

THIS IS A WORKING DRAFT: PLEASE DO NOT QUOTE WITHOUT
AUTHOR'S PERMISSION.

**Closing the Book on the Cybercrime Debate: Comments from the CIP
paper series¹**

Daniel J. D'Amico
George Mason University
Graduate School of Economics
ddamico@gmu.edu
<http://austrianaddiction.rationalmind.net>

JEL codes: K4, O3, H4, F1

Abstract:

This paper attempts to complete the laissez faire analysis of cybercrime begun by the Critical Infrastructure Protection Project presented at George Mason University in the Spring 2005 semester. First, a five section analytical outline is presented which organizes the CIP material in a cohesive manner. By concluding the analytical outline this paper hopes to define and explain the justification for laissez faire policy promotion by using the CIP presented material as its foundation. Two critical areas expanded beyond the CIP material include distinctions made between ex-ante and ex-post mechanisms of enforcing justice and the unavoidable differences of enforcement at play in the context of intellectual v. tangible property claims. By filling in these implied but missing aspects of analysis this paper hopes to strengthen the case for laissez faire policy suggestions in both the cybercrime context and beyond.

¹ Much appreciation is shown to the Mercatus Institute and the Earhart Foundation for financial support of this research. A special note of thanks is also due to the Ludwig von Mises Institute for housing and support throughout the 2005 summer months, during which much of the research for this paper was performed. Thank you also to all of the helpful suggestions and comments I have received from workshop participants including but not limited to: Peter Boettke, Richard Wagner, Nick Schandler, Mike Makowsky, Jennifer Dirmeyer, Geoff Lea, Josh Hill, Nicolai Wenzel, and Jen Smith, and all of the original participants of the CIP presentations as listed in the reference sheet. Any errors contained within this draft are of course my own. This paper is also scheduled to be presented at the [Austrian Students Scholars Conference](#), and an earlier presentation of the material here is available at:
http://austrianaddiction.rationalmind.net/archives/2005/07/cybercrime_pres.html

1. Introduction:

The Critical Infrastructure Protection Project (referred to as CIP from here on)² sponsored the weekly event entitled; “Seminar on the Law, Economics and Technology of Private Enforcement of Contract on the Internet.”³ It was held at George Mason University’s law school in the spring of 2005, and contained presentations of the following papers:

1. “The Capability of Government in Providing Protection Against Online Fraud,” by Edward Stringham.
2. “Is Cybersecurity a Public Good,” by Ben Powell.
3. “Private Dispute Resolution in the Card Context: Structure, Reputation, and Incentives,” by Andrew Morriss and Jason Korosec.
4. “From Imperial China to Cyberspace: Contracting Without the State,” by David D. Friedman.
5. “Who’s to Protect Cyberspace?” by Christopher J. Coyne and Peter T. Leeson.
6. “The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement Without the State,” by Bruce Benson.
7. “The Economics of Computer Hacking,” by Peter T. Leeson and Christopher J. Coyne.

This paper begins by summarizing the inferred conclusions of the seminar. Scholarly work is often produced with a direct intention to refute or combat an existing explanation or theory. Upon successfully eliminating fallacies and misunderstandings a new outlook is left to be implied but should ideally be synthesized from the existing material and used to develop a replacement corrected explanation of the phenomenon in question. Given the situation that an accepted answer is prevalent, those theorists who wish to challenge it have a two fold task ahead of them; first, to explain its error, and second to return to the original question and offer an explanation more reasonable and accurate in its conclusions.

The CIP seminar’s purpose was to investigate the potential of market forces to provide security against crime on the World Wide Web. Along its path, particular pieces offered models for apparently unexplainable behavior involved in computer crime⁴, described historical comparisons that paralleled modern technology savvy criminal behavior⁵, traced technological advancement in relevant industries effected by cybercrime⁶, and refuted popular conceptions of cybercrime as a market failure in need of state intervention⁷. At first glance it is difficult to determine if this sequence has achieved its goals, but with a proper analytical outline of progressing such an applied research agenda and viewing the individual pieces as an integrated unit, the remaining conclusions are apparent and exposed, hopefully shutting the book on the question of cyber crime in favor of laissez faire rather than public policy responses.

² For more information on the CIP project see the homepage at, <http://cipp.gmu.edu/>.

³ For a full schedule and linked paper texts see:

<http://www.gmu.edu/departments/economics/pboettke/cip.html>

⁴ (Leeson and Coyne, “Economics of Computer Hacking,” forthcoming)

⁵ (Friedman, forthcoming)

⁶ (Morriss and Korosec, forthcoming)

⁷ (Stringham, forthcoming and Powell, forthcoming)

This paper outlines the structure of a successful applied research agenda and how the CIP papers fit within it, then it will elaborate points which were not directly made within the texts of the CIP seminar, but are implied by expanding the analytics and filling in market process abstractions where no such theorizing has been done. These new process oriented abstractions rest upon two key definitional distinctions applied to cybercrime originally in this paper. The first is a distinction between ex-ante and ex-post mechanisms of justice provision, and the second is a distinction between intellectual and tangible property claims in cyberspace. By expanding the cybercrime analysis with these distinctions, this paper hopes to replace the market failure explanation of cybercrime with an analysis which fully explains the economic structure of cybercrime, and how market forces simultaneously adjust and respond to such phenomenon. Market adjustment takes place by actors on the margin of influence. Having traced more fully the forces which influence such marginal actors, one can recognize that subtle nature in which markets adjust. The paper will conclude by drawing notice to the fact that cyberspace stands as an ideal example to support the case for laissez faire policy suggestions, because of its frontier-like characteristics as a cutting edge technology. Thus the case for free markets in due thanks to the work of the unified research efforts of the CIP project will have been strengthened.

The benefit of having such an analysis is to hold a point of comparison between economically sound laissez faire perspectives on the one hand, and incongruent state growing interventionism on the other. The particular research interest of cybercrime goes beyond an applied theoretic and stands as an example of the superior logical integrity of a laissez faire society, given a growing dynamic conception of technological advancement. In this broader understanding cybercrime serves as an ideal example of a dynamic technological advancement which has outgrown state legislative institutions.

Though the individual papers draw out the point by point defenses of market responses to cybercrime they more generally imply a more serious problem of legal authority. Cybercrime may be one of many frontier arenas which centralized legal institutions are inept at handling. As the internet proportion of the greater economy is growing ever more dominant, the solution of this particular issue may have serious presidential effects on the way problems are solved and institutions are shaped in the future, thus exposed is the great importance of the CIP seminar as a whole. The management of legal institutions applied to the internet holds the fate of an unquestionably vast amount of wealth and resources. It is in this hope that the mission of the CIP program is worded; "The Critical Infrastructure Protection Program seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the nation's critical infrastructures."⁸ Take notice of the effort to integrate the disciplines of law, policy, and technology. It is the failure to draw on the dispersed knowledge of these fields which causes responsive policy to miss its mark. This mission holds the key to avoiding the setting up of short sighted policy with unintended consequences and promoting effective policy framed with an

⁸(CIP, "Mission," 2005). Cyberspace is not the only form of infrastructure; other infrastructure examples include roads, schools, public utilities, and many more.

understanding of that which is seen and of that which is unseen. Doing so reclaims the definitional meaning of the term critical infrastructure. No longer do market solutions have to take defensive stances against centralized interventionist policy arguments, but it is such policy arguments which must be defensive as they will be exposed as predominantly detrimental to their stated ends of protecting such critical infrastructure. If one is to accept such a critical nature of infrastructure then one should truly support the laissez faire solution as the only mechanism to produce optimal allocations of such provisions necessary to develop said infrastructure.

2. The CIP project as an applied research agenda.

The CIP project papers can be organized to fit within a five stage analytical outline of addressing the issue of cybercrime. This process may serve useful at structuring more applied research agendas in the future. Whether this approach was planned or not is unknown to the author of this paper, but it is certainly present from reading the material as a collective whole. Perhaps the ideology of the CIP project was planned from the beginning as is implied by the selection of the predominantly market oriented author base, but seeing the extent to which the papers overlap material and semantically differ in their definitions, it is clear that no systematically planned outline of research was coordinated. This implied analytical outline could just be a product of the mere bulk of material dedicated to a similar ideological perspective. The structure of inquiry is as follows:

1. What is the problem in question?
2. How is the current state response inadequate, and what elements of the market have the potential to respond to the problem without the state?
3. How is the market preferable to the state at responding to the problem?
4. What is to be done in the immediate sense to respond to the problem of cybercrime, given what we know from answering our earlier questions?
5. Can insights be taken from the applied agenda and re-enforce our broad understanding of the way things work, in other words, what has been learned?

The following sections hope to walk through the analytical structure, organizing the material from the collected papers into each accordingly. Where gaps are left over upon completion, this paper will offer abstractions and finally conclude.

1: What is the problem in question?

To offer an explanation or proposed solution to a problem an analyst must know what the problem is. It must be clearly defined in its magnitude and relative importance to himself and his audience. Each paper within the CIP collection defined its own particular task in a subtly nuanced way distinct from one another. In doing so each paper addresses a clearly defined question, but when viewed together a unified or broad understanding is not so much obviously presented as it is implied from further extrapolation.

Friedman (forthcoming) describes the cyberspace frontier as one which will stretch the boundaries of the way contracts are created to promote security and privacy. He explains that:

Commercial activity in cyberspace, mostly on the World Wide Web, is increasing rapidly. Such commerce poses two rather different problems for conventional mechanisms of public contract enforcement. One, likely to be important in the near future, is that cyberspace has no geographical boundaries. Purchasing goods and services from the other side of the world is as easy as purchasing them from your next door neighbor. Delivery of physical goods is more costly from the other side of the world—but a considerable part of cyberspace commerce is in information goods and services, and they can be delivered online just as they can be purchased online. It follows that an increasing fraction of commercial transactions, especially of transactions by private individuals, will be between parties in different countries.⁹

Stringham (forthcoming) brings up similar concerns as Friedman regarding the logistically cumbersome characteristics of cyberspace in its compatibility with current conceptions of enforcement and the rule of law. He draws attention to three key issues which must be kept in mind throughout the stages of our analytical outline. First, particular resources are needed to operate and regulate computer networks, including costly cutting edge technologies and capable human labor. Second, cyberspace is an ever changing environment of new people and places; it seems too hard for a central authority to ever keep up. And third, the international nature of cyber commerce makes current legal enforcement have miniscule deterrent effects despite its intentions.

Stringham begins his paper by drawing attention to the problems that are posed by online fraud. “In today’s world up to 40 percent of online international orders are fraudulent which has the potential to cripple electronic commerce.”¹⁰ This statement is an adequate illustration of the hazardous nature of trading via the internet, but points the reader’s direction towards a more technical point of recognition; the incentives which drive entrepreneurship and the importance of gains from trade.

The statistic has two parallel accountings of losses intrinsic within its meaning. First, the obvious losses to those within the industry who directly experience the negative effects of such fraudulent orders and the second, more important aspect of this opening statistic is not its mere quantitative value of 40 percent, though it does seem striking, but the way in which this numeric value is perceived to potential cyber-market entrants and potential cyber-market expanders.

If merchants have no recourse to fraud and they cannot easily distinguish between good and bad orders, they will end up acting cautiously and

⁹ (Ibid, 10) All page numbers refer to the page numbers of the CIP papers as each beginning with page one, because no manuscript of the compiled papers is available as of yet.

¹⁰ (Stringham, forthcoming, 1).

turning down a number of legitimate orders. Some merchants may even eschew electronic commerce altogether and the market will not reach its full potential.¹¹

All of society suffers a great loss from this unrealized gain from trade. At this stage there is little ability at quantifying this potential gain from trade so there is no way of calculating true estimated losses from the problems of cybercrime.

Stringham's figures show that cybercrime is a problem of financial magnitude, but one is forced to blur the quantifiable lines of such a magnitude because of the uncertainty associated with trades that have not taken place. With this in mind Powell's (forthcoming) paper is focused on putting the reader's mind at ease to the notion of the cyber market unraveling. He posits that while cyber security does possess a number of the characteristic problems which public goods tend to carry with them, recent history is showing us a market environment demonstrative of responsiveness, innovation, and investment nonetheless. He concludes by stating:

Cyberterrorism against private critical infrastructure is not a problem that requires special government attention. According to the evidence examined here, the government should not be concerned with any general market failure in the provision of cybersecurity. While some aspects of cybersecurity have certain "publicness characteristics," we find many ways in which private orderings in the market provide security despite theoretic problems. Examining the financial services industry, part of the critical infrastructure of our economy, we find no evidence of a pervasive market failure to provide cybersecurity. Instead we find wide spread uses of many technologies, increasing budgets and innovation in adopting new technology. When compared to firms in other countries, financial firms in the U.S. are early adopters and generally better prepared for cyber attacks than foreign competitors. Since any externality created by unsecured computers is not limited by national boundaries, it is not likely U.S. policy could correct for such an externality anyway. Cybersecurity is being provided in the private sector and it is best left free of cumbersome government regulations that may prevent private voluntary orderings from continuing to innovate to secure cyberspace.¹²

While the authors previously mentioned have taken the offense by hunting down theories of market failure and calls for government intervention, some of the authors provide useful descriptions to building such pro-market defenses by offering historical documentation of where the problem of cyber crime came from and make parallels throughout broader legal and technological histories. Friedman (forthcoming) and Benson (forthcoming) most specifically try to fill in the gaps of answering the questions; where did the problem of cyber crime come from? Friedman introduces his paper as predominantly a historical piece with the following statement.

¹¹ (Ibid, 1)

¹² (Ibid, 11)

The problem of settling commercial disputes without state courts was dealt with in medieval Europe in part by the development of private courts at the major trade fairs, run by merchants and relying heavily on reputational enforcement. No equivalent seems to have developed in China, perhaps due to Imperial hostility to any rival authority.¹³

He continues by presenting the cyber crime question in a broader notion of security technologies.

Whatever the mechanisms responsible—interested readers can find a more detailed account in Brookman’s chapter—Chinese merchants a century ago succeeded in maintaining a sophisticated system of contracts with very nearly no use of state enforcement. It is the thesis of this paper that the past of China is our future—that parties to online transactions will, over the next few decades, face essentially the same problem, and find, *mutatis mutandis*, similar solutions.¹⁴

These historical accounts help to start the analytical outline in the right direction by forcing us to recognize the simultaneous elements of cutting edge unique technologies with long developed legal traditions. Friedman explains logistical similarities between present day internet commerce and ancient China, and how both are capable of overcoming such logistical set backs through entrepreneurial creativity. Benson (forthcoming) draws a parallel between cyber-markets and physical markets in a broader sense by showing the general trend of spontaneous emergent rules of order to facilitate contracts and enforcement in relatively anarchic states. Benson’s body of research beyond the CIP project is dedicated to similar topics and can be summarized in saying that not only are such spontaneous developments possible but they are also preferable to centralized policies. Such bottom up emergent rules tend to be more feasible to be enforced and representative of citizenries preferences for freedom and autonomy as a product of their promotion within competitive polycentric environments.¹⁵

These historical explorations force the analytical outline to be one which constantly returns to its first stage for re-assessment. The problem of cybercrime must be continually redefined from new insight gained throughout the stages of inquiry. If such lines of inquiry expose vast similarities between cybercrime (our new frontier) and existent legal systems, then perhaps no special case is needed to be applied. If such similarities exist but dysfunction reigns supreme in the existent system nonetheless, than the investigation of the frontier realm has taught us something unrecognized before. Perhaps no successful applied research agenda can be performed without universal abstractions correctly applied to the broadest level of institutional influence, otherwise the traced lines of influence are blurred and confusing.

¹³ (Ibid, 1)

¹⁴ (Ibid, 3)

¹⁵ (Benson, forthcoming, 1990 and 1998)

2. How is the current state response inadequate, and what elements of the market have the potential to respond to the problem without the state?

It may be said that the second step of the analytical outline was defined by the intention of the CIP project and the intentions of selecting the chosen authors. In this sense it appears that the analytical outline is dictated by ideology, I disagree. I would claim that the structure of the analytical outline was dictated long before any of the authors of the CIP project were commissioned to participate. It was set in stone by the mere necessity of balanced scientific inquiry and the lack of such market explanations in such policy debates. The second stage takes the approach of showing the potential of the free market to solve the problem in question. It may appear as ideologically biased, but recognizing the place of such a research agenda within the context of a greater battle over ideas, one could make the argument that the bias is surely tipped in the opposing direction.

Stringham's (forthcoming) focus was to demonstrate how the state was incapable of successfully preventing fraud in electronic commerce. Though Stringham does not attempt to describe the micro process of cyber crime his paper provides a macro framework which a micro structure must aim to explain. Though his approach may seem simplistic in this lacking, his successful demonstration of government's futility in performing the role of justice provider points proposed solutions towards the free market.

Stringham's paper successfully demonstrates that government policy and action are incapable of alleviating fraud in the ever changing, fast-paced, and international environment of electronic commerce. His secondary conclusion portrays the classical liberal analysis promoting state justice as suffering from the "Nirvana fallacy."

More importantly Stringham's paper draws attention to a growing area of applied anarcho-capitalist theorizing¹⁶, containing vital importance in highly technical areas such as cyberspace where common knowledge and social norms are rarely known and often misunderstood. It is this logistically dynamic nature of the cyber environment which makes it such an ideal candidate for applied anarcho-capitalist theorizing. Computer information systems and communication technologies are ever more changing the way particular aspects of business are conducted which requires reassessment of traditional legal institutions. The application of a successful theory of cybercrime may in fact have serious effects on the common perceptions of crime in general, and the broader institutions devoted to justice.

By now it should be evident that the realm of the internet is not completely alien to existent institutions of law and order. Friedman (forthcoming) explains the overlay of theory which exists between the relatively unknown realm of cybercrime with that of traditional contracts in general.

¹⁶ The explanations and investigations of anarcho-capitalism is a growing field of literature including but not limited to the following resources. For descriptions of societal structure under anarcho-capitalism from different ideological perspectives see: (Friedman, 1989), (Tannehill, 1970), (Rothbard, 1982 and 1985). For an explanation of the potential to be found in an anarcho-capitalist research design see: (Boettke, unpublished)

Problems arise in situations where canceling a contract and leaving everything in the possession of whoever at the moment has it will advantage one party, a situation that encourages opportunistic breach. One solution is to redesign the contract so that the two parties' performance is more nearly synchronized, reducing the incentive of either to breach. An alternative is to rely on reputation enforcement, structuring the contract so that the incentive to breach, if it occurs, is likely to be on the party who will suffer reputation penalties from breaching.¹⁷

This excerpt from Friedman's piece expresses the outlets for entrepreneurial creativity at reaping these gains from trade by structuring contracts so as to be less risky such as explained above. The implication being that as it has happened in the physical economy resulting from coordinated action inclined by economic forces, so must it and will happen in cyberspace. Friedman continues:

For controversies with substantial amounts at stake, arbitration provides a second mechanism for lowering information costs to interested third parties. A New York diamond merchant does not have to know the details of a controversy—merely the verdict of the arbitrator as to who was at fault and whether or not the party at fault provided suitable compensation to the injured party. That system works because, even if the interested party does not know the details of the controversy, he does know that the arbitrator is competent and honest. As we will see computer technology provides an equivalent that requires considerably less information and functions at even lower cost.¹⁸

And from this notion one is left to ask if such entrepreneurial incentives are the same under centralized state involvement as they are in the unhampered market? It becomes more apparent that they are not. The unintended consequence of the intended helpful efforts of state response is to mute these incentives which guide the contractual process from more to lower states of risk. And it is this recognition that leads us into the next section of our analytical outline.

3. How is the market preferable to the state at responding to the problem?

Upon successfully demonstrating the futility of state efforts to handle the dynamic conditions associated with cybercrime, the applied research agenda must move on to present the case that the market offers, if not the only solution, but at least a solution preferable to that of state control.

Such a preferable argument is best presented within the series by the pair of coauthored papers of Leeson and Coyne ("Whose to Protect," forthcoming and "Hacking," forthcoming). They recognize that the task of explaining the markets potential to solve

¹⁷ (Ibid, 2)

¹⁸ (Ibid, 8)

problems is preliminarily a task of explaining the question at hand through the insights of economics, essentially blurring the lines of where applied theory begins and ends. All of the actions and interactions within the context of behavior under question are subject to the laws of economic forces. As examples of such endeavors Leeson and Coyne model the behaviors and incentives of some of the particular actors within the example of cybercrime, ie. Hackers.

Leeson and Coyne dissect the Hack community into three groups: good hackers, greedy hackers, and fame driven hackers. The incentives of the first two groups seem in-line with typical market behavior and serve relatively little special attention as compared to the unique characteristics associated with the third. Leeson and Coyne model this group's behavior with simple economic tools.

The interaction of the supply curve for hacking and the hacking community's reaction function creates two possibilities, depicted in Figure 1 and Figure 2...

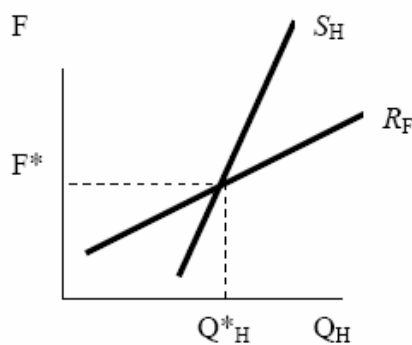


Figure 1.

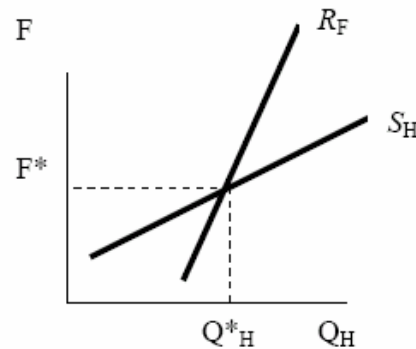


Figure 2.

In Figure 1 hackers' supply curve is less elastic than the hacking community's fame reaction function. In Figure 2 the reverse is true. This means that in Figure 1 the producers of hacks are more responsive (sensitive) to changes in fame than the community of reacting hackers, and in Figure 2 the community of reacting hackers is more responsive to changes in fame than are producers of hacks. These two possibilities have very different (and in fact, contradictory) implications for policy aimed at reducing the quantity of hacking in the fame-driven hacking industry.¹⁹

The above description doesn't appear to directly answer the question which headlines as title of this section, with good reason. The distinction between market action and state action is not so clearly defined as black and white, lots of gray matter most definitely

¹⁹ (Ibid, 19)

exists. The realm of reality to which economic science can be applied has no clearly defined boundaries and thus no actors stand clearly within nor beyond such boundaries especially within a context as logistically complicated as cybersecurity has been made out to be.

The most important insight to be attributed in this section of the analytical outline is that by explaining the economic conditions under which actors within cyberspace act and interact, one can recognize the complexity of such incentive structures and the uncertainty which shadows the anticipated outcomes of such action. With such insight in mind one cannot ignore the incongruity that exists between such complexity and the nature of centralized respondent policy. In this sense the solution of cybercrime becomes one similar to much economic activity, that of the problem of coordinating knowledge between isolated individual actors.

The peculiar character of the problem of a rational economic order is determined precisely by the fact that the knowledge of the circumstances of which we must make use never exists in concentrated or integrated form but solely as the dispersed bits of incomplete and frequently contradictory knowledge which all the separate individuals possess. The economic problem of society is thus not merely a problem of how to allocate "given" resources—if "given" is taken to mean given to a single mind which deliberately solves the problem set by these "data." It is rather a problem of how to secure the best use of resources known to any of the members of society, for ends whose relative importance only these individuals know. Or, to put it briefly, it is a problem of the utilization of knowledge which is not given to anyone in its totality.²⁰

What is apparent from looking at applied research agendas such as the CIP project is that state provision of particular goods and services lack the ability interpret and respond to such time and place specific knowledge. No mechanism is present in the provision of security via internet or otherwise which justifies or legitimizes the particular quantities which are chosen and acted upon to be allocated by the state. Ostram (1961) explains that "advances in the measurements and quantification of performance levels in the public service economy will consequently permit much greater flexibility in the patterns of organization for the production and provision of public goods and services."

4. What is to be done in the immediate sense to respond to the problem of cybercrime, given what we know from answering our earlier questions?

No sense of centralized policy seems successful at alleviating the presented problems of cybercrime, while many activities which emerge from existing forces and incentives within the free market seem to be alleviating these problems. This refocuses the direction with which we must address our policy concerns. No longer are they out to fix that which the market has failed to do but they must be framed so as not to disrupt that which the market can do. In this sense the only compatible market solution is a repellent policy

²⁰ (Hayek, 1945, 520)

promotion of repealing those policies which we recognize as being inhibitory to the functioning market for cyber security. The question which lies ahead is which policies are to be focused on for repeal? This question will be answer if only in part by the enxt section.

5. Can insights be taken from the applied agenda and re-enforce our broad understanding of the way things work, in other words, what has been learned?

This section will elaborate two areas not particularly addressed in the CIP paper series. The two definitional distinctions which are unique to this paper in regards to cybercrime are the difference between ex-ante and ex-post mechanisms of justice provision and the difference between intellectual and tangible property rights. Upon completion of these sections, I hope to strengthen the case for laissez faire conclusions and draw focus to the idea that applied research agendas operate within a context of relative importance to one another. A research agenda obtains its magnitude of importance by the scope of its institutional influence. Only upon completion of such applied research agendas as presented within similar analytical outlines such as this one can one recognize the accuracy of such magnitudes of pertinence attributed to particular social problems.

5.1 Ex-ante and ex-post mechanisms of justice provision.

When analyzed in the broader sense, the problem of cybercrime is one which concerns the provision of law and order in cyberspace. Coyne and Leeson (“Whose to Protect,” forthcoming) define their contribution to solving this broader problem by focusing their analysis on security provision and elaborating economic explanations where none existed before. This honed focus exposes a critical element to aid in the process of developing answers of the broader cybercrime question. By distinguishing between the problem in terms of broad and narrow focus we reveal a critical element to cybercrime and policy aimed at solving it and that is the contextual placement of policy aimed at solving cybercrime existing within a broader constitutional context. The critical element of such a constitutional environment is the difference between ex-ante and ex-post mechanisms of providing law and order. The terms ex-ante and ex-post are descriptive of the relationship to when crime occurs. Ex-ante mechanisms deter crime from taking place before hand while ex-post attempt to deal with the problems of crime left in their wake after they have occurred. Coyne and Leeson’s narrowed topic, security, is an ex ante mechanism while laws, investigations, arrests, incarcerations, and policy formation are ex-post mechanisms.

To show the critical difference of how ex-ante and ex-post justice mechanisms influence the rate of criminal behavior in society a formalized model is helpful to expose where the critical point of incentive comparison exists to drive the action of criminal behavior. Payoffs reaped from crime times the probability of success all multiplied by the probability of not getting caught, minus the losses associated with getting caught multiplied by the probability of getting caught, all multiplied by the probability of failure, leaves a remainder which can be defined as the driving incentive of crime.²¹ It is with

²¹In functional form the equation looks something like:
Probability of success = Ps

comparison to this remainder that other activities are compared for individuals to choose action which maximizes their own subjective utility. If the remainder is negative it can be said that he views the expected benefit of crime to be no benefit at all but a loss, and one would never expect him to perform such behavior unless his entire scope of action is directed at minimizing losses rather than reaping any benefit and crime produces fewer losses than other activities. If the remainder is positive, he views the expected benefit to indeed be a benefit, but another point of comparison must still exist to determine whether this individual will participate in crime. The ability of the remainder to out-weigh benefits (be placed higher along a listing of ranked opportunities) reaped through alternatives is the extent that an individual will opt towards criminal activities and away from lower returning activities. The key to successful action to deter such crime is to diminish the remainder of such a formula whether it is positive or negative when compared to as many of these alternatives as possible.

There are two ways to diminish such a remainder given the conditions of available resources and particular levels of economies of scale, but they each operate differently in the constitutional context. Either one may diminish the probability of success through ex-ante justice mechanisms, examples in the physical market place would include security systems, locks, fences, and the communication devices used to signal that an individual has obtained such products, or he may increase the probability of being caught and brought to justice through ex-post mechanisms, which include as stated earlier, laws, investigations, arrests, incarcerations, and policy formation.

Notice the difference between the scopes of influence that the two mechanisms have on individuals operating beneath their umbrellas. Ex-ante mechanisms must be interpreted by each subjective actor and compared to his host of present alternatives. While these mechanisms may serve to deter marginal actors (those whose scales are indeed tipped by rising probabilities of failure, diminished probability of success and most probably rising opportunity cost of investment) they do not completely eradicate the phenomenon from society as there are most likely a host of additional actors who exist beyond the margin. For example, a very successful criminal may face a slightly higher cost of success when confronted with a cutting edge security technology but that is not to say he cannot overcome the challenge. The realization must be accepted that higher costs of crime may not be inferred as high at all by some actors within a wide array of diverse individuals each possessing their own unique preference scales.

Payoff of crime = C

Probability of of not getting caught = Pn/c

Probability of getting caught = Pc

Loss from getting caught = L

Probability of not succeeding = Pn/s

Incentive to commit crime = F

So the total equation looks like: $(P_s * C) * P_{n/c} - [P_{n/s} * (P_c * L)] = F$.

Notice that the probability of success and the probability of getting caught do not necessarily sum to one. A criminal can be unsuccessful in completing his criminal activity without necessarily being held accountable for such action. The probabilities which do sum to one in this equation are the original probabilities of getting caught and success with their inverse probabilities of not getting caught or not succeeding accordingly.

Unlike ex-ante mechanisms, ex-post mechanisms do affect all actors with equal force. Raising the probability of capture and restitution has the potential to effectively eliminate the driving force of crime resultant from the proportionality that exists between the relative gains from trade in an area of commerce and crime in that same area. In this sense only ex-post mechanisms have the potential to completely eliminate rather than divert the effects of social problems such as crime.

Because of the usurpation of criminal justice by centralized provisions, the ex-ante – ex-post distinction parallels the pre- v. post- constitutional distinction familiar to Public Choice theory²². In regards to the pre- v. post- constitutional distinction, more powerful broad applications and understandings are to be found in the pre-constitutional analysis. All post-constitutional analysis takes place within the contexts of our given legal system, but avoids explaining or understanding notions of the process behind the creation of that legal system or any other possible legal system. One can only go so far in explaining the conflicting interactions of incentives between market and state actors within the post-constitutional context until he must begin asking whether the path dependent nature of our assumptions draw our conclusions to insist on more radically different structures. In this sense Coyne and Leeson's paper is a post-constitutional analysis. It describes economic forces throughout the context of the cybercrime environment (an environment encased within our current constitutional environment of state provided ex-post justice mechanisms) and how incentives are guiding individuals' behavior to provide security services which diminish the negative impact of cybercrime. By referring to pre-constitutional analysis as more powerful, I in no way tend to diminish the value of such post-constitutional theorizing, for it is from within the fertile soils of post-constitutional investigations that the seeds of a meaningful and correct pre-constitutional structure may be sown. Cybercrime has a unique potential to serve as a hinge capable of opening the door between pre and post constitutional analysis without forcing the pre-constitutional moment so often characterized by violence, revolution, or crisis. The driving force of scarcity in regards to law and order in its frontier quality can serve as mimic for the crisis of what in the physical economy is described as chaos and commonly misperceived as anarchy.

Coyne and Leeson's focus on ex-ante security issues succeeds in elaborating how private market inclined security provision outperforms the statist alternatives, but their conclusions can be strengthened by recognizing the issue of laissez faire ex-post justice provision. Without operational market forces existing between the ex-ante and ex-post justice provision simultaneously one has no way of claiming efficient conditions of resource allocation. The problem of cybercrime will not be solved but merely cycled over and over again to continually resurge and drive political responses and action. The ambiguity of quantifying the magnitude of the cybercrime problem and the hesitation to refer to any such resource allocation as efficient contextualizes all of the actions and incentives that are under our post-constitutional investigation.

²² For an explanation of the pre- v. post- constitutional distinction see: (Boettke, 1998).

Coyne and Leeson begin their analysis from basic economic principles to explain and expose the role that incentives resulting from cost benefit analysis play in the cyber crime context.

When considering any potential course of action, economists focus on weighing the benefits of the action versus its costs. More specifically, economists are concerned with the costs and benefits of undertaking an additional, or marginal, unit of the activity in question. If there is a net gain, where the marginal costs outweigh the marginal benefits, the activity should be undertaken the result being an economic improvement. Likewise if the marginal costs outweigh the marginal benefits, the activity in question should not be undertaken. Economists refer to a situation as efficient if all possible improvements have been made such that no further improvements are possible... Ultimately, what this means is that the efficient level of cyber breaches is not necessarily zero.²³

Just as Powell (forthcoming) devoted his topic; Coyne and Leeson have to overcome the public good problem of sub optimal provision in the cyber crime example in order to support a laissez faire solution.²⁴

I claim that applying the economic insight of cost benefit analysis and incentive responsive behavior to the ex-post mechanisms of security simultaneously to the ex-ante mechanisms not only strengthens the case of the laissez faire conclusions but eliminates the Public Goods concern all together in favor of theoretically unambiguous optimal allocation by the furthest reaching application of private property titles possible.

To explain let me make an example outside of the cyber crime context and back into the realm of physical real world exchange and security. In the early eighties car stereo theft was a serious problem to many urban residents. Recognizing now that few people have such serious concerns about the same issue, forces one to recognize that something must have happened between then and now which changed the incentives and conditions under which such behavior took place. Regardless of the context of laws that car stereo theft took place market mechanisms adapted so as to advance technologies to provide for the drastic depletion of car stereo theft.

Such technologies are everywhere in today's auto market, such as specialized keys, anti-theft devices so stereos only work in their registered owner's car, car alarms, and many more. In the car stereo example, the security mechanisms were successful at counter balancing the cost benefit decisions of criminals and potential victims so as to all but eliminate the behavior. For a low price consumers take precautions which raise the costs

²³ (Coyne and Leeson, "Whose to Protect," forthcoming, 7-8)

²⁴ Cowen (1992), presents a Nozickian argument that polycentric systems inevitably form into central ones. He is refuted along post-constitutional analysis as Coyne and Leeson by Stringham and Caplan (2003). Upon conclusion of the analytical outline offered through the CIP project this line of literature may serve as an example of broader areas which this project has insight in explaining from its expanded perceptions of the problem of Public Goods provision.

and lower the probabilities of success to would be thieves. Why didn't the Public Goods problem dominate the car stereo example?²⁵

I claim that the honing of technology guided by entrepreneurship under laissez faire constitutional arrangements promotes the optimal provision of security mechanisms rather than sub-optimal, thus eliminating the Public Goods problem. The only reason why such allocations are continually accused of being sub-optimal is because of logistical continuation of the negative phenomenon to take place. But diminishing the probability of success is not the only avenue to effect the cost benefit decision of would be criminals. But the example of cybercrime is different from that of car stereos in that the payoffs expected from crime on the internet is proportional to the gains from trade reaped there legitimately, while car stereos over time have become less and less expensive (thus less valuable on the stolen market), knowledge of the internet and skills at navigating it both legitimately and illegitimately leave the skilled individual with a veritable smorgasbord of profitable opportunity.

The desire to eliminate the un-reclaimable costs of crime seems to drive the purchase of security technologies. Victims prefer the crime to have never taken place rather than the justice offered within the constitutional context available. This may be representative of a universal principle of action or it may point us to notice a failure of simultaneous market operation between ex-ante and ex-post justice mechanisms. Markets are inhibited from operating in the provision of justice enforcement after crime has taken place. To illustrate what is meant by this last point think of the distinction between civil and criminal law. Civil law is enforced when individuals take suit against one another for losses that occur which lack criminal intent, while criminal law is invoked when such criminal intent does exist.

Historically private mechanisms of justice and security developed before state provisions which then crowded out such private alternatives. Only recently have such state provisions become so inefficient that economists are slowly beginning to see opting out efforts to go above and beyond these menial efforts. For example, patrol cars are a typical form of security for neighborhoods, but recently cities and states have found that lack of competitive market mechanisms have led to wasteful and costly provisions and inevitably lower levels of quality. Thus rising rates of home security systems, gun ownership, and private community security are observed as of lately. These purchases and private mechanisms is what is meant by the term opting out.²⁶ Notice how the opted out mechanisms are more honed to provide security for private individuals without promoting the incentives of free-riders, if not fully, at least better than traditional centralized patrol units. Such a trend in technological characteristics is not merely coincidental. In regards to enforcement after crime has taken place no such opting out mechanisms exist. This is inherent in the definition of a state as a monopoly of force over a particular geographical region.²⁷ For what is meant by ex-post justice provision if

²⁵ I owe the application and insight of this example to Russell Roberts of George Mason University.

²⁶ (Benson, 1990 and 1998)

²⁷ (Oppenheimer, 1975)

not the “go get ‘em” aspect of holding criminals accountable for the crimes which they have committed?

The descriptions in this paper accuse the civil v. criminal distinction as being futile if not harmful to the successful operation of law and order in society. The civil v. criminal distinction is essentially a monopolization of ex-post justice provision by a centralized state. It is marked by the change from conflict existing between individual actors to conflict being claimed to exist between society and individual actors. Note the phraseology of criminal cases as they are always framed as such; “the people v. Mr. Smith,” or “the state of Illinois v. Mr. Smith.” What effect does this monopoly have on the way criminals act and innocent citizens re-act to avoid the losses of crime?

If foreseeing that after a crime takes place, investigation, arrest, trial, and incarceration of a criminal multiplied by the probability that these mechanisms occur successfully, still leaves a victim in the red, then his actions are obviously driven to avoid the mishap altogether. This driving force is manifested through the purchase of security and ex-ante justice mechanisms. The purchase of such ex-ante mechanisms has to be interpreted as an optimal allocation in the post-constitutional setting, even if car stereos continue to get stolen, but hope is not all lost. Once such technologies are installed driven by ex-post ineptitude, purchasers want to signal to would be thieves that they are secure and their probability of success is low so they’d be better to pass on by. In the eighties even people whose stereos had already been stolen would put signs in their windows pronouncing such, so as to avoid the costly burden of replacing a broken window. This changes the climate of activity for those who would be typically accused as free riding and thus contributing to the under provision of the Public Good security. By signaling the purchase of security devices, buyers increase the non-purchasers’ probability of being targeted for theft. On the margin more non-purchasers-of-old will change to present-purchasers, further changing the climate of remnant non-purchasers, so on and so forth. Under such conditions the problems of car-stereo theft all but disappear.²⁸

Can one expect to see the same elimination of the Public Goods problem to occur in the example of cyber crime? Coyne and Leeson elaborate on some current trends which seem to be helping to move the allocation of security from sub-optimal towards more-optimal states. “Theoretically positive externalities will be undersupplied on the market due to the free-rider problem stemming from non-excludability and pricing issues related to non-rivalry²⁹.” They present “Private Provision via Voluntary Donation,”³⁰ “The Private Provision of Internet Security via By-Product,”³¹ and the lack of applied property rights as a “Theory of Government Failure,”³² as avenues which may work together to diminish free rider problems moving secure conditions of cyber space closer to optimal

²⁸ The process of explaining the interaction between individual and his environment is a growing field known as emergent theorizing. It traces the changes in action resultant from environmental changes which are in turn resultant from actors’ choices. For more on this topic see (Schelling, 1978) and (Reznick, 1997)

²⁹ (Coyne and Leeson, “Whose to Protect,” forthcoming, 10)

³⁰ (Ibid, 14)

³¹ (Ibid, 20)

³² (Ibid, 24)

conditions. But the gains from trade within the cyber crime example stand as a mighty lure to drive the ingenuity of both thieves and defenders.

The development and expansion of the Internet has created innumerable new opportunities for access to information, personal interaction and entrepreneurial ventures. Not only have the costs of communication fallen considerably but perhaps even more importantly, the sphere of potential trading partners has expanded dramatically creating immense new gains from exchange.³³

While both scenarios lack market provisions in ex-post mechanisms of justice, the cybercrime example is different from the car stereo example because the gains from trade associated with the internet seem to be enormous. With reference to the formal model presented earlier the payoff of crime (C) is a direct function of the gains from trade associated with the internet. The more money there is to be made on the internet the more money there is to be made from crime on the internet. In other words reaping a billion dollars with a very small probability can be preferred to getting a penny with a decent probability of certainty.

Essentially this proportionality can drive criminal ingenuity so as to increase their probability of success by investing in their criminal talent. How can one be sure that his efforts at increasing security do not just raise the stakes of cyber crime to promote further technological advancement on the side of theft? It is almost as though he has entered an arms race which may never end.

Allow me to elaborate a pre-constitutional analysis which strengthens the laissez faire conclusion by offering advice on how to avoid such an arms race. If simultaneity in operational markets exists in the provision of ex-ante and ex-post justice mechanisms, then this arms race may be avoided. Individuals will be capable of purchasing bundles of ex-ante and ex-post mechanisms so as to accommodate their own preferences for risk and loss aversion. Some people may find it silly to spend extravagant amounts of wealth to have the world's greatest detective on call while having a state of the art lock on their door at the same time. Generally I would expect a sense of balance to exist between the purchasing of these two types of goods. This balance is often seen in the insurance market where premium discounts are awarded to policy holders who take addition ex-ante provisions to avoid being victimized. A purchase of each type of good in turn will be performed until the preference of the individual actor for security or peace of mind or pleasure in owning such goods is satiated.³⁴

First, a balance will exist between the subjective preferences of would be victims and their purchase of ex-post insurance or enforcement. Earlier it was mentioned that anytime such a victim is left in the red, after crime takes place a driving force is left to purchase security devices. The purchase of ex-ante and ex-post mechanisms will operate

³³ (ibid, 1 – 2)

³⁴ Such an operating force of satiation is referred to as the seeking of a plain state of rest see: (Mises, 1998, 245)

together so as to eliminate this in the red condition and leave the would-be-victim at lower and lower levels of loss if not complete indifference.

By indifference I make reference to the satisfaction of full restitution of loss after criminal loss is suffered by a residual claimant victim. This full satisfaction according to the subjective preferences of the victim would manifest itself by an optimal selection of insurance purchase in a present timely fashion before events happen. This would eliminate the aversion to victim experience being driven by current inept enforcement mechanisms so the only force left would be an inherent aversion to risk and victim aversion itself. Thus remnant purchases of security and insurance combinations would be theoretically optimal.

Allowing a competitive market process to function in ex-post arenas would mean allowing the free entrance of competitive ex-post criminal enforcement mechanisms, while simultaneously allowing free exit of individuals residing under current central provisions, and the depletion of, if not total elimination of such centralized provisions.

Under the current system of market incentives for ex-ante without ex-post no conception of optimality can be attributed to the levels of provision which individuals within the system choose. Benson (2003) questions the very notion of any central action being taken in the name of efficiency given questions of pre-constitutional legitimacy.

With this notion of ambiguous optimality exposed about our present system, the stylized facts of cyber crime seem obscure.

[I]n 2003, hacker-created computer viruses alone cost businesses \$55 billion – nearly double the damage they inflicted in 2002 (SecurityStats.com 2004). In a 2004 survey by the Computer Security Institute, over half of respondents indicated a computer security breach in the past 12 months and 100 percent of respondents indicated a Web site related incident over the same period (CSI 2004).³⁵

Returning to the original stage of the analytical outline (What is the problem in question?) seriously diminishes the magnitude of importance which was placed upon the question, by recognizing that such condensed effects are largely a result of the interplay between forces effecting the provision of ex-ante and ex-post justice mechanisms differently. This splits our analysis into two parts. The problem of cybercrime in the logistically present sense is that which the CIP papers adequately address, and the more abstract notion of cybercrime would be in general a problem which naturally emerges. The latter notion of the problem's magnitude is greatly diminished which in turn also diminishes the magnitude of the former in fact it changes the nature of the former entirely away from a problem associated with cybercrime per se and onto a problem of social interventionism. Some insight to answer the explicit question presented by Coyne and Lesson is even gained.

³⁵ (Leeson and Coyne, "Whose to Protect," forthcoming, 4)

One of our main aims in this paper is to provide a realistic understanding of how cyber security fits in with national security. It is our contention that in the context of cyberspace, individual security, as it relates to each and every user, and “national security” are inseparable.³⁶

One is left to wonder if given the free operation of markets in both of these arenas simultaneously, would cybercrime be a problem worthy of such great political attention? If conclusions lead towards the negative, then a stronger case is made for polycentric systems because they maintain a greater element of political sustainability than realized before.³⁷ Without such concentrated problems and attention paid to issues like cyber crime lower the tendency to shift towards centralized solutions as one is presented with fewer problems drawing centralized attention.³⁸

The offered broader context of ex-post justice satisfies a degree of uncertainty in regards to the stylized facts listed above. While they question the notions of optimality, efficiency, and characteristics as high or low, they do not fully explain where the given magnitudes are coming from. Next it will be proposed that a large proportion is being fueled by a result of the missing competitive application of markets to ex-post justice. Lacking such competition has eliminated notions of weeding out in regards to the creation of unsuccessful or infinite enforcement costs of criminal legislation. The most prominent example relevant to these stylized facts has to be the trend of criminality associated with intellectual property which will be elaborated in the next section of this paper.

5.2 Tangible Property v. Intellectual Property.

Each paper within the CIP series presents its own referenced material and statistics that are intended to express the degree of importance to which attention is and should be paid to the issue of cybercrime.

[I]n 2003, hacker-created computer viruses alone cost businesses \$55 billion – nearly double the damage they inflicted in 2002 (SecurityStats.com 2004). In a 2004 survey by the Computer Security Institute, over half of respondents indicated a computer security breach in the past 12 months and 100 percent of respondents indicated a Web site related incident over the same period (CSI 2004).³⁹

³⁶ (Ibid, 5)

³⁷ Ostrom (1961) defines polycentricism as such: “‘polycentric’ connotes many centers of decision-making which are formally independent of each other. Whether they actually function independently, or instead constitute an interdependent system of relations, is an empirical question in particular cases.” For more on polycentricism see: (Wagner, 2005).

³⁸ One could even make the case that the present paper attempts to contribute into the debate between monarchism and anarchism spawned predominantly by the claims of Nozick (1974) that anarchistic states devolve into states or that it is state operation itself which is spontaneous in addition to order.

³⁹ (Leeson and Coyne, “Whose to Protect,” forthcoming, 4)

In the previous sub-section I made the claim that such figures should be discounted in their abstract notion and in regards to their being representative of market failure seeing as how no such market provision is applied to ex-post justice mechanisms. This sub-section hopes to expose such figures as being entirely meaningless in their flawed reporting even in the immediately relevant logistical nature because of the ambiguous notions of what crime is within the cyber context.

Some of the individual papers within the CIP project honed their topic of attention to particular elements of activity within the broader heading of cyber crime. Morris and Korosec (forthcoming) focused primarily on fraud committed through credit card transactions that take place over the internet, while Stringham (forthcoming) addressed issues of fraud that develop from the international characteristics of internet trade, and Leeson and Coyne (“Hacking,” forthcoming) modeled the behavior of computer hackers. While the term cybercrime was continually used to refer to behaviors which shared similarities of internettedness, no clear and consistent definition for cybercrime was explicitly presented throughout the entire CIP project, nor was one apparently presented in any number of the sources used in performing the research for any of the pieces within the CIP project.

By reading the CIP papers and participating in its weekly workshop I have accepted the notion of cybercrime to refer to all of the following activities: hacking, making and sending viruses and worms, spamming, stealing software, sharing files under copyright, committing fraudulent sales over the internet, stalking and sexual harassment via the internet, and possibly many more technical behaviors which I am unaware of. The question that immediately comes to mind when trying to address this broad array of activities under the single umbrella of cybercrime is which of these is the oomph behind the statistics which are drawing our attention? In the remainder of this section I make the claim that the setting of monopolized ex-post justice provision has diminished the costs associated with producing prohibitive laws that otherwise would not have been produced under polycentric legal systems, these laws lack the certainty and quantifiable nature of emergent laws under competitive ex-post justice markets, therefore they possess an infinite magnitude in quantifiable loss terms and it is these notions of legality which are driving the numerical representations of cybercrime.

Return to the previous paragraph and run through the list of activities under the cybercrime umbrella. As a rule of thumb try to delineate which of these activities is associated with tangible property claims and which is not. The task is difficult indeed. But in today’s hi-tech environment the notion of intellectual property rights seems to drive a sharp wedge separating this bulk of activity into two distinct categories. That is not to say that cyberspace is the only arena of such a distinction, a motivated libertarian can do essentially the same task for traditional notions of crime, separating all such claims into either property violations or victimless prohibitive violations. In the cybercrime context this distinction can be traced by recognizing a difference between security and privacy. Security being a method of taking precautions against theft and loss while privacy taking similar precautions against the spread of knowledge to unintended individuals.

Kinsella (2001) has elaborated these characteristic elements of intellectual v. tangible property so as to make the natural law claim that intellectual property titles are illegitimate. For the purposes of this paper, a brief comparative approach is more helpful at showing the warped incentive structures promoted by the movement to secure intellectual property, though it is greatly inspired by insights revealed by Kinsella's natural law approach. Given the situation of a monopolized provision of ex-post enforcement mechanisms of justice the authority of governance has a lower opportunity cost of expanding its role as legislature. Basically it can afford to enforce laws that may not have otherwise been affordably enforced under non-monopolized conditions. Intellectual property claims is most likely such an example of an over expanded legislation, because of the un-tangible nature of loss associated with intellectual property rights violations. When tangible property is stolen or damaged, victims are self-motivated so as to report and seek damages through systems of justice. A competitive market of such services would maintain standards of reporting such losses and keep estimates of such losses reasonable in a social context and appropriate to market rates for similar or comparable repairs or replacements. But how do you quantify the value of knowledge? Surely it cannot be done. Alleged victims of intellectual property theft follow the same incentive system to report damages but they have no quantifiable measurement with which to express such losses.

The inclusion of this section is not meant to be a knock down case against the legitimacy of intellectual property claims as Kinsella's attempts to be. Whether he succeeds or not is not for debate here. I merely recognize that it raises interesting concerns to the notion of feasible enforcement in regards to cybercrime and incentives behind the trend of politicizing such a debate. By questioning the false oomph behind claims of intellectual property loss, theft or damage I hope to diminish the justification for placing cybercrime as an issue of social concern and cause for centralized action.

Conclusion

This paper has surveyed the CIP project paper series as a reputable source of material for providing free market solutions to problems deriving from conflict via the internet. This paper series hosted a bulk of material directly aimed at demonstrating how market forces were operating effectively at diminishing the negative effects of conflict over the internet. This paper recognizes such descriptions as accurate and illustrative of how markets effectively solve social problems, but recognizes that such explanations are still losing the battle of political viability in common discourse. To help against the latter front, this paper attempted to broaden the scope of analysis into the pre-constitutional realm. I made the case for applied markets in both ex-ante and ex-post provision of justice so as to eliminate the traditional problems associated with public goods, and explained how the inhibition of such simultaneity has lead to the promotion of legal policies that have no grounding in tangible quantifiable terms. By showing this, I hope to greatly diminish the degree to which cybercrime is claimed to be a problem in need of social action.

Returning to the first step of the analytical outline it can be seen that cybercrime is a much smaller concern than it has been made out to be by policy makers and the media.

All policy initiative takes place under an umbrella of statist enforcement and therefore has a level of unintended consequences. Solving cybercrime like solving many social problems is a matter of pre- and post-constitutional analysis. Which of the existing policies promote the incentives to commit such problematic actions, inhibit incentives for actors to self help against such problems, and call for a repeal of such policies? Only such repellent policy proposals are capable of having pre-constitutional influence so as to free up the notion of entrance into the market for governance in general. The specific applied research agenda of cybercrime held with it a unique characteristic of frontier like quality. Cyber technologies are cutting edge and new conceptions to users and governance alike. If markets can operate so as to promote law and order in a polycentric and purely voluntary setting within cyberspace, there is a greater case for applying such logic to more domesticated arenas of governance that lack its cutting edge quality. The way in which provision is made for the free emergence of societal order and structure in cyberspace, if done successfully, may serve as a model for societal structure of all new frontier aspects of technological-savvy civilization and even reconsiderations of our existing societal structures.

References:

Benson, Bruce. "The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement Without the State." *Journal of Law, Economics, and Policy*, Vol. 1, No. 2; forthcoming.

--*The Enterprise of Law: Justice without the State*. San Francisco: Pacific Research Institute for Public Policy, 1990.

-- *To Serve and Protect: Privatization and Community in Criminal Justice*. NY: NYU Press, 1998.

--"Do We Want the Production of Prisons to be More 'Efficient'?" found in: Tabarrok, Alexander (Editor). *Changing the Guard, Private Prisons and the Control of Crime*. Oakland: Independent Institute, 2003 pp 163-216.

Boettke, Peter. "James M. Buchanan and the Rebirth of Political Economy," in Holt and Pressman, ed., *Economics and its Discontents* (Edward Elgar, 1998): 21-39.

--unpublished. "Anarchism as a Progressive Research Program in Political Economy," *George Mason University Economics Department Working Papers*: http://www.gmu.edu/departments/economics/wp_author.html.

Caplan, Bryan and Ed Stringham 2003. "Networks, Law, and the Paradox of Cooperation." *Review of Austrian Economics* 16(4), pp. 309-26.

Computer Security Institute and Federal Bureau of Investigations. 2004. *CSI/FBI Computer Crime and Security Survey*. Available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

Cowen, Tyler. 1992. "Law as a Public Good: The Economics of Anarchy." *Economics and Philosophy* 8:249-67.

Coyne, Christopher J. and Peter T. Leeson. "Who's to Protect Cyberspace?" *Journal of Law, Economics, and Policy*, Vol. 1, No. 2; forthcoming.

Critical Infrastructure Protection Program, 2005. *Mission and Vision*, September 28, 2005. Available at: <http://cipp.gmu.edu/mission/>.

-- *Seminar on the Law, Economics and Technology of Private Enforcement of Contract on the Internet*, September 28, 2005. Available at: <http://www.gmu.edu/departments/economics/pboettke/cip.html>.

Friedman, David D. "From Imperial China to Cyberspace: Contracting Without the State." *Journal of Law, Economics, and Policy*, Vol. 1, No. 2; forthcoming.

- The Machinery of Freedom: Guide to a Radical Capitalism*. La Salle: Open Court, 1989.
- Hayek, F.A. "The Use of Knowledge in Society." *American Economic Review*, XXXV, No. 4; September, 1945, pp. 519-30.
- Morris, Andrew and Jason Korosec. "Private Dispute Resolution in the Card Context: Structure, Reputation, and Incentives." *Journal of Law, Economics, and Policy*, forthcoming.
- Kinsella, Stephan. 2001. "Against Intellectual Property." *Journal of Libertarian Studies*, Vol. 15, No. 2: 2001.
- Leeson, Peter T. and Christopher J. Coyne. "The Economics of Computer Hacking." *Journal of Law, Economics, and Policy*, Vol. 1, No. 2; forthcoming.
- Mises, Ludwig Von. *Human Action: The Scholars Edition*. Auburn: Ludwig von Mises Institute, 1998 pp 245-251.
- Nozick, Robert. *Anarchy, State and Utopia*. New York: Basic Books, 1974.
- Openheimer, Franz. *The State*. New York: Free Life Editions, 1975.
- Ostrom, Vincent. 1961. "The Organization of Government in Metropolitan Areas: A Theoretical Inquiry." *The American Political Science Review*, Vol. 55, No. 4. pp. 831-842.
- Powell, Ben. "Is Cybersecurity a Public Good?" *Journal of Law, Economics, and Policy*, Vol. 1, No. 2; forthcoming.
- Resnick, Michael. *Termites, Turtles and Traffic Jams: Explorations in Massively Parallel Microworlds*. Cambridge: MIT Press, 1997.
- Rothbard, Murray N. 1982. *The Ethics of Liberty*, Humanities Press, Atlantic Highlands, N.J.
- For a New Liberty, The Libertarian Manifesto*. New York: Macmillan, 1985.
- Schelling, Thomas C. *Micromotives and Macrobehavior*. New York: W. W. Norton and Company, 1978.
- SecurityStats.com. 2004. *Virus Statistics*, January 16, 2004. Available at: <http://www.securitystats.com>

Stringham, Edward. "The Capability of Government in Providing Protection Against Online Fraud." *Journal of Law, Economics, and Policy*, Vol. 1, No. 2; forthcoming.

Tannehill, Linda and Morris. *A Market for Liberty*. Lansing: Morris and Linda Tannehill, 1970.

Wagner, Richard. "Self-Governance, Polycentricism and Federalism," *Journal of Economic Behavior and Organization*, 57 (2) 2005: 173-188.