person

[33] According to UNODC, "theft" means depriving a person or organisation of property without force with the intent to keep it. It excludes burglary, housebreaking, robbery, and theft of a motor vehicle. "Persons prosecuted" means alleged offenders prosecuted by means of an official charge, initiated by the public prosecutor or the law enforcement agency responsible for prosecution. "Persons convicted" means persons found guilty by any legal body authorized to pronounce a conviction under national criminal

or organisation of property. The prosecution and conviction data included people who committed white-collar crimes, which are good physical counterparts to cybercrimes. The number of untried/pre-trial persons held may include those committing relatively minor offenses, possibly cyber or general white-collar crimes as well.

We used each of these statistics as the dependent variable in the outcome model as specified in equation (3), keeping the same indepedendent variables except the selection bias correction term.[34] As reported in Table 8, column 2, the effect of COC enforcement was not statistically significant in any of these regressions. So, the effect of COC was specific to DDOS attack, a kind of cybercrime that it targets, but not to other conventional crimes, which it does not target.[35]

Finally, we tested the specificity of the treatment effect by replacing COC enforcement with COC signature. Because a country that signed the COC without ratification practically had not enforced it, the signature should not affect perpetrators' actions. On the other hand, COC enforcement and signature were necessarily correlated and should be driven by common factors (e.g., international politics, being members of trade organizations and unions, etc.). If the effect of COC enforcement identified above were caused by some of these other factors instead of cybercrime deterrence, then we would expect the effect of COC signature to be also significant.

law, whether or not the conviction was later upheld. "Persons held" excludes non-criminal prisoners held for administrative purposes, including persons held pending investigation into their immigration status and foreign citizens without a legal right to stay held prior to removal.

[34] It was infeasible to estimate the selection model for these crimes because all countries had recorded a positive number of offenses in every year. Because it was unlikely for these conventional crimes to exhibit spatial autocorrelation, we clustered the standard errors by country (instead of using spatial correlation consistent standard errors) in these four regressions.

[35] Because the statistics on the conventional crimes were available for fewer countries, the insignificant results could also be due to sample size (cf. those reported in Table 6). We repeated the estimation of the main specification in Table 6, column 3 by including only the countries whereby the statistics on the conventional crimes were available. The sample size became much smaller (only 5,727 observations), even than those reported in Table 8, columns 1 and 2, but COC enforcement continued to be significant in the outcome model ($\beta_2 = 0.730$, $p < 0.01$). So, sample size did not matter. In another set of falsification tests, we used assult, burglary, kidnapping, and robbery as the dependent variables. The effect of COC enforcement was always statistically insignificant. Because the nature of these crimes are different from cybercrimes, we do not report the results of these tests.

As reported in Table 8, column 3, the effect of COC signature was insignificant in both the selection and outcome models. So, we concluded that our findings in Table 6 were caused by failure of the COC in achieving marginal deterrence, not other spurious trends or unobserved factors.

C. Robustness

We checked the robustness of our findings in multiple ways. First, because many countries did not enforce the COC, to show that the effect of COC enforcement was not due to group-common characteristics, we repeated the estimation of the main specification by confining the sample to only countries that had enforced the COC. The identification of the COC effect would then rely solely on variations in DDOS attacks over time (instead of across the panel unit, country). Compared with the samples used in Table 6, the test using this restricted sample should be more stringent.[36]

Second, we conducted another estimation using only member countries of the Council of Europe. These countries were more likely to enforce the COC, and they may share common characteristics too. If some of these characteristics were correlated with the COC, then its effect could be spurious. Third, we checked whether the effect of the COC was persistent over time by lagging the time of enforcement by 6 and 12 months. Fourth, to ensure that our results were not rendered by outliers, in the next two estimations we excluded, respectively, the countries that were attacked in only one day, and the countries that were attacked in every day in the sampling window.

Table 9 reports the estimation results. The effect of COC enforcement was very consistent – always insignificant in the selection model and significant in the outcome model. The elasticity of COC enforcement in the outcome model was stable, ranging from 47% to 56%, except in the specification excluding the frequently attacked countries,

[36] This also served as another powerful test to rule out the reverse causation explanation.

where it was larger ($\beta_2 = 1.076, p < 0.01$). Apparently, the failure of the COC in achieving marginal deterrence was more pronounced in less frequently victimized countries.

Table 9: Robustness

Finally, we tested if the effect of COC enforcement was actually due to unobserved country-specific developments over time. We included the interaction of each of the 23 COC country dummy variables with the 42 time trend variables in the regressions. With these $23 \times 42 = 966$ country-specific time trends, the random-effects probit selection model failed to converge, so we were not able to compute the selection bias correction term. However, the coefficient of COC enforcement in a fixed-effects OLS model remained similar without the selection bias correction term, with ($\beta_2 = 0.565$, $p < 0.05$) or without the country-time trends ($\beta_2 = 0.484$, $p < 0.01$). For brevity, we do not report the results of this regression.[37]

D. Heterogeneous Effects

We next ask the question: Was the failure in marginal deterrence consistent across countries? Could it have been driven by some countries that had less effective or less credible enforcement against cybercrimes? We conducted two tests to answer this question. First, we repeated estimating the main specification by excluding the 23 countries that had enforced the COC one-by-one. Figure 4 plots the coefficients of COC enforcement and their 95% confidence intervals. In the selection model, the COC enforcement effect mostly lied around -0.2, and the 95% confidence intervals almost always enclosed zero. By contrast, in the outcome model, the COC enforcement effect mostly lied around 0.5, and the 95% confidence interval always lied above zero. So, the increase in DDOS attack intensity

[37] We also plotted the least-squares predicted daily average number of packets per victim IP address captured by the country-specific time trends. The country-specific time trends had captured the variations in DDOS attack intensity over time in each of the COC countries well. For brevity, we omit the graphs here. In another robustness check, we added the interactions of continents (Asia, Europe, Africa, etc.) and the time trends. The results were similar.

with COC enforcement was not caused by a specific outlier.

Figure 4: Consistency of the COC Effect

Second, we estimated another model with a full parameterization of COC enforcement, allowing its coefficient to differ across countries. For brevity, we do not report the regression results. Instead, Table 10 tabulates the estimated effects of COC enforcement in each of the 23 countries in the outcome model.[38]

Table 10: Country-Specific Effect

The coefficients of COC enforcement were negative for seven countries, but only two of them were statistically significant. By contrast, the coefficients were positive for 16 countries, and 10 of them were statistically significant. Among these 10 countries, the coefficient of COC enforcement ranged from 0.687 to 2.266. Hence, the effect of COC enforcement on DDOS attack intensity did seem to vary across countries, but the overall effect tended to be positive.

VI. Was it Really Deterrence?

We found robust *positive* impact of COC enforcement on DDOS attack intensity (measured by packets per victim IP address). We interpret this finding as failure in marginal deterrence. To lend further confidence in our conclusion, we should show that perpetrators were indeed rational, that they cared about the expected benefit of a successful DDOS attack, and the expected cost of being apprehended and convicted.

Given the scale of our study it is difficult to draw direct evidence about perpetrator motivation. However, it has been increasingly recognized that cyber criminals are motivated by financial incentives – for example, Kaspersky recorded that in Q2 2011, the

[38] All country-specific COC enforcement coefficients were insignificant in the selection model.

majority of DDOS attacks were directed at online shopping and gaming Web sites, and also, banks and stock exchanges (Mansfield-Devine, 2011). Attacks against government sites comprised only 1% of all DDOS attacks.

We also traversed some posts in Hack Forums (see footnote 11) to explore hacker motivations. The following are some relevant posts:

- "*Has anyone here ever successfully extorted money from a business or organization by performing DDoS attacks...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,*" (posted by user "vladmir" in September 2010).

- "*this is the official european unions site right?? ...do they run like security agencies like the CIA and FBI...,*" (posted by user "mrjokerq8" in November 2011).

- "*avoid your own country* avoid good friends of your own country* avoid countries you may want to go live in* if you are living within the european union it is preferable not to hack into countries that are members of the union...,*" (posted by user "crackerjacks" in July 2011).

- "*fact is if youre using your net for extortion, cc fraud, industrial espionage or espionage for that matter you are more likely to have government agencys look into you...as to which are safer i would say html...what you do however need to do is daisy chain them. choosing ones which delete there logs every week or so. its best to have them in different countrys with different languages...,*" (posted by user "Facebook marketer" in October 2010).

- "*Difficult but not impossible, Also depends upon the intensity of your illegality,*" (posted by user "Transient" in May 2011).

- "*more packets and longer time will result in a more powerful ddos...,*" (posted by user "alchemist1221" in December 2010).

- "*Nah....a good price is 10 cents per bot. (OP: you probably want more bots to have a chance of DDOSing a decent)*," (posted by user "Unreality" in August 2010).

Evidently, some perpetrators would weigh the benefit of DDOS attack against the expected cost, particularly the cost of apprehension and legal sanction. The enforcement against cybercrimes may deter some novice perpetrators (as the first two posts above imply), but may not deter sophisticated or committed perpetrators who may then seek means to lower their risks (as the third and fourth posts show) while continuing, or even escalating, their attacks (as the last three posts imply).

VII. Implications

The results in Table 6 show that enforcing the COC increased the attack intensity by 51.1% (s.e. 6.5%). How significant was this impact at the national level? To answer this question, we regressed the number of victim IP addresses, packets generated, and hours of attack per Internet host on COC enforcement and reservation, and the demographic and control variables. As reported in Table 11, COC enforcement had decreased the number of victims by 26% (s.e. 4.3%) and hours of attack by 22% (s.e. 4.4%), but increased the packets generated by 71% (s.e. 9.0%). In general, the reservations tended to weaken the impact of the enforcement. This is consistent with their purpose.

Table 11: COC Enforcement: National Impacts

In the United States, there were roughly 2 million unique victim IP addresses and a total of 11.5 million hours of attack during the 177 days in our dataset. The estimates in Table 11 suggest that enforcing the COC could potentially have prevented hundreds of thousands of IP addresses from being attacked, or reduced millions of hours of attacking time in those 177 days.

A research commissioned by Verisign had found that among 19 companies with annual revenues exceeding one billion dollars, the loss in revenue due to DDOS attacks could range from 0.2 to 10 million dollars per hour (Forrester Consulting, 2009). A recent survey by HP Enterprise Security had also found that the annualized cost of DDOS attacks per incident was around \$172,238 (Ponemon Institute, 2012). It is reasonable to expect that most of the backscatter data observed in our dataset did not arise from successful DDOS attacks, and also, some of the attacked hosts may not be commercial, or could be of substantially smaller scales of operation. Even with these provisions, the potential saving realized from COC enforcement seems large.

However, COC enforcement was also correlated with DDOS attack packets. Because the probability of successful DDOS attacks increases with the number of packets launched for the attacks (Forrester Consulting, 2009), COC enforcement might have increased the chance for some systems to be incapacitated as well. This tends to offset the benefit of reduced number of victims and hours of attacks. On balance, the effect of enforcing the COC on the losses caused by DDOS attacks is ambiguous.[39]

To deter serious offenses, a well known suggestion has been to increase the marginal cost of committing serious offenses relative to minor offenses, so that utility-maximizing perpetrators would switch to less harmful offenses (Stigler, 1970). One way to facilitate this "marginal cost difference" is to raise the standard of proof for conviction (Ognedal, 2005), so that the marginal cost of committing minor offenses is decreased. Our results in Table 11 show, however, that this approach has a well-expected disadvantage – although it successfully discouraged serious offenses, it might have reduced the effectiveness of the enforcement. Overall, in the case of DDOS attack, raising such standard of proof through reservations on the COC had led to more victims and longer hours of attack at the national level. Hence, the evidence suggests that a better way to facilitate marginal deterrence for a new class of crimes would be to impose graduated penalties (Mookherjee

[39] Note that there could be substitutions in DDOS attacks across countries. After a country had enforced the COC, instead of not carrying out the attacks, perpetrators may switch to attacking targets in other countries. This may raise the observed DDOS attack rates and intensity in countries that had not enforced the COC, and so bias against our findings.

and Png, 1992, 1994; Wilde, 1992; Shavell, 1992), perhaps on every well-defined level of offenses, instead of reducing the sanction for minor offenses.

If we assume that DDOS attacks are mostly targeted at organizations, especially, large organizations,[40] then our results imply that enforcing the COC had re-distributed the risks among potential victims. The risks of large organizations, such as the government or multinational corporations, may become higher, whereas the risk of "smaller" parties, such as individuals or small and medium sized enterprises, may become smaller. Future enforcement of new laws, especially on the cyberspace, should carefully weigh the balance of interest between these different parties. One possible solution is to combine law enforcement such as the COC with precautions at the victim side. When attack is targeted, facilitating victim precaution would be effective especially for high-value victims, such as large organizations (Png and Wang, 2009). The intuition is that their elasticity with respect to the facilitation of the precaution will be higher, so they would more likely undertake additional efforts to protect their systems.[41]

Finally, similar to Vaillant and Wolff (2009), our findings also cast doubt on the broken windows theory – at least in the case of DDOS attack, criminalizing all offenses (including the minor ones) did not make perpetrators better behaved. There seems to be a need for more targeted deterrence against major offenses.

[40] Several reasons suggest that utility-maximing perpetrators would want to attack large organizations. First, if the attack is motivated by monetary gain, for example, cyber extortion, then such organizations are more likely to have the financial resources to pay the perpetrators (and they would be more likely to pay too since their opportunity cost of not paying is higher). Second, if the attack is motivated by pride, then incapacitating the site of a prominent organization, such as the government, would certainly give a higher sense of achievement to the perpetrator. Third, if the motivation is defiance, then attacking large organizations would create more visible impacts.

[41] Another advantage of victim precaution is that it may help alleviate the "weakest link" problem in interdependent systems (Varian, 2004), which may dissuade perpetrators from displacing cyber attacks to other countries, a trend identified in Kim et al. (2012).

VIII. Concluding Remarks

This paper presents the first attempt to demonstrate the challenge in achieving marginal deterrence using a large-scale dataset from the field. We find that enforcement of the Convention on Cybercrime had motivated undeterred perpetrators to launch more serious offenses. We also find that reservations weakened the effect of the COC, and so could lead to more effective marginal deterrence. However, such reservations also tended to increase the number of victims and total time of attack. We suggest that the best path to marginal deterrence is to impose graduated enforcement, setting different penalties for different extents of offenses. We do recognize, however, that this could be challenging in the cyberspace because new crimes emerge over time. Lacking effective means to impose marginal deterrence, another possible solution is to combine law enforcement such as the COC with precautions at the victim side.

Our dataset started from the second quarter of 2004 and ended in the last quarter of 2008. While this window may not capture the most recent developments of DDOS, it does carry the advantage of excluding some politically-motivated attacks, such as the cyber warfare between North Korea and South Korea and the United States in 2009, or between China and the United States, and Taiwan and Phillippines in 2013. Such warfare may be motivated by political ideology or patriotism, and so the economic cost/benefit tradeoff of DDOS attack and marginal deterrence may not apply.

Although our study was conducted in the setting of an international convention on cybercrime, and for only one particular offense, viz., DDOS, our results seem generalizable to other contexts where marginal deterrence matters.

The most pressing issue for future work is to explore the best means for marginal deterrence, given that imposing graduated penalty is not always feasible. Perhaps having a better understanding of the perceived sanction risk and the actual implementation of the enforcement would be helpful for policy design (Nagin, 1998). It would also be helpful to buttress our findings with the attack patterns of other cybercrimes (e.g., distribution of malware), and if we could identify perpetrators.[42] Finally, under the COC framework, it is worthwhile to investigate if facilitating victim precautions could help reduce the rate and intensity of cyber attacks in an empirical setting.

References

Ayres, Ian and John J. Donohue (2003) “Shooting down the more guns, less crime hypothesis,” *Stanford Law Review*, Vol. 55, No. 4, pp. 1193–1312.

Becker, Gary S. (1968) “Crime and punishment: An economic approach,” *Journal of Political Economy*, Vol. 76, No. 2, pp. 169–217.

Black, Dan A. and Daniel S. Nagin (1998) “Do right-to-carry laws deter violent crime,” *J. Legal Stud.*, Vol. 27, No. 1, pp. 209–219.

Bouffard, Leana Allen and Nicole Leeper Piquero (2010) “Defiance Theory and Life Course Explanations of Persistent Offending,” *Crime & Delinquency*, Vol. 56, No. 2, pp. 227–252, April.

Brenner, Susan W. (2006) “Cybercrime jurisdiction,” *Crime, Law and Social Change*, Vol. 46, No. 4-5, pp. 189–206, March.

Bronars, Stephen G. and John R. Lott (1998) “Criminal deterrence, geographic spillovers, and the right to carry concealed handguns,” *American Economic Review*, Vol. 88, No. 2, pp. 475–479.

CAIDA (2004-2005) *UCSD Backscatter 2004-2005 Dataset, May 2004 – November 2005.* http://www.caida.org/data/passive/backscatter_2004_2005_dataset.xml.

——— (2006) *UCSD Backscatter 2006 Dataset, February 2006 – November 2006.* http://www.caida.org/data/passive/backscatter_2006_dataset.xml.

——— (2007) *UCSD Backscatter 2007 Dataset, January 2007 – November 2007.* http://www.caida.org/data/passive/backscatter_2007_dataset.xml.

——— (2008a) *UCSD Backscatter 2008 Dataset, February 2008 – November 2008.* http://www.caida.org/data/passive/backscatter_2008_dataset.xml.

[42] We inferred perpetrator actions from victim-side data by exploiting the nature of the backscatter data, that there was a direct correspondence between backscatter and DDOS attack packets. Identifying perpetrators would give even more precise observations of crime rates and magnitude.

——— (2008b) *AS Relationships Dataset, January 2004 – December 2008.* http://www.caida.org/data/active/as-relationships/.

Calderoni, Francesco (2010) "The European legal framework on cybercrime: striving for an effective implementation," *Crime, Law and Social Change*, Vol. 54, No. 5, pp. 339–357, November.

Choi, Sang-Hun and John Markoff (2009) "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times*, July 8, 2009.

Donohue, John J. (2004) "Guns, crime, and the impact of state right-to-carry laws," *Fordham Law Review*, Vol. 73, No. 2, pp. 623–652.

Driscoll, John C. and Aart C. Kraay (1998) "Consistent covariance matrix estimation with spatially dependent panel data," *Review of economics and statistics*, Vol. 80, No. 4, pp. 549–560.

Ehrlich, Isaac (1973a) "The deterrent effect of capital punishment: A question of life and death," *The American Economic Review*, Vol. 65, No. 3, pp. 397–417.

——— (1973b) "Participation in Illegitimate Activities: A Theoretical and Empirical Investigation," *Journal of Political Economy*, Vol. 81, No. 3, pp. 521–565, January.

——— (1977) "Capital punishment and deterrence: Some further thoughts and additional evidence," *Journal of Political Economy*, Vol. 85, No. 4, pp. 741–788.

Ehrlich, Isaac and George D. Brower (1987) "On the issue of causality in the economic model of crime and law enforcement: Some theoretical considerations and experimental evidence," *The American Economic Review*, Vol. 77, No. 2, pp. 99–106.

Ekelund, R.B., J.D. Jackson, R.W. Ressler, and R.D. Tollison (2006) "Marginal deterrence and multiple murders," *Southern Economic Review*, Vol. 72, No. 3, pp. 521–541.

Forrester Consulting (2009) *DDoS: A Threat You Can't Afford To Ignore.*

Frees, Edward W. (1995) "Assessing cross-sectional correlation in panel data," *Journal of Econometrics*, Vol. 69, No. 2, pp. 393–414, October.

Friedman, Milton (1937) "The use of ranks to avoid the assumption of normality implicit in the analysis of variance," *Journal of the American Statistical Association*, Vol. 32, No. 200, pp. 675–701, December.

Ghose, Anindya and S.P. Han (2011) "An empirical analysis of user content generation and usage behavior on the mobile Internet," *Management Science*, Vol. 57, No. 9, pp. 1671–1691, June.

Goodin, Dan (2010) “Sex, lies, and botnets: the saga of Perverted Justice – Ex-vigilante vents DDoS fury over sham affair,” *The Register*, September 23, 2010.

Greene, William (2002) “The bias of the fixed effects estimator in nonlinear models,” *Unpublished manuscript*, pp. 1–31.

Heckman, James J. (1979) “Sample selection bias as a specification error,” *Econometrica*, Vol. 47, No. 1, pp. 153–161.

Katyal, NK (1997) “Deterrence’s Difficulty,” *Michigan Law Review*, Vol. 95, No. 8, pp. 2385–2476.

Katyal, Neal K. (2001) “Criminal law in cyberspace,” *University of Pennsylvania Law Review*, Vol. 149, No. 4, pp. 1003–1114.

Kaufmann, Daniel, A. Kraay, and M. Mastruzzi (2010) “The worldwide governance indicators: methodology and analytical issues,” *Unpublished report*.

Keyser, Mike (2003) “The Council of Europe Convention on Cybercrime,” *Journal of Transnational Law & Policy*, Vol. 12, No. 2, pp. 287–326.

Kim, Seung Hyun, Qiu-Hong Wang, and J.B. Ullrich (2012) “A comparative study of cyberattacks,” *Communications of the ACM*, Vol. 55, No. 3, p. 66, March.

Kirchgässner, Gebhard (2011) “Econometric estimates of deterrence of the death penalty: Facts or ideology?,” *Kyklos*, Vol. 64, No. 3, pp. 448–478.

Korgaonkar, Pradeep K. and Lori D. Wolin (1999) “A Multivariate Analysis of Web Usage,” *Journal of Advertising Research*, Vol. 39, No. 2, pp. 53–68.

Lee, D. and Thomas Lemieux (2010) “Regression discontinuity designs in economics,” *Journal of Economic Literature*, Vol. 48, No. 2, pp. 281–355.

Li, Xingan (2007) “International actions against cybercrime: Networking legal systems in the networked crime scene,” *Webology*, Vol. 4, No. 3.

Library of Congress (2009) *Cybercrime: An Annotated Bibliography of Select Foreign-Language Academic Literature*.

Lott, John R. and David B. Mustard (1997) “Crime, deterrence, and right-to-carry concealed handguns,” *The Journal of Legal Studies*, Vol. 26, No. 1, pp. 1–68.

Mansfield-Devine, Steve (2011) “DDoS: threats and mitigation,” *Network Security*, Vol. 2011, No. 12, pp. 5–12, December.

Mao, Z. Morley, Vyas Sekar, Oliver Spatscheck, Jacobus Van Der Merwe, and Rangarajan Vasudevan (2006) “Analyzing Large DDoS Attacks Using Multiple Data Sources,” *SIGCOMM’06 Workshops*, September.

Mookherjee, Dilip and I.P.L. Png (1992) “Monitoring vis-a-vis Investigation in Enforcement of Law,” *The American Economic Review*, Vol. 82, No. 3, pp. 556–565.

——— (1994) “Marginal deterrence in enforcement of law,” *Journal of Political Economy*, Vol. 102, No. 5, pp. 1039–1066.

Moore, D., G. Voelker, and S. Savage (2001) “Inferring Internet Denial of Service Activity,” *Proceedings of the 2001 USENIX Security Symposium*, August.

Nagin, Daniel S. (1998) “Criminal deterrence research at the outset of the twenty-first century,” *Crime and justice*, Vol. 23, No. 1998, pp. 1–42.

Ognedal, Tone (2005) “Should the Standard of Proof be Lowered to Reduce Crime?,” *International Review of Law and Economics*, Vol. 25, No. 1, pp. 45–61, March.

Pesaran, M.H. (2004) “General diagnostic tests for cross section dependence in panels,” *Cambridge Working Papers in Economics*.

Png, Ivan P. L., Chen-Yu Wang, and Qiu-Hong Wang (2008) “The Deterrent and Displacement Effects of Information Security Enforcement: International Evidence,” *Journal of Management Information Systems*, Vol. 25, No. 2, pp. 125–144, September.

Png, Ivan P. L. and Qiu-Hong Wang (2009) “Information Security: Facilitating User Precautions Vis-à-Vis Enforcement Against Attackers,” *Journal of Management Information Systems*, Vol. 26, No. 2, pp. 97–121, September.

Polinsky, A.M. and S. Shavell (2000) “The economic theory of public enforcement of law,” *Journal of Economic Literature*, Vol. 38, No. 1, pp. 45–76.

Ponemon Institute (2012) *2012 Cost of Cyber Crime Study: United States*.

Putsis, William P. and Barry L. Bayus (2001) “An empirical analysis of firms’ product line decisions,” *Journal of Marketing Research*, Vol. 38, No. 1, pp. 110–118.

Raphael, Steven and R. Winter-Ebmer (2001) “Identifying the Effect of Unemployment on Crime,” *Journal of Law and Economics*, Vol. 44, No. 1, pp. 259–283.

Shavell, S. (1992) “A note on marginal deterrence,” *International Review of Law and Economics*, Vol. 12, No. 3, pp. 345–355.

Shepherd, Joanna M. (2005) “Deterrence versus brutalization: Capital punishment’s differing impacts among states,” *Michigan Law Review*, Vol. 104, No. 2, pp. 203–256.

Sherman, Lawrence W. (1993) “Defiance, Deterrence, and Irrelevance: A Theory of the Criminal Sanction,” *Journal of Research in Crime and Delinquency*, Vol. 30, No. 4, pp. 445–473, November.

Stigler, George J. (1970) “The optimum enforcement of laws,” *Journal of Political Economy*, Vol. 78, No. 3, pp. 526–536.

Vaillant, Nicolas Gérard and François-Charles Wolff (2009) “Does punishment of minor sexual offences deter rapes? Longitudinal evidence from France,” *European Journal of Law and Economics*, Vol. 30, No. 1, pp. 59–71, November.

Vamosi, Robert (2008) “First conviction for Estonia’s ‘cyberwar’,” *CNET News*, January 24, 2008.

Varian, Hal (2004) “System reliability and free riding,” *Economics of information security*, pp. 1–15.

Wilde, Louis L. (1992) “Criminal Choice, Nonmonetary Sanctions, and Marginal Deterrence: A Normative Analysis,” *International Review of Law and Economics*, Vol. 12, No. 3, pp. 333–344, August.

Wooldridge, Jeffrey M. (2001) “Applications of Generalized Method of Moments Estimation,” *Journal of Economic Perspectives*, Vol. 15, No. 4, pp. 87–100, November.

——— (2006) *Introductory Econometrics: A Modern Approach*, Southwestern, Mason, OH: Thomson.

Yang, Bijou and David Lester (2008) “The deterrent effect of executions: A meta-analysis thirty years after Ehrlich,” *Journal of Criminal Justice*, Vol. 36, No. 5, pp. 453–460, September.

Zorz, Zeljka (2011) “Man convicted for using DDoS attacks in extortion scheme,” *Net Security*, June 15, 2011.

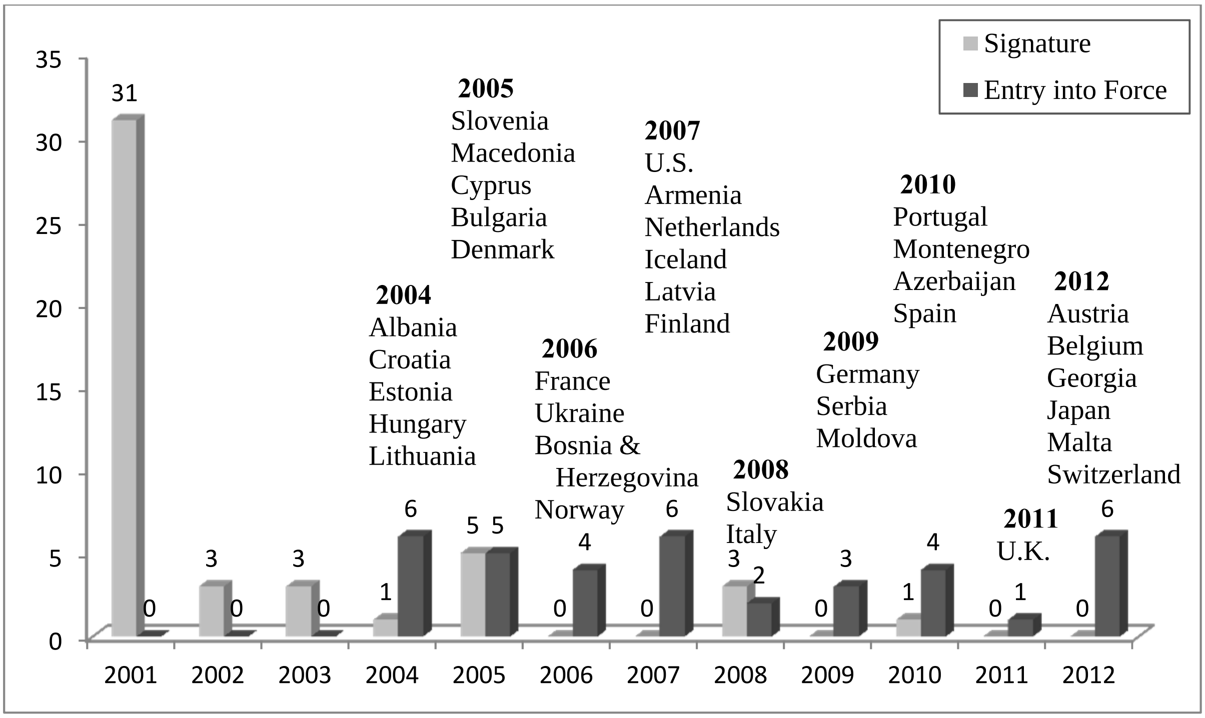
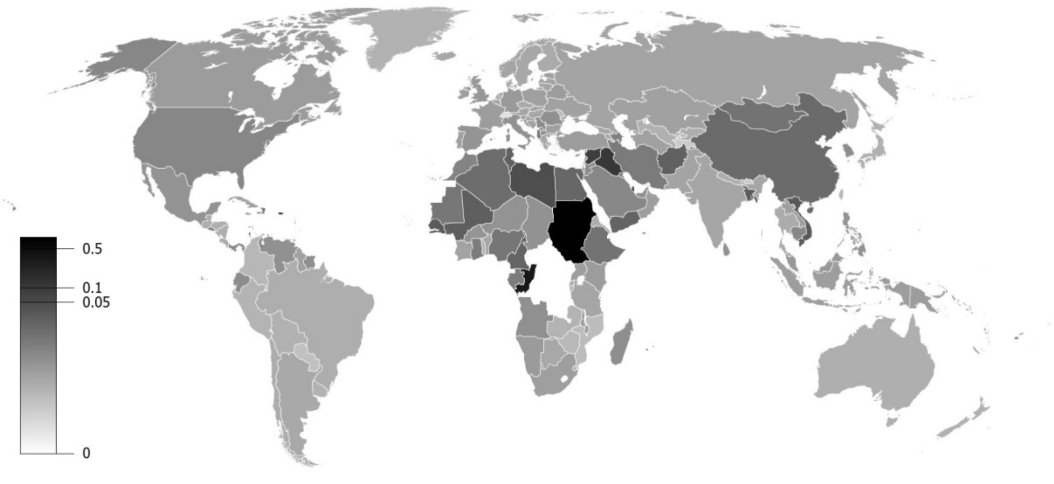


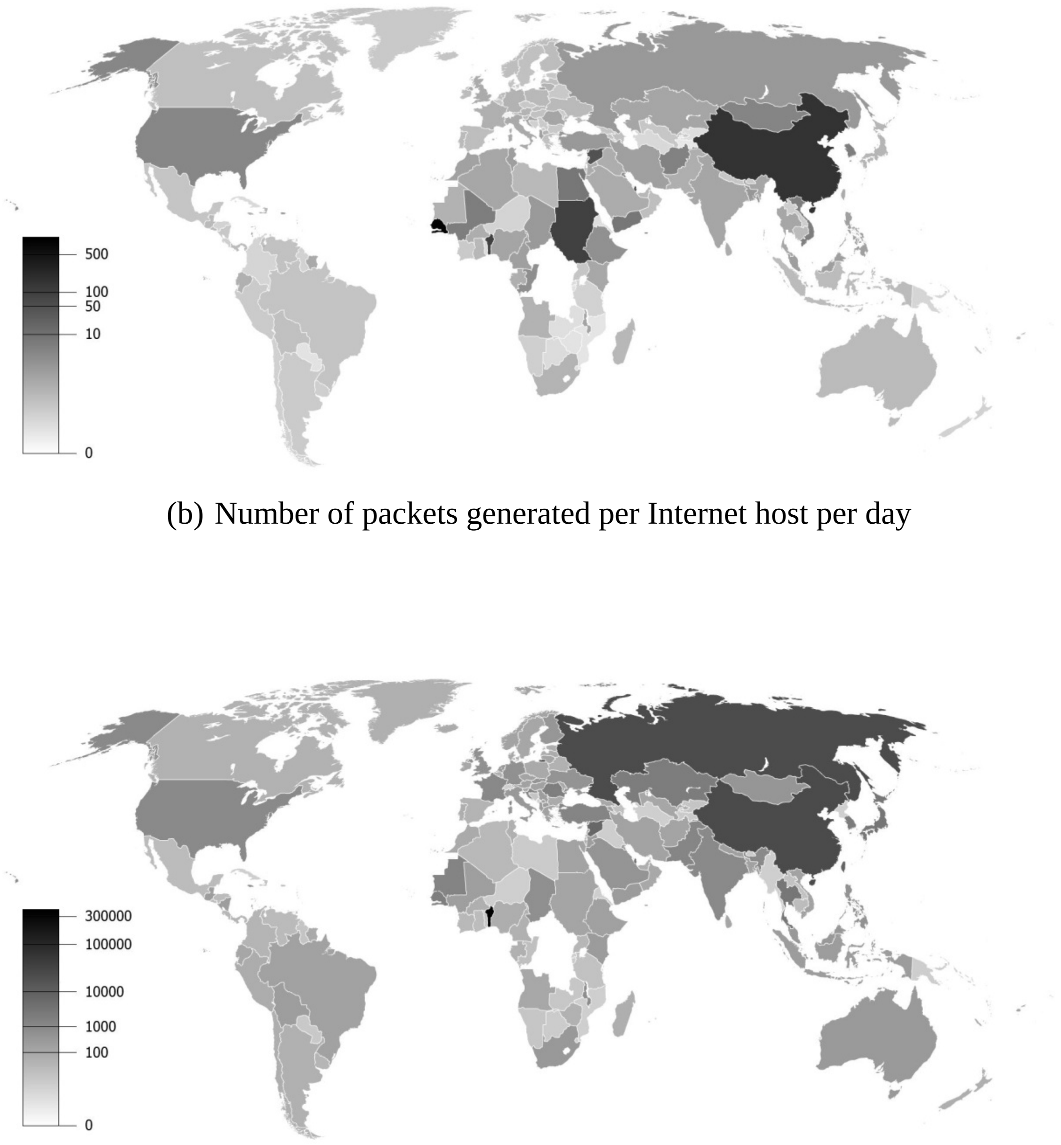
FIGURE 1 – SIGNATURE AND ENFORCEMENT OF THE CONVENTION ON CYBERCRIME



(a) Number of victim IP addresses per Internet host per day

FIGURE 2 – DISTRIBUTION OF DDOS ATTACKS

Note: Darker shade corresponds to more DDOS attacks. Internet host data are unavailable for North Korea, Montenegro, Myanmar, and Occupied Palestinian Territory.



(b) Number of packets generated per Internet host per day

(c) Number of packets generated per IP address per day

FIGURE 2 – DISTRIBUTION OF DDOS ATTACKS (CONTINUED)

Note: Darker shade corresponds to more DDOS attacks. Internet host data are unavailable for North Korea, Montenegro, Myanmar, and Occupied Palestinian Territory.

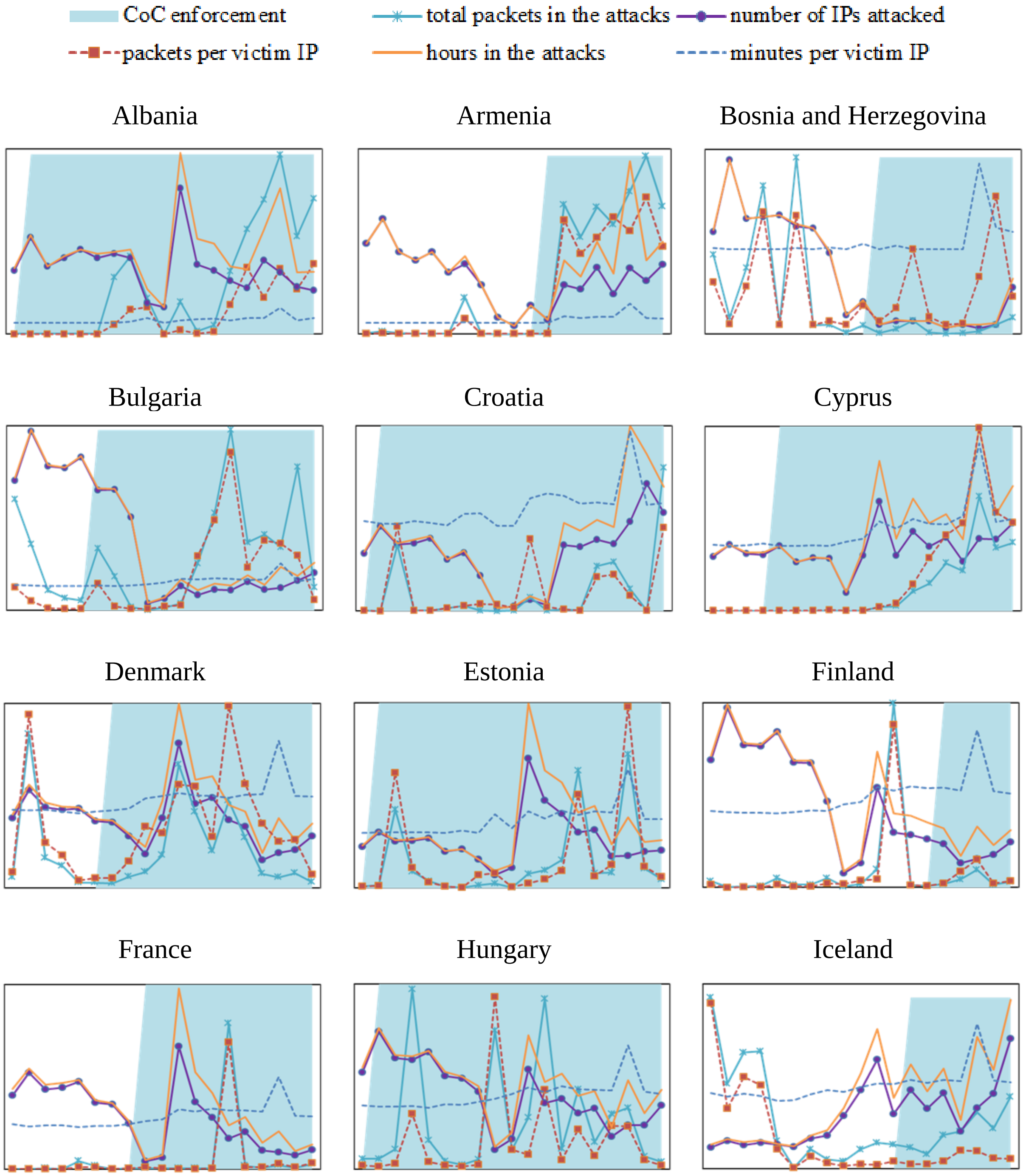


FIGURE 3 – DDOS ATTACKS OVER TIME

Note: The figures show the average DDOS attack per day in each quarter from the second quarter of 2004 to the last quarter of 2008. The trends are not plotted on the same scale and so should be examined separately. The shaded areas correspond to periods after the COC was enforced.

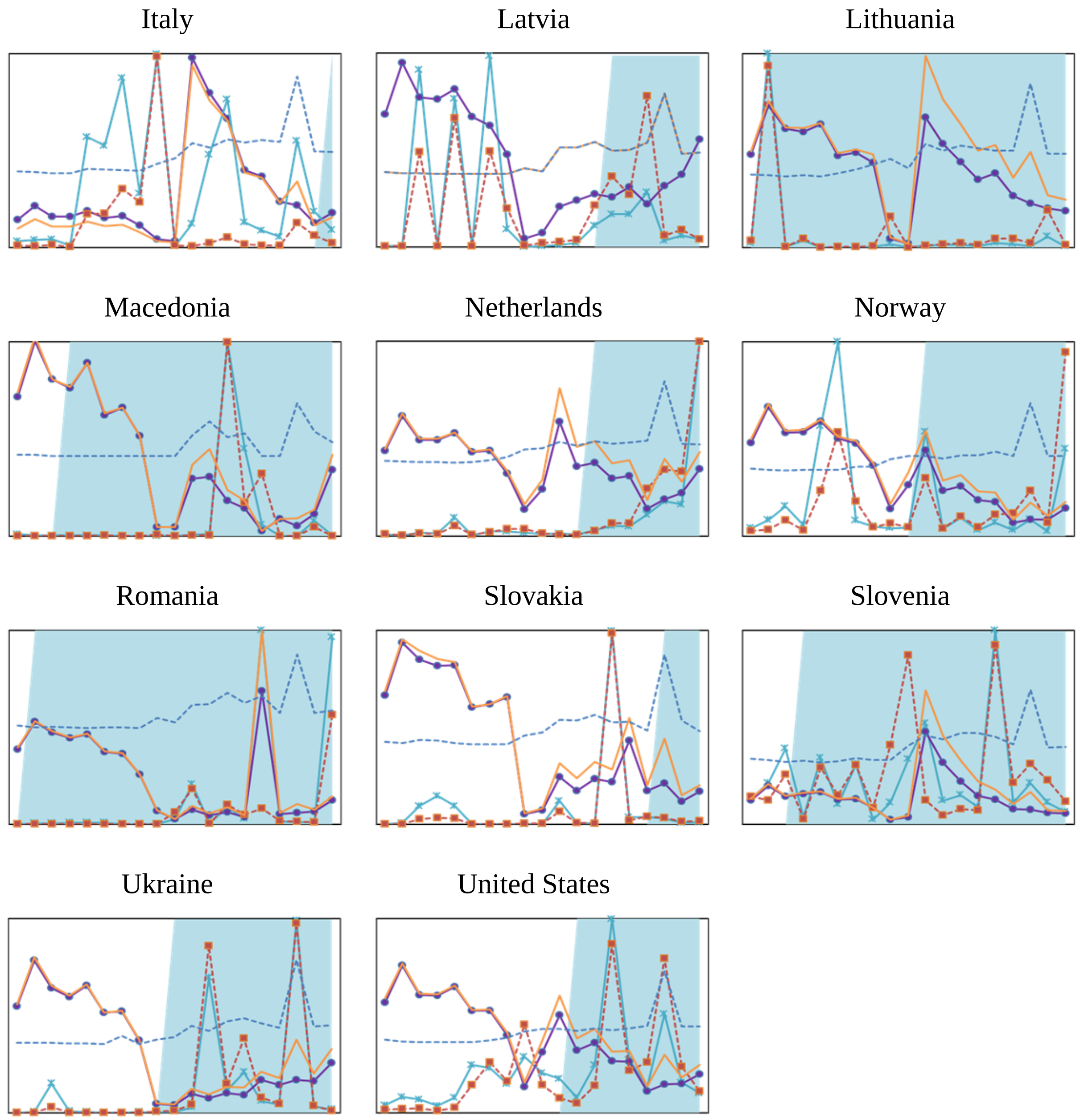
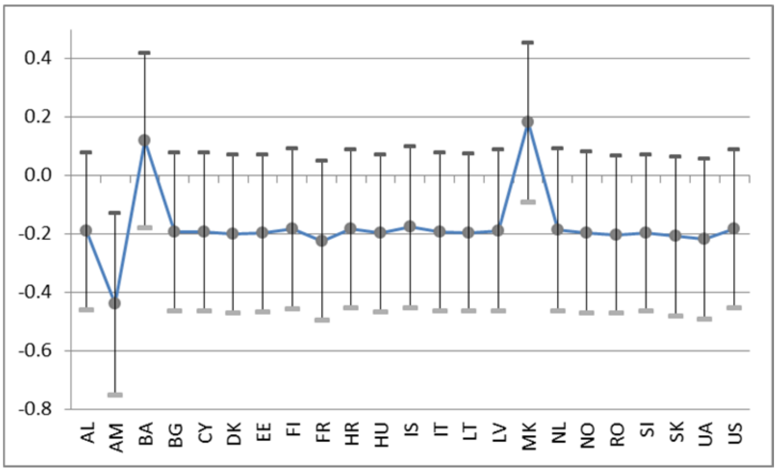
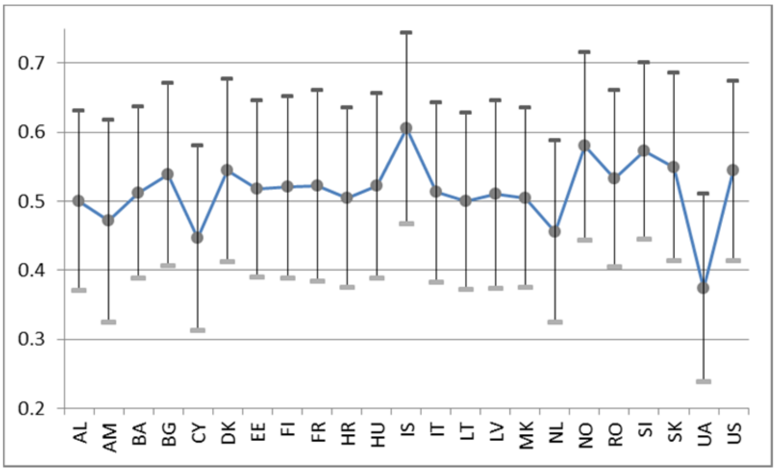


FIGURE 3 – DDOS ATTACKS OVER TIME (CONTINUED)

Note: The figures show the average DDOS attack per day in each quarter from the second quarter of 2004 to the last quarter of 2008. The trends are not plotted on the same scale and so should be examined separately. The shaded areas correspond to periods after the COC was enforced.



(a) Coefficients of COC Enforcement in the Selection Model



(b) Coefficients of COC Enforcement in the Outcome Model

FIGURE 4 – CONSISTENCY OF THE COC EFFECT

Note: The horizontal axis lists the specific countries excluded in each set of regression.
AL – Albania, AM – Armenia, BA – Bosnia and Herzegovina, BG – Bulgaria, CY – Cyprus, DK – Denmark, EE – Estonia, FI – Finland, FR – France, HR – Croatia, HU – Hungary, IS – Iceland, IT – Italy, LT – Lithuania, LV – Latvia, MK – Republic of Macedonia, NL – Netherlands, NO – Norway, RO – Romania, SI – Slovenia, SK – Slovakia, UA – Ukraine, US – The United States.

TABLE 1 – RESERVATIONS ON THE CONVENTION ON CYBERCRIME

Country	Article 3	Article 4	Article 6	Article 9	Article 10	Article 11	Article 14	Article 22	Article 29	Article 41
Austria*									√	
Azerbaijan*		√	√						√	
Belgium*								√		
Bulgaria							√			
Denmark				√			√			
Finland						√	√			
France				√				√		
Germany*	√		√						√	
Hungary				√						
Iceland				√						
Japan*			√	√		√		√	√	
Latvia									√	
Lithuania		√							√	
Montenegro*				√			√			
Norway			√				√		√	
Slovakia		√							√	
Switzerland*			√	√			√		√	
Ukraine			√	√						
U.K. *				√				√	√	
U.S.		√	√	√	√			√		√

* Ratified the Convention on Cybercrime after 2008, the end of sampling window in this study.

Note: Article 3 – Illegal interception; 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	Quarter	Period	Number of days
2004	2	5/26/2004 – 6/3/2004	9
	3	8/26/2004 – 9/3/2004	9
	4	11/24/2004 – 12/2/2004	9
2005	1	2/23/2005 – 3/3/2005	9
	2	5/25/2005 – 6/2/2005	9
	3	8/24/2005 – 9/1/2005	9
	4	11/23/2005 – 12/1/2005	9
2006	1	2/22/2006 – 3/2/2006	9
	2	5/24/2006 – 6/1/2006	9
	3	8/23/2006 – 8/31/2006	9
	4	11/22/2006 – 11/30/2006	9
2007	1	1/8/2007 – 1/11/2007 2/21/2007 – 3/1/2007	13
	2	5/23/2007 – 5/31/2007	9
	3	8/22/2007 – 8/30/2007	9
	4	11/20/2007 – 11/29/2007	10
2008	1	2/20/2008 – 2/28/2008 3/18/2008 – 3/19/2008	11
	2	5/21/2008 – 5/29/2008	9
	3	8/20/2008 –8/28/2008	9
	4	11/12/2008 – 11/19/2008	8
Total			177

TABLE 3 – DESCRIPTIVE STATISTICS

Variable	N	No. of countries	Unit	Mean	Std. dev.	Min	Max	Source	Form
Convention on Cybercrime (daily data)									
Signature	42,480	240	1 = signed; 0 = not signed	0.17	0.38	0	1	COE	
Enforcement	42,480	240	1 = enforce; 0 = not enforced	0.06	0.23	0	1	COE	
Reservation	42,480	240	Number of articles	0.06	0.40	0	6	COE	
DDOS Attack (daily data)									
Number of packets	42,480	240	×1,000	450.86	6,326.03	0	456,948.30	CAIDA	log
Hours of attack	42,480	240		388.39	3,374.49	0	94,071	CAIDA	log
Number of victim IP addresses	42,480	240		334.63	3,122.39	0	91,751	CAIDA	log
Packets per victim IP address	23,263	196	×1,000	1.41	92.60	1	13,974.54	Computed	log
Packets per victim IP address per hour	23,263	196	×1,000	0.46	31.36	1	4,658.18	Computed	log
Packets per hour	23,263	196	×1,000	0.95	47.27	1	6,987.27	Computed	log
Packets per Internet host	35,423	201		6.40	384.30	0	52,041.29	Computed	log
Hours of attack per Internet host	35,423	201		0.012	0.134	0	6	Computed	log
Number of victim IP addresses per Internet host	35,423	201		0.011	0.127	0	6	Computed	log
Country Demographics (annual data)									
Unemployment rate	24,960	147	% economically active people	8.57	6.55	0.20	77.00	GMID	
Higher education students	29,310	166	per 100 inhabitant	0.025	0.019	0	8.8	GMID	log
GDP in PPP	32,178	182	Thousand dollars per capita	12.54	14.27	0.25	84.25	GMID	log
Number of Internet users	35,010	198	per 1,000 inhabitant	242.15	245.00	0.24	911.32	GMID	log
Number of Internet hosts	31,638	230	per 1,000 inhabitant	63.66	240.81	0	5,302.74	CIA	log
% digital main lines	35,514	201	% of telephone main lines	94.61	15.10	0.70	100	GMID	

ISDN subscribers	25,222	146	per 1,000 inhabitant	15.90	37.44	0	239.44	GMID	log
Land area	36,099	204	sq. kilometer per 1,000 inhabitant	41.57	83.02	0.05	617.12	GMID	log
External AS connections	27,157		per 1,000 Internet hosts	0.025	0.11	0	1.67	CAIDA	
Quality of Governance (annual data)									
Control of corruption	36,150	206	Normalized index	0.01	1.00	-1.92	2.59	WGI	
Government effectiveness	36,150	206	Normalized index	0.01	1.00	-2.45	2.37	WGI	
Political stability and absence of violence/terrorism	36,717	208	Normalized index	0.01	1.00	-3.30	1.59	WGI	
Regulatory quality	36,150	206	Normalized index	0.00	1.00	-2.66	1.99	WGI	
Rule of law	36,743	208	Normalized index	0.01	1.00	-2.68	2.01	WGI	
Voice and accountability	36,603	207	Normalized index	0.01	1.00	-2.30	1.83	WGI	
Conventional Crime Statistics (annual data)									
Money laundering/financial crimes country/jurisdiction	42,480	240	1 = Yes; 0 = No	0.24	0.43	0	1	USDOS	
Judge	11,127	111	Per 100,000 inhabitant	15.45	19.46	0	195.70	UNODC	log
Theft	15,224	96	Per 100,000 inhabitant	864.46	951.40	1.90	4,926.40	UNODC	log
Total untried/pre-trial persons held	17,813	98	Per 100,000 inhabitant	69.48	107.13	1.30	725.10	UNODC	log
Prosecuted	10,802	79	Per 100,000 inhabitant	1,312.02	1,784.89	0.40	10,321.10	UNODC	log
Convicted	10,840	83	Per 100,000 inhabitant	798.81	1,117.63	6.10	7,390.70	UNODC	log

Data sources: COE = Council of Europe; CAIDA = Cooperative Association for Internet Data Analysis; GMID = Global Market Information Database; CIA = Central Intelligence Agency; WGI = Worldwide Governance Indicators; UNODC = United Nations Office on Drugs and Crime; USDOS = U.S. Department of State.

TABLE 4 – CORRELATIONS

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
1. Signature	1																										
2. Enforcement	0.49	1																									
3. Reservation	0.27	0.56	1																								
4. Number of packets	-0.04	0.00	0.13	1																							
5. Hours of attack	0.13	0.01	0.24	0.22	1																						
6. Number of victim IP addresses	0.13	0.00	0.20	0.20	0.99	1																					
7. Packets per victim IP address	-0.05	-0.02	-0.01	0.32	0.00	0.00	1																				
8. Packets per victim IP address per hour	-0.03	-0.01	-0.01	0.23	0.00	0.00	0.81	1																			
9. Packets per hour	-0.05	-0.02	-0.01	0.30	0.00	0.00	1.00	0.81	1																		
10. Packets per Internet host	-0.05	-0.02	-0.01	0.31	0.04	0.04	0.27	0.09	0.24	1																	
11. Hours of attack per Internet host	-0.12	-0.05	-0.03	0.04	0.00	0.00	0.00	0.00	0.00	0.18	1																
12. Number of victim IP addresses per Internet host	-0.12	-0.05	-0.03	0.05	0.00	0.00	0.00	0.00	0.00	0.17	0.98	1															
13. Unemployment rate	0.19	0.12	-0.10	-0.07	-0.07	-0.06	-0.03	-0.02	-0.03	-0.03	-0.03	-0.03	1														
14. Higher education students	0.29	0.22	0.26	-0.03	0.12	0.12	0.03	0.03	0.03	-0.05	-0.15	-0.15	-0.18	1													
15. GDP in PPP	0.30	0.02	0.17	-0.03	0.16	0.15	-0.01	0.00	-0.02	-0.01	0.08	0.09	-0.40	0.15	1												
16. Number of Internet users	0.49	0.17	0.25	-0.02	0.16	0.15	-0.02	-0.01	-0.02	-0.04	-0.10	-0.10	-0.32	0.43	0.76	1											
17. Number of Internet hosts	0.39	0.23	0.37	0.01	0.25	0.24	-0.02	-0.01	-0.02	-0.03	-0.09	-0.09	-0.27	0.35	0.53	0.72	1										
18. % digital main lines	-0.05	-0.10	-0.02	0.03	0.05	0.05	-0.07	-0.06	-0.07	0.02	0.02	0.01	-0.16	-0.13	0.27	0.28	0.18	1									
19. ISDN subscribers	0.53	0.17	0.10	-0.04	0.04	0.03	-0.03	-0.02	-0.03	-0.03	-0.07	-0.08	-0.12	0.10	0.52	0.53	0.38	0.17	1								
20. Land area	-0.06	-0.06	-0.01	-0.03	-0.01	-0.01	0.01	0.01	0.01	-0.01	0.00	0.00	-0.15	0.27	0.04	0.10	0.24	-0.02	-0.05	1							
21. External AS connections	-0.13	-0.06	-0.04	-0.02	-0.03	-0.03	-0.01	-0.01	-0.01	0.06	0.67	0.67	-0.03	0.20	0.05	-0.10	-0.10	0.00	-0.08	0.12	1						
22. Control of corruption	0.42	0.06	0.17	-0.05	0.14	0.13	-0.04	-0.03	-0.04	-0.04	-0.07	-0.07	-0.29	-0.13	0.78	0.86	0.67	0.36	0.52	0.13	-0.09	1					
23. Government effectiveness	0.45	0.08	0.19	-0.01	0.16	0.15	-0.03	-0.01	-0.03	-0.03	-0.11	-0.11	-0.27	0.32	0.74	0.87	0.63	0.37	0.51	0.07	-0.12	0.95	1				
24. Political stability & absence of violence/terrorism	0.48	0.17	0.16	-0.05	0.00	0.00	-0.04	-0.02	-0.04	-0.02	-0.03	-0.03	-0.29	0.34	0.67	0.71	0.47	0.18	0.45	0.18	-0.02	0.74	0.72	1			
25. Regulatory quality	0.51	0.15	0.19	-0.04	0.15	0.15	-0.04	-0.02	-0.04	-0.04	-0.11	-0.11	-0.22	0.34	0.71	0.83	0.58	0.33	0.48	0.04	-0.11	0.90	0.94	0.73	1		
26. Rule of law	0.47	0.08	0.20	-0.03	0.14	0.14	-0.04	-0.03	-0.04	-0.03	-0.07	-0.07	-0.28	0.33	0.76	0.86	0.63	0.38	0.53	0.10	-0.09	0.96	0.96	0.77	0.93	1	
27. Voice and accountability	0.63	0.22	0.20	-0.14	0.13	0.12	-0.08	-0.05	-0.07	-0.09	-0.17	-0.17	-0.11	0.35	0.48	0.72	0.56	0.31	0.54	0.11	-0.17	0.76	0.78	0.63	0.82	0.79	1

TABLE 5 – ESTIMATIONS USING DIFFERENT DEFINITIONS OF CRIME RATE

VARIABLES	(1) Random-effects probit	(2) OLS: Victim IP addresses	(3) OLS: Number of packets	(4) OLS: Packets per victim IP address
COC enforcement	-0.135	-0.639***	0.202*	0.344***
	(0.108)	(0.065)	(0.106)	(0.064)
Constant	-0.597***	-6.973***	-5.821***	2.285***
	(0.199)	(0.140)	(0.215)	(0.131)
Country-specific effects	Random	Fixed	Fixed	Fixed
Time trends	Inc.	Inc.	Inc.	Inc.
Observations	42,480	35,423	35,423	23,263
Within R-square		0.214	0.082	0.252
Number of countries	240	229	229	196

Notes: Random-effects probit model in column (1); fixed-effects OLS specification in columns (2)-(4). Column (1): Whether a country was attacked as dependent variable; Column (2): Log number of victim IP addresses per Internet host as dependent variable; Column (3): Log number of packets per Internet host as dependent variable; Column (4): Log number of packets per victim IP address as dependent variable. Because Internet host data were missing for some countries, and some countries were not attacked at all (so did not have any victim IP address) in the sample, we had to exclude these countries in the OLS regressions in columns (2)-(4). Spatial correlation consistent standard errors in parentheses except for column (1); *** p<0.01, ** p<0.05, * p<0.1.

TABLE 6 – MAIN ESTIMATION RESULTS

	(1)		(2)		(3)		(4)	(5)	(6)		(7)	
	Only COC enforcement		Only demographic and control variables		With COC enforcement and all control variables (preferred specification)		Packets per victim IP per hour	Packets per hour	Day fixed effects		Add COC reservations	
VARIABLES	Selection	Outcome	Selection	Outcome	Selection	Outcome	Outcome	Outcome	Selection	Outcome	Selection	Outcome
COC enforcement	-0.135	0.715***			-0.192	0.511***	0.519***	0.493***	-0.373*	0.427***	-0.240	0.705***
	(0.108)	(0.100)			(0.134)	(0.065)	(0.058)	(0.062)	(0.203)	(0.067)	(0.157)	(0.083)
COC reservation											0.058	-0.137***
											(0.099)	(0.033)
GDP in PPP			0.228	1.268***	0.241	1.226***	0.438	0.905**	0.557*	-0.246	0.236	1.153***
			(0.215)	(0.406)	(0.216)	(0.400)	(0.327)	(0.367)	(0.333)	(0.377)	(0.216)	(0.404)
Unemployment rate			0.046**	-0.016	0.046**	-0.011	-0.006	-0.004	0.109***	-0.001	0.046**	-0.007
			(0.018)	(0.016)	(0.018)	(0.015)	(0.014)	(0.015)	(0.027)	(0.015)	(0.018)	(0.015)
Higher education students			0.488***	3.599***	0.509***	3.515***	2.784***	3.405***	1.269***	3.501***	0.513***	3.470***
			(0.183)	(0.289)	(0.184)	(0.295)	(0.237)	(0.285)	(0.286)	(0.294)	(0.185)	(0.295)
Number of Internet users			-0.295***	0.240***	-0.314***	0.281***	0.197***	0.233***	-0.257*	0.126	-0.315***	0.294***
			(0.099)	(0.087)	(0.100)	(0.089)	(0.074)	(0.086)	(0.135)	(0.088)	(0.101)	(0.088)
% digital main lines			-0.004	0.013**	-0.004	0.009	0.005	0.011**	0.011	0.015***	-0.004	0.008
			(0.008)	(0.006)	(0.008)	(0.005)	(0.005)	(0.005)	(0.011)	(0.006)	(0.008)	(0.005)
ISDN subscribers			-0.018	0.769***	-0.011	0.838***	0.715***	0.835***	-0.150	0.889***	-0.007	0.809***
			(0.075)	(0.098)	(0.076)	(0.097)	(0.082)	(0.094)	(0.106)	(0.096)	(0.076)	(0.099)
Land area			0.053	-3.791***	0.056	-4.151***	-2.773***	-4.052***	0.003	-3.488***	0.054	-4.114***
			(0.098)	(0.812)	(0.099)	(0.814)	(0.731)	(0.787)	(0.160)	(0.811)	(0.099)	(0.814)
Control of corruption			-0.660***	-0.083	-0.697***	-0.114	-0.148	-0.106	-1.072***	-0.180	-0.693***	-0.183
			(0.211)	(0.182)	(0.213)	(0.182)	(0.160)	(0.180)	(0.293)	(0.182)	(0.213)	(0.183)
Government effectiveness			0.301	-0.320*	0.248	-0.149	0.082	-0.069	0.253	0.017	0.244	-0.144
			(0.213)	(0.168)	(0.217)	(0.166)	(0.152)	(0.162)	(0.278)	(0.167)	(0.217)	(0.168)
Political stability & absence of violence/terrorism			-0.604***	0.547***	-0.609***	0.518***	0.579***	0.551***	-1.070***	0.525***	-0.612***	0.582***
			(0.128)	(0.132)	(0.128)	(0.131)	(0.108)	(0.125)	(0.175)	(0.130)	(0.128)	(0.132)
Regulatory quality			-0.433*	-0.447***	-0.409*	-0.408**	-0.614***	-0.364**	-0.486	-0.490***	-0.404*	-0.448***
			(0.222)	(0.156)	(0.224)	(0.156)	(0.135)	(0.151)	(0.306)	(0.157)	(0.224)	(0.155)
Rule of law			1.390***	1.234***	1.449***	1.113***	0.930***	0.975***	2.191***	1.200***	1.442***	1.175***
			(0.283)	(0.248)	(0.288)	(0.250)	(0.203)	(0.244)	(0.392)	(0.253)	(0.288)	(0.251)
Voice accountability			0.278	-0.132	0.280	-0.151	-0.481***	-0.089	0.721***	0.031	0.275	-0.183

			(0.172)	(0.173)	(0.173)	(0.173)	(0.150)	(0.168)	(0.274)	(0.170)	(0.173)	(0.171)
Number of Internet hosts			-0.129**		-0.128**				0.047		-0.129**	
			(0.062)		(0.062)				(0.096)		(0.062)	
Number of Internet hosts squared			-0.011***		-0.011***				-0.003		-0.011***	
			(0.004)		(0.004)				(0.005)		(0.004)	
Selection bias correction term		-4.272***		-0.061*		-0.065*	-0.015	-0.069**		-0.011		-0.064*
		(0.803)		(0.034)		(0.035)	(0.030)	(0.033)		(0.011)		(0.035)
Constant	-0.597***	3.327***	0.685	51.603***	0.706	55.485***	40.828***	54.451***	3.905	53.200***	0.738	55.114***
	(0.199)	(0.259)	(1.748)	(8.203)	(1.756)	(8.266)	(7.357)	(7.986)	(2.686)	(8.238)	(1.757)	(8.277)
Country specific effects	Random	Fixed	Random	Fixed	Random	Fixed	Fixed	Fixed	Random	Fixed	Random	Fixed
Time trends	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	--	--	Inc.	Inc.
Day fixed effects	--	--	--	--	--	--	--	--	Inc.	Inc.	--	--
Within R-square		0.256		0.284		0.286	0.234	0.244		0.308		0.286
Observations	42,480	23,263	16,429	13,827	16,429	13,827	13,827	13,827	16,429	13,827	16,429	13,827
Number of countries	240	196	106	104	106	104	104	104	106	104	106	104

Notes: Selection model uses random-effects probit specification with an indicator denoting whether a country was attacked as dependent variable; outcome model uses fixed-effects OLS specification with log number of packets per victim IP address as dependent variable, except otherwise stated. Column (1): Only COC enforcement as regressor; Column (2): Only demographic and control variables as regressors; Column (3): All variables, including COC enforcement, as regressors – the preferred specification; Column (4): Use log packet per victim IP address per hour as dependent variable in the outcome model; Column (5): Use log packet per hour as dependent variable in the outcome model; Column (6): Day fixed effects instead of time trends; Column (7): Include COC reservation interacted with COC enforcement as independent variable. Spatial correlation consistent standard errors in parentheses in all outcome models; *** p<0.01, ** p<0.05, * p<0.1.

TABLE 7 – IDENTIFICATION TESTS

	(1)		(2)	
	Add number of professional judges or magistrates		Add external AS connections	
VARIABLES	Selection	Outcome	Selection	Outcome
COC enforcement	1.077	2.419***	-0.264	-0.041
	(0.674)	(0.495)	(0.282)	(0.148)
Judge	0.015	0.076		
	(0.149)	(0.174)		
COC enforcement × Judge	-0.342	-0.778***		
	(0.256)	(0.171)		
External AS connections			0.139***	0.129***
			(0.048)	(0.039)
COC enforcement × External AS connections			0.020	0.110***
			(0.066)	(0.028)
Selection bias correction term		-0.030***		0.007
		(0.009)		(0.035)
Constant	0.981	69.260***	0.672	55.908***
	(2.332)	(22.133)	(1.559)	(8.836)
Country specific effects	Random	Fixed	Random	Fixed
Time trends	Inc.	Inc.	Inc.	Inc.
Within R-square		0.280		0.292
Observations	9,005	7,674	15,379	13,380
Number of countries	66	65	100	100

Notes: Selection model uses random-effects probit specification with an indicator denoting whether a country was attacked as dependent variable; outcome model uses fixed-effects OLS specification with log number of packets per victim IP address as dependent variable. All specifications include the demographic and control variables, and the governance quality indicators reported in Table 6 as independent variables. Column (1): Add number of professional judges or magistrates and its interaction with COC enforcement as independent variables; Column (2): Add external AS connections and its interaction with COC enforcement as independent variables. Spatial correlation consistent standard errors in parentheses in all outcome models; *** p<0.01, ** p<0.05, * p<0.1.

TABLE 8 – FALSIFICATION TESTS

	(1)	(2)				(3)	
	Money Laundering (Y/N)	Theft	Prosecution	Conviction	Untried/pretrial held	COC signature	
VARIABLES						Selection	Outcome
COC enforcement	-0.422	-0.019	-0.029	0.002	0.034		
	(1.142)	(0.053)	(0.050)	(0.029)	(0.092)		
COC signature						0.155	-0.041
						(0.257)	(0.186)
Selection bias correction term							-0.060*
							(0.034)
Constant	54.046***	5.473	66.965*	34.548***	-8.646	0.541	51.645***
	(16.767)	(4.694)	(36.630)	(12.495)	(6.974)	(1.753)	(8.196)
Country specific effects	Random	Fixed	Fixed	Fixed	Fixed	Random	Fixed
Time trends	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.
Within R-square		0.125	0.145	0.210	0.148		0.284
Observations	16,429	12,122	9,009	9,046	10,079	16,429	13,827
Number of countries	106	83	61	66	74	106	104

Notes: Random-effects probit specification in column (1); fixed-effects OLS specification in column (2); for column (3), the selection model uses random-effects probit specification with an indicator denoting whether a country was attacked as dependent variable; the outcome model uses fixed-effects OLS specification with log number of packets per victim IP address as dependent variable. All specifications include the demographic and control variables, and the governance quality indicators reported in Table 6, as independent variables. Column (1): An indicator denoting whether a country was listed as a money laundering/financial crime country/jurisdiction by USDOS as dependent variable; Column (2): Log per-capita crime statistics as dependent variables; Column (3): Use COC signature in place of COC enforcement. Robust standard errors clustered by country in parentheses in column (2); spatial correlation consistent standard errors in parentheses in the outcome model in column (3); *** p<0.01, ** p<0.05, * p<0.1.

TABLE 9 – ROBUSTNESS

	(1)		(2)		(3)		(4)		(6)		(7)	
	Only countries that enforced COC		Only countries in Council of Europe		6-month lag		12-month lag		Only countries attacked for at least 1 day		Exclude countries attacked every day	
VARIABLES	Selection	Outcome	Selection	Outcome	Selection	Outcome	Selection	Outcome	Selection	Outcome	Selection	Outcome
COC enforcement	-0.039	0.466***	-0.052	0.550***					-0.168	0.511***	-0.294*	1.076***
	(0.162)	(0.067)	(0.288)	(0.073)					(0.131)	(0.064)	(0.172)	(0.114)
COC enforcement lagged by 6 months					-0.118	0.551***						
					(0.129)	(0.062)						
COC enforcement lagged by 12 months							-0.028	0.561***				
							(0.128)	(0.064)				
Selection bias correction term		-0.026		0.012*		-0.056		-0.062*		-0.067**		-0.097***
		(0.034)		(0.006)		(0.035)		(0.035)		(0.033)		(0.035)
Constant	-0.381	-253.169***	4.147	-114.054***	0.711	57.271***	0.691	57.043***	1.296	55.274***	-1.196	75.869***
	(4.496)	(32.845)	(11.102)	(24.343)	(1.750)	(8.289)	(1.747)	(8.294)	(1.543)	(8.275)	(2.612)	(9.412)
Country specific effects	Random	Fixed	Random	Fixed	Random	Fixed	Random	Fixed	Random	Fixed	Random	Fixed
Time trends	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.	Inc.
Within R-square		0.3212		0.2969		0.2866		0.2868		0.2859		0.3363
Observations	5,679	5,125	6,945	5,871	16,429	13,827	16,429	13,827	15,952	13,826	9,004	6,576
Number of countries	34	34	41	40	106	104	106	104	103	103	61	59

Notes: Selection model uses random-effects probit specification with an indicator denoting whether a country was attacked as dependent variable; outcome model uses fixed-effects OLS specification with log number of packets per victim IP address as dependent variable. All specifications include the demographic and control variables, and the governance quality indicators reported in Table 6, as independent variables. Column (1): Include only countries that had enforced the COC; Column (2): Include only Council of Europe countries; Column (3): COC enforcement lagged by 6 months; Column (4): COC enforcement lagged by 12 months; Column (5): Exclude Cape Verde, Dominical Republic, and Saint Lucia which were not attacked in any day in the sample; Column (6): Exclude Australia, Austria, Belgium, Canada, Chile, China, Czech Republic, Denmark, Ecuador, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Israel, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Norway, Philippines, Poland, Portugal, Romania, Russian Federation, Singapore, Slovenia, South Korea, South Africa, Spain, Sweden, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, and the United States which were attacked in every day in the sample. Spatial correlation consistent standard errors in parentheses in all outcome models; *** p<0.01, ** p<0.05, * p<0.1.

TABLE 10 – COUNTRY-SPECIFIC EFFECTS

Country	Net effect of COC enforcement	Wald Statistic	
Iceland (control)	-1.185	F(1, 103) = 30.42	Prob > F = 0.000
Albania	0.902	F(1, 103) = 12.37	Prob > F = 0.001
Armenia	1.666	F(1, 103) = 30.60	Prob > F = 0.000
Bosnia and Herzegovina	-1.027	F(1, 103) = 5.90	Prob > F = 0.000
Bulgaria	0.011	F(1, 103) = 0.00	Prob > F = 0.972
Cyprus	2.095	F(1, 103) = 133.51	Prob > F = 0.000
Denmark	-0.089	F(1, 103) = 0.17	Prob > F = 0.679
Estonia	0.732	F(1, 103) = 4.30	Prob > F = 0.041
Finland	0.687	F(1, 103) = 8.55	Prob > F = 0.004
France	0.456	F(1, 103) = 3.84	Prob > F = 0.053
Croatia	1.080	F(1, 103) = 4.16	Prob > F = 0.044
Hungary	0.351	F(1, 103) = 1.02	Prob > F = 0.314
Italy	-1.251	F(1, 103) = 2.65	Prob > F = 0.107
Lithuania	0.238	F(1, 103) = 0.13	Prob > F = 0.717
Latvia	0.704	F(1, 103) = 9.11	Prob > F = 0.003
Republic of Macedonia	0.474	F(1, 103) = 3.61	Prob > F = 0.060
Netherlands	1.336	F(1, 103) = 35.66	Prob > F = 0.000
Norway	-0.174	F(1, 103) = 0.77	Prob > F = 0.383
Romania	1.044	F(1, 103) = 12.60	Prob > F = 0.001
Slovenia	-0.735	F(1, 103) = 3.20	Prob > F = 0.077
Slovakia	-1.283	F(1, 103) = 2.50	Prob > F = 0.117
Ukraine	2.266	F(1, 103) = 80.54	Prob > F = 0.000
The United States	0.205	F(1, 103) = 0.91	Prob > F = 0.342

Note: We first estimated the fixed-effects OLS outcome model with the selection bias correction term by including interactions of each country with the COC enforcement variable, treating Iceland as the control. The coefficient of Iceland (–1.185) was then added to each interaction variable involving another country to compute the net effect of COC enforcement for that other country.

TABLE 11 – COC ENFORCEMENT: NATIONAL IMPACTS

VARIABLES	(1) Victim IP addresses	(2) Packets	(3) Hours of attack
COC enforcement	-0.258***	0.714***	-0.224***
	(0.043)	(0.090)	(0.044)
COC reservation	0.249***	-0.213***	0.246***
	(0.037)	(0.065)	(0.037)
Constant	42.276***	21.862**	40.133***
	(3.534)	(10.177)	(3.649)
Country specific effects	Fixed	Fixed	Fixed
Time trends	Inc.	Inc.	Inc.
Within R-square	0.3905	0.2363	0.3516
Observations	16,429	16,429	16,429
Number of countries	106	106	106

Notes: Fixed-effects OLS specification in all columns. All specifications include the demographic and control variables, and the governance quality indicators reported in Table 6, as independent variables. Column (1): Log number of victim IP address per Internet host as dependent variable; Column (2): Log number of packets per Internet host as dependent variable; Column (3): Log hours of attack per Internet host as dependent variable. Spatial correlation consistent standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1.