Research Journal of Applied Sciences, Engineering and Technology 7(15): 3056-3063, 2014
DOI:10.19026/rjaset.7.642
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: July 30, 2013 Accepted: August 16, 2013 Published: April 19, 2014

Research Article

The Role of International Law and Economics Procedures to Overcome the Specified Crimes and Terrorism in Cyberspace

Nazanin Miralaei and Ebrahim Erfani
No 83, Mahyar Ave, Africa St, Tehran, Iran

Abstract: Internet and cyberspace as many other shapes of technology has its own pros and cons. In addition to many advantages of internet, there are many crimes in different types which have unfavorable effects on people who use this pervasive kind of information technology. To deal with this situation we have employed international law according to economics procedures. In fact, the main goal of this study is about the survey of the role of international law according to economics approaches to conquer cyber-terrorism. Economic analysis of law suggests that customary international law is a more flexible, efficient and effective method for the development of international law capable of responding to cybercrime. Unlike treaty law, customary international law is based upon state cooperation without the requirement of formal written agreements. It is a dynamic process that minimizes the problems raised by transactional costs by allowing states to forego explicit negotiations and to function even in the absence of a formal structure. This study explains how these economic tools can assist states in developing dynamic and flexible customary international law that is sufficiently responsive to the scourge of cybercrime. Customary law presents the most efficient and effective means for the international community to address cybercrime. By borrowing principles from economics to align states' interests for purposes of forming cybercrime rules, states may achieve optimal customary international law that maximizes the welfare of the entire international community.

Keywords: Customary law, cybercrime, cyber-terrorism, economics procedures, international law

INTRODUCTION

Into the second decade of Internet life-a duration dependent to a millennium in the offline world-the international community continues to struggle with the issue of cybercrime.

The criminal potential and the magnitude of cybercrimes parallel the growth of the Internet. To take just one example, over an eleven year period ending in 1999, the number of recorded computer security incidents grew by more than 133,000% (Economist, 2004).

A new strain of cybercrime is also making its debut. With cyber-terrorism, terrorists are asking, why hi-jack an airplane using a bomb and relying on unpredictable variables, when we can sky-jack the entire airline industry from behind the comfort, safety and predictability of our portable and unidentifiable computers. Countless other digital doom scenarios exist in which unseen cyber terrorists could wreak havoc at the stroke of a key or click of a mouse (Nagy, 2007). As this digital dilemma has no national boundaries, it is clearly international in scope. The question is whether the international community has a sufficient response to repel the growing threat of cybercrime, including cyber terrorism.

Creating a multilateral treaty to address cybercrime represents one possible solution. Indeed, on November 23, 2001, in Budapest, Hungary, the Council of Europe opened for signature the Convention on Cybercrime. The Convention goes far to define international crimes, to provide for domestic criminal procedural law powers and to further international cooperation involving cybercrimes (Nerep, 2001). However, inherent problems with treaty law suggest that it is not the only and perhaps not the best, tool for solving problems in the dynamic world of cyberspace. To wit, formation of treaty law usually requires an extensive and cumbersome process of negotiation that may eventually yield formal codification (Weitbrecht, 2008). By the time that states have actually "fixed" a solution to a problem, the realities giving rise to the original problem may have changed greatly (especially given the nature of cyberspace), or the answer may be the result of too much compromise. Economic analysis of law suggests that customary international law is a more flexible, efficient and effective method for the development of international law capable of responding to cybercrime. This study focuses on customary international law, rather than treaty law.

Unlike treaty law, customary international law is based upon state cooperation without the requirement of formal written agreements (Nerep, 2001). It is, in and

Corresponding Author: Nazanin Miralaei, No 83, Mahyar Ave, Africa St, Tehran, Iran

of itself, a dynamic process that "minimizes the problems raised by transaction costs by allowing states to forego explicit negotiations and to function even in the absence of a formal structure." Perhaps most importantly, customary international law is flexible and may be used by states to respond to new, dynamic problems, such as those that arise in the context of computers and the Internet. The development of efficient customary international law, without more, is also challenged by real world circumstances. For example, states often have divergent interests in solving international problems such as cybercrime (Weitbrecht, 2008). While capturing cybercriminals that threaten economic stability may be worthwhile, fighting cybercrime can be expensive and easing rules relating to territorial sovereignty-a keystone of statehood-is a rather imposing notion.

Nevertheless, economics offers customary international law several tools that may be used to align the interests of states. These economic devices, namely, role reversibility, reciprocity constraints and articulation, create structures in which states' incentives become symmetrical (Stothers, 2001). Under symmetric incentive structures, states continue to pursue their individual economic interests, but they arrive at optimal solutions that promote the good of the entire international community. Furthermore, customary international law continues to emerge in spontaneous fashion from the decentralized practice of states. This study explains how these economic tools can assist states in developing dynamic and flexible customary international law that is sufficiently responsive to the scourge of cybercrime.

However, the objectives of this study are as follow:

- The role of international law as an efficient tool for dealing crimes and terrorism in cyberspace
- The role of economics approaches based on principles of international law to combat that specified cyber crimes
- Theoretical and practical application of international law and economics procedures to deal with crimes in cyberspace

LITERATURE REVIEW

Cybercrime:

The internet and cyberspace: Before discussing crimes that occur on the Internet and international law's ability to respond to such threats a brief introduction to the nature of that forum is in order (Glader, 2004). The United States Supreme Court has explained, "The Internet is an international network of interconnected computers... (that) enables millions of people to communicate with one another and to access vast amounts of information from around the world." It was originally designed by the U.S. Government to permit the military, defense contractors and university researchers to have uninterrupted communication with one another notwithstanding any potential damages as a result of nuclear war (Frazer, 1992). By the early 1990s, this computerized network was opened up to the general public. Today, the Internet exists as an international forum in which individuals and organizations representing broad interests come together to share a variety of ideas and information (Stothers, 2001).

From an international perspective, the Internet renders borders largely irrelevant. This medium is often referred to as "cyberspace" because it has no physical location of its own and it is available to any person who has access to the Internet, regardless of their citizenship, or national borders. In the words of one commentator, "More than any other technology, the Internet facilitates cheap, fast and difficult-to-detect multi-jurisdictional transactions." Thus, even though the Internet is often praised for its ability to "inform, educate, entertain and conduct business on a world-wide scale," it is also recognized as the vehicle for a great deal of potential harm. Because the threats are not bounded in the traditional sense, the interests of the entire international community are at stake-therefore, any solutions must be international in scope.

From an economic viewpoint, the Internet is efficient in that it allows its users to accomplish diverse tasks at virtually no cost. Internet users have the ability to communicate and retrieve information worldwide using a variety of means such as electronic mail, list serves, chat rooms and the Web. With respect to crime, the "Internet fosters certain efficiencies that may make detection and subsequent prosecution considerably more difficult." Moreover, computers have the ability to increase the expected return from criminal conduct and to decrease the fixed costs. Primarily because the cost of using the Internet-i.e., the cost of entry-is so low and its reach so broad, the Internet is a unique medium with unparalleled efficiency.

A vehicle for cybercrime: Merely describing the nature of the Internet demonstrates its potential to be used for illicit purposes. Speaking of the Internet five years ago, the U.S. Supreme Court observed that "at any given time 'tens of thousands of users are engaging in conversations on a huge range of subjects... (making it) no exaggeration to conclude that the content on the Internet is as diverse as human thought.'" Since human thought has long contemplated many means of criminal activity, crime occurring in the Internet forum comes as little surprise[1].

With the growth of the Internet, however, came opportunities to commit more advanced and devastating computer crimes. The media has made most people aware of the potential for these types of crimes to wreak havoc within the Internet community. Two recent

examples from 2000 are particularly illustrative (Glader, 2004). First, was the debilitating attack on the eight largest of the U.S.-based Internet companies. In February of 2000, a hacker unleashed several computer programs that made thousands of simultaneous requests each minute to connect to the computer systems of the Internet companies. Shutting down these companies for days, the attack was estimated to have caused over $1.2 billion in damages.

Even more damaging was a virus reaching the entire Internet community and infecting over 45 million computers. The "I Love You" virus, originating from hackers located in the Philippines and affecting people throughout the world, was programmed to self-install on a computer's system files. When a computer user generated an email, the virus caused the computer to forward an e-mail attachment to all of the addresses in the user's e-mail address book, thereby infecting all those who opened the attachment Wood (Wood, 1981). The aggregate economic damage of this crime was estimated to cost from $10 billion to over $11 billion.

The above mentioned crimes are considered "cybercrimes," which, if defined loosely, mean computer crimes committed over the Internet in cyberspace. Most commentators recognize three types of cybercrime. First, is where the computer itself is the target of the crime, such as when a hacker infects a specific computer or network with a virus (e.g., the attack on the Internet companies' systems) (Nagy, 2007). Second, a computer may be used as the instrument of a crime. For example, someone may use a computer to defraud consumers, to steal information from a competitor, or to embezzle money from an employer (e.g., the "I Love You" bug which used other computers to spread a virus). Finally, a computer may be incidental to a crime or store evidence of a crime (Nerep, 2001). For instance, a bank robber may use a computer to store records pertaining to past robberies or plans for future robberies.

The definitive cybercrime-cyber-terrorism: In addition to the above-mentioned types of cybercrime, the idea of "cyber-terrorism" is gaining recognition. As a preliminary matter, the international community has had trouble enough attempting to define "terrorism," let alone its offspring, "cyber-terrorism." For instance, the United States, the United Kingdom and the United Nations all define terrorism in slightly different terms. One commentator has come up with the following working definition: "the calculated employment or the threat of violence by individuals, sub-national groups and state actors to attain political, social and economic objectives in violation of law, intended to create an overwhelming fear in a target area larger than the victims attacked or threatened."

Aside from the teenage hacker who may disrupt a company's website, the possibility that "cyber-terrorists" will use computers to commit crimes that result in death or mass destruction is real. Discussing the threat of cyber-terrorism, a U.S. ex-Terrorism Czar said, "I'm talking about people shutting down a city's electricity, ... 911 systems, ... telephone networks and transportation systems. You black out a city, people die. Black out lots of cities, lots of people die. It's as bad as being attacked by bombs...." Echoing the same sentiment, one commentator noted that "bombing the right junction station might shut down an air traffic control net work or phone-communications for a large city, but inserting a computer virus which shuts down or overloads the system could accomplish the same ends."

Like the Internet, terrorism-whether cyber or not-is also a low-cost and efficient tool that knows no national boundaries. In addition, cyber-terrorism consists of low-intensity conflict and is especially effective for its ability to project psychological intimidation in its targets. Consider this: "a well-coordinated attack with about thirty computer experts strategically placed around the globe and with a budget of approximately 10 million dollars, could bring the United States, the only superpower, to its knees." Such realities give nations, big or small, substantial cause for worry. Without an adequate, efficient and international response to the threat of cybercrime, including cyber-terrorism, such worries will not ease anytime soon.

Effectively combating cybercrime-say national scholars, national leaders and national law enforcement officials-will depend greatly upon the ability of the international community to cooperate in detecting, preventing and deterring potential cybercriminals, as well as prosecuting and punishing those who commit cybercrimes. More specifically, the international community must develop international standards regarding extradition, mutual legal assistance, transfer of criminal proceedings, transfer of prisoners, seizure and forfeiture of assets and recognition of foreign penal judgments. This study does not attempt to make specific recommendations for achieving each objective (Thompson, 2008). Nonetheless, this study does address the threat of cybercrime in broad stroke by examining how international law and economics may contribute to achieving such objectives.

Customary international law: A global problem as large as and as pervasive as cybercrime should find a solution within the framework of international law (Hildebrand, 2002). Although international law has no criminal system of its own, from its beginnings, it has served to keep the peace among nations. Without constitutive documents to rely upon, international law nevertheless sets forth the body of rules that are legally binding on states in their interactions with each other (Economist, 2004). Formal and material sources of international law provide evidence of the existence of

consensus among states regarding accepted rules or practices, which are legally binding on each state[2]. This study will explore the ability of customary international law to combat the plague of the Internet that is cybercrime.

General principles: A primary source of international law is found in state custom. By one account, customary international law may be regarded as an "implied and often non-verbalized exercise of direct legislation by the members of society," which constitutes "a spontaneous norm (Wood, 1981)." Such deduction is made based upon the fact that the international legal system identifies customary law in the form of established norms, rather than by creating customary law through some exercise of sovereign authority. To wit, customary international law is formed and has the force of law because of the practice and behavior of states, not because of any legislated or written rules. Thus, the two elements of customary international law consist of:

- State practice
- Opinio juris[3]

Finally, customary international law-like the common law and unlike statutory law-is a dynamic process of creating law that is universal in application, which is especially relevant to addressing the threat of cybercrime given the objective of implementing an international solution.

State practice: In determining whether a state practices a certain custom, courts consider the duration, the consistency, the repetition and the generality of a particular practice. No hard-and-fast rules have evolved regarding a time element. However, the International Court of Justice has elucidated basic rules regarding continuity and repetition. For example, a customary rule must accord with a "constant and uniform usage practiced by the States in question." Furthermore, state practice must be "extensive and virtually uniform (Dibadj, 2007)." However, the uniformity rule is not absolute: the state practice requirement will be satisfied if "consistent with (customary) rules and... (if) inconsistent with a given rule, (it) should generally have been treated as (a) breach of that rule." Repetition may even be completely unnecessary under certain circumstances (i.e., customary international law may be created in a single act or spontaneously). Thus, to the extent that customary law is capable of quickly responding to the crime committed in cyberspace, it is a valuable tool to combat cybercrime.

Finally, the courts consider whether a state practice is general. The generality requirement implicitly means that the state practice must be generally accepted practice in the international community. The general application, however, does not require every state to observe or accept the practice. In fact, even if a practice is limited to just a couple of states, it may still constitute customary international law as applied to those two states (Etro, 2006). In such cases, the practice is considered to have specific application, rather than general application. In the Internet realm, specification application of state practice may assist in addressing certain instances of cybercrime, but it is obviously less meaningful than practice of general applicability, which would bind all states to a custom (Hildebrand, 2002).

Opinio juris: The second requirement of customary international law is that each state view a certain practice as legally obligatory, as opposed to a mere usage performed out of "courtesy, morality, or fairness." It is this subjective belief in owing a legal obligation that turns usage into a custom. The International Court of Justice, has on three occasions, interpreted the opinio juris requirement rather strictly. For example, in the Lotus case, the North Sea Continental cases and the Nicaragua case, the International Court of Justice rejected a presumption of opinio juris.

Instead the Court required evidence of a belief that the practice was obligatory. Obviously, a strict interpretation of the opinio juris requirement would tend to fasten customary law to a rigid and potentially outdated rule, which is contrary to the very idea of customary international law as an organic and continuously growing source of international law. To the extent that the courts view evidence of opinio juris liberally, customary law may serve as a viable tool to protect the interests of the international community against cybercrime (Johansen, 2005).

To summarize, the fact that customary international law applies universally throughout the international community makes customary international law especially well-suited to address legal issues arising in the context of the Internet. Furthermore, customary law has, on occasion, been quick to develop when previously unaddressed issues of international concern arise, as was the case with the development of custom regarding outer space law. Probably not detrimental to its applicability to cybercrime, but definitely weighing against it, the fact that "custom is normally a relatively slow process for evolving rules of law" (Hopgood, 2006). Finally, the more rigidly the courts interpret opinio juris, the less useful customary international law can be used as a tool to end cybercrime. With the help of economic principles, the rest of this study attempts to fine tune customary international law to meet the needs of states fighting cybercrime.

RESULTS AND DISCUSSION

Applying international law and economics to combat cybercrime: "International law is the product

of its environment." It is a system that regulates and defines the rights and obligations of states as they interact with each other. International law developed as a result of the customary notions of international relations. In order for international law to endure, it must adapt to the prevailing realities of the cyber age. Somewhat differently, economics is concerned with determining which laws are the most efficient (Economist, 2004). An economically efficient law is one that provides for achieving a goal (transaction) at the least possible cost. In the international domain, economic analysis of law provides a behavioral theory that predicts how actors-in this case, states interacting in the international community-will respond to different structures of the international legal regime. As this study stresses, an economic approach to international law, as this study stresses, can assist states in developing optimal solutions that address the cybercrime problem.

An economics approach to customary international law: Economic analysis provides that decentralized market processes are comparatively more efficient than centralized processes. In this respect, customary law, which is created voluntarily and spontaneously, is a highly efficient process for creating rules of international cyber-law (Hovenkamp, 2001). Historically, traditions of international economic law can be traced back to the law merchant and sets of principles used to resolve conflicts involving jurisdictions. Presently, the international community is challenged by similar problems that in order to rid the Internet of cybercrime. Because customary international law permits states to cooperate in the absence of formal written agreements, it minimizes the transactions costs associated with negotiating bi- or multi-lateral treaties (Gerber, 2008). Thus, on its face, customary international law appears to provide an efficient means for responding to cybercrime.

Symmetrical cybercrime interests: In a perfect digital world, each state is confronted with symmetrical conditions and preferences. Here, the incentives of each state are perfectly aligned with other states. For example, states concerned about cyber-crime may each regard permission prior to chasing digital data across borders as an unnecessary hindrance to combating cybercrime. Under this scenario, an international cybercrime custom would emerge to which all states would agree. Regardless of the custom, each state expects the same levels of costs and benefits to create and adhere to such custom (Duncan and Brian, 2008). Therefore, in creating international custom relating to cybercrime, each state has an incentive to agree to rules that not only maximize its benefits, but also incidentally maximize the welfare of the entire international community.

Asymmetrical cybercrime interests: In the real digital world, however, states are unlikely to have perfect incentive alignment.

One reason is because customary international law and law enforcement relating to cybercrime constitute public goods (Gerber, 2008). In the context of cybercrime, the public goods problem arises because each individual state faces a private cost and generates a public benefit when it engages in creating and enforcing customary international rules that address cybercrime. Without reframing the public goods problem, states will produce and enforce suboptimal levels of customary international law in response to the threat of cybercrime. In fact, a state confronted with a public goods problem will only create or enforce customs addressing cybercrime to the extent that its marginal cost of doing so is less than or equal to the marginal benefit that it expects in return (Hopgood, 2006).

Where, states have diverse interests and the probability of future interaction with respect to a subject such as cybercrime is high, each state's discount factor bears on the likelihood of an optimal solution. Under game theory, a discount factor is a function of both:

- A state's time preference
- The probability of future interactions

First, the more that a state prefers quick resolution of an international problem, the less it values future resolution of such problem (Etro, 2006).

In cybercrime cases, state law enforcement agents must be able to search and seize electronic data before it is destroyed, which may be done at the click of a mouse. Therefore, states responding to cybercrime will generally have a high preference for time and they will be less interested in trading present payoff (i.e., the chance to catch a cybercriminal now) for an expected increase in future payoff (i.e., the less likely chance to catch a cybercriminal at some future date). In other words, states pursuing cybercrime beyond their borders will be less likely to cooperate with states viewed as unlikely to permit them digital entry into their sovereignty; thus, the pursuing states have a low discount factor (Economist, 2004).

Second, the greater the probability that states will interact in the future, the greater the expected value of future cooperation (Hopgood, 2006). A state that believes it will interact with other states in the future-as the result of it pursuing a cybercrime abroad or because another state may seek to pursue a cybercrime within its borders-will be more willing to develop efficient customary rules relating to cybercrime. Conversely, if a state believes that future interaction is unlikely, or that a "one-shot" interaction is likely, it has no incentive to cooperate because doing so will not increase the expected value of future cooperation (Rodger, 1996).

As the expectation of future interaction of any one state is unknown and may not be generalized, the discount factor for this element is unknown. "Only where there is a relatively large discount factor, do long-run optimization strategies become evolutionarily stable."

Several other misalignments of cybercrime interests may exist in the international community. For example, states that are economically less dependent upon technology have less incentive to create rules in which cybercriminals are effectively deterred and punished. To go further, some states may even benefit from loose national rules relating to cybercrime and strict rules relating to territorial sovereignty, which would effectively create a refuge for cybercriminals (Bishop and Marsden, 2006). Put somewhat differently, states that opt out of international customs relating to cybercrime may permit by default the development of a market for cybercrime.

Asymmetric or unknown state interests present obvious challenges to international cooperation in preventing and deterring cybercrimes and in subsequently punishing cybercriminals. Nevertheless, states seeking to induce a socially optimal level of cybercrime custom in international law may employ several economic tools to align diverse interests.

Creating symmetrical cybercrime interests: As was demonstrated above, perfect incentive alignment among states would be a rare occasion. Incentives can be aligned, however, once states agree to a framework in which certain conditions reduce the likelihood of uncooperative behavior (Hovenkamp, 2001). Three methods described below-namely, role reversibility, reciprocity constraints and articulation-can help align state interests so that efficient customs of international cyber-law may emerge.

State role reversibility: One mechanism for aligning states' interests is to impose role reversibility constraints upon each state (Dibadj, 2007). Advocates of the law and economics school often use the example of the law merchant to demonstrate the effect of role reversibility on the emergence of efficient customary international law (Craig and De Búrca, 2008). In medieval times, traveling merchants conducted business abroad in a capacity as both buyer and seller. In establishing customary norms, merchants sought to protect both their interests as buyer and their interests as seller. Because they knew that any rule having a positive effect on one set of interests (e.g., seller interests) could negatively affect their interests on the other side of the equation (e.g., buyer interests), merchant law evolved which took into equal consideration the interests of buyers and sellers. The crux of role reversibility is that "an otherwise conflicting set of incentives (is changed) into one that converged toward symmetrical and mutually desirable rules."

In the same way, role reversibility could be used to align each of the states the cybercrime interests (Dibadj, 2007). Take for example, international law concerning territorial sovereignty on the one hand and a state's need to pursue cybercrimes being perpetrated from abroad on the other. A large debate surrounds the issue of when a state may independently perform cross-border data searches without violating international law. One forceful argument concludes, "In the criminal context, customary international law generally prohibits law enforcement officials from one country from exercising their functions-such as conducting searches or making arrests-in the territory of another state without that state's permission." Without a supplemental rule, such custom seriously impedes any state's ability to quickly respond to cybercrime (Economist, 2004).

On the other side, however, is the United States, which recently manifested its views on the issue by engaging in a remote cross-border search and seizure of electronic data located on computers located in Russia. Even though the United States had a strong interest in obtaining evidence and in capturing cybercriminals before it was too late, if asked, its government would be unlikely to advocate a rule in which states were permitted to transgress territorial sovereignty at will. Clearly, the United States would object-as did most of the international community in the Alvarez-Machain kidnapping-if the roles were reversed. Similar to the case of the traveling merchant, states will seek rules that protect two distinct sets of interests. At times, states will want to protect their territorial sovereignty interests; while at other times, they will want expedient rules that permit pursuing cybercrime transgressions that originate from abroad (Duncan and Brian, 2008). The development of efficient rules of customary international law relating to cybercrime depends, in part, on a successful system in which spontaneous and decentralized decisions are made by state actors. Over time, as states engage in interactions involving cybercrime, their roles will reverse and international cybercrime customs will emerge and be followed by states acting in pursuit of their economic interests.

State reciprocity constraints: A second and perhaps stronger, method of converging the interests of states is by inducing reciprocity constraints. So for instance, if Goldsmith and Posner are correct in believing that reputational effects have little do with compliance with customary international law, a state may be tempted to ignore custom in exchange for a higher payoff. States may eliminate the incentive to pursue opportunities that are sub-optimal by binding their strategic choices to those of other states. Professor Parisi explains that the key to the reciprocity principle is embodied in the age old ideal of "do unto others as you would have done to you."

Without reciprocity constraints, states will not achieve the best solution to combat the threat of

cybercrime. For example, states pursuing digital evidence of crimes committed in cyberspace must act quickly before data is lost or destroyed. In contrast, states from which permission is sought to collect evidence have traditionally required such requests to proceed through an often formal and cumbersome process, which is not conducive to capturing invisible and fleeting cybercriminals (Bishop and Marsden, 2006). In addition, the state withholding its permission is better off under the status quo because it expends no energy or resources in providing legal assistance.

Also adding to the expense of legal assistance in the area of cybercrime requires developing technical expertise. Finally, with the growth of the Internet, "more and more evidence will be located across international borders." These costs suggest that the state from which permission is requested can achieve a higher pay-off by stonewalling (Rodger, 1996).

Automatic reciprocity constraints would induce states to arrive at an optimal cybercrime outcome because a state's incentive to behave opportunistically would be eliminated. Analyzing the problem from an ex ante perspective-that is to say before cybercrimes occur-each state will create customary rules that it would like to be applied to it regardless of the circumstances (i.e., regardless of whether the state was requesting legal assistance or whether the state was presented with a request for legal assistance). If a state established rules taking into account and hoping to benefit from, only one set of probabilistic circumstances, it may be gambling unwisely.

This will happen because if in the future converse circumstances exist, reciprocity will dictate applying the same opportunistic rule previously established by the state, against the same state.

Therefore, states confronted with the possibility of being in either of two situations-requesting permission from a state or considering a request for permission from a state-will create international cyber-law custom that is socially optimal.

State articulation: A third technique for aligning the interests of states involves in requiring states to clearly articulate their intentions to follow certain international customs. As professor D'Amato explains the theory, articulation requires states to make an objective (notice the element of subjectivity is removed) statement or expression regarding the legality of particular international customs either prior to engaging in state practice or at the same time the state begins to engage in state practice. The purpose of articulation theory is to fix the primary challenge that the opinio juris requirement presents to the spontaneous formation and continuous development of customary international law-the requirement that a state produces evidence that another state believes it is obliged to perform a specific state practice. In application, articulation theory crystallizes. International law emerging to address cybercrime would benefit greatly if states articulated customs that they intend to apply. Consider once more the issue of territorial sovereignty in cyberspace (Johansen, 2005). Viewing the problem ex ante, states have an incentive to "articulate and endorse norms that maximize their expected welfare." The incentive arises because states must base their decisions on unforeseen events and some probability that they will be on either side (or on both sides) of the issue at some future date. No state knows in advance whether it will need to pursue evidence of a cybercrime in another state, or whether a foreign state will seek evidence of a cybercrime within its digital borders. So, for instance, based on articulation, the following customary rule might emerge: a state may pursue digital evidence of a cybercrime located in another state's territory so long as it notifies the appropriate jurisdictional authorities of its activities and investigates in good faith (Thompson, 2008). The example, although perhaps not arriving at "the" solution, demonstrates that states will articulate rules that tend to maximize the expected welfare of the entire international community, rather than one side's narrow interests.

The primary benefit of articulation is that it eliminates the guesswork associated with the opinio juris requirement. Consistent with the goals of economics, articulation improves the efficiency of international customary law by reducing the transaction costs associated with creating and following such laws. Similarly, articulation of customary law prior to engaging in state practice (Alese, 2008), puts other states on notice of the articulating state's state practice intentions. In these ways, customary international law is allowed to grow and to respond to new challenges such as those that have arisen in the fight against cybercrime (Thompson, 2008).

CONCLUSION

If any international issue is ripe for a "transnational" solution, it is the enigmatic and borderless disease of cybercrime. This study argues that any "cyber-law" solution seeking to deny the digitally depraved of the ability to employ the Internet as a vehicle of criminal enterprise must be international in scope. In addition, due to the nature of the Internet, which is in a state of continuous flux and evolution, any response by states hoping to stop cybercrime must also be flexible and capable of evolving. Customary law presents the most efficient and effective means for the international community to address cybercrime. By borrowing principles from economics to align states' interests for purposes of forming cybercrime rules,

states may achieve optimal customary international law that maximizes the welfare of the entire international community.

REFERENCES

Alese, F., 2008. The EC Commission Article 82 Guidance. Institute for Consumer Antitrust Studies, Loyola University Chicago Law School.

Bishop, S. and P. Marsden, 2006. Editorial the article 82 discussion paper: A Missed Opportunit. Eur. Compet. J., 2(1).

Craig, P. and G. De Búrca, 2008. EU Law, Text, Cases and Materials. 4th Edn., Oxford University Press, Oxford, New York, pp: 1016-1005.

Dibadj, R., 2007. Article 82: Gestalt, myths, questions. Santa Clara Comput. High Technol. Law J., 615, 23(4).

Duncan, A.R. and M.S. Brian, 2008. Loyalty and Fidelity Discounts and rebates in the U.S. and E.U.: Will divergence occur over cost-based standards of liability? Sedona Conference Journal, J.133 , Fall 2008.

Economist, 2004. Slackers or Pace-setters: Monopolies may have More Incentives to Innovate than Economists Have Thought. Economic Focus, 20 May 2004, pp: 84.

Etro, F., 2006. Competition policy: Towards a new approach. Eur. Compet. J., 2: 29-55.

Frazer, T., 1992. Monopoly, Competition and the Law. Harvester Wheat Sheaf, 2nd Edn., New York, London, Toronto, Sydney, Tokyo Singapore, 1992, pp: 43-53.

Gerber, D.J., 2008. Two forms of modernization in european competition law. Fordham Int. Law J., 1235, May.

Glader, M., 2004. The Innovation Markets and Competition Analysis: EU Competition Law and US Antitrust Law. Lund University, Malmo, pp: 55-61.

Hildebrand, D., 2002. The Role of Economic Analysis in the EC Competition Rules. 2nd Edn., Kluwer Law International, The Hague/London/New York, pp: 126-170, 278-305.

Hopgood, S., 2006. Keepers of the Flame: Understanding Amnesty International. Cornell University Press, Ithaca, N.Y.

Hovenkamp, H., 2001. Post-Chicago antitrust: A review and critique . Columbia Bus. Law Rev., 2001(2): 257.

Johansen, E., 2005. I say antitrust; You say anticompetitive: Why bridging the divide between U.S. and E.U. competition policy makes more economic sense. Penn State Int. Law Rev., 24(2): 331-352.

Nagy, C.I., 2007. Refusal to deal and the doctrine of essential facilities in US and EC competition law: A comparative perspective and proposal for a workable analytical framework. Eur. Law Rev., 32(5): 664-685.

Nerep, E., 2001. Extraterritorial Control of Competition under International Law 1983. New York Times, 24 June, 2001.

Rodger, J.B., 1996. The oligopoly problem and the concept of collective dominance: EC developments in the light of US trends in antitrust law and policy. Columbia J. Eur. Law, 2(1996): 25.

Stothers, C., 2001. Refusal to supply as abuse of a dominant position: Essential facilities in the european union. Eur. Compet. Law Rev., 22(7): 256-262.

Thompson, A., 2008. Beyond expression: Amnesty international's decision to oppose capital punishment, 1973. J. Hum. Rights, 7(October): 327-340.

Weitbrecht, A., 2008. From freiburg to Chicago and beyond: The first 50years of European competition law. Eur. Compet. Law Rev., 29(2): 81-88.

Wood, E.M., 1981. The separation of the economic and the political in capitalism. New Left Rev., 127(June): 66-95.

End notes:

1: European Policy for Intellectual Property
2: Report by Economic Advisory Group for Competition Policy, 2005
3: Opinio juris vel necessitates