VIRTUAL CRIME, VIRTUAL DETERRENCE: A SKEPTICAL VIEW OF SELF-HELP, ARCHITECTURE, AND CIVIL LIABILITY

Orin S. Kerr[*]

Recent scholarship in the field of computer crime law reflects a surprising trend: much of it does not concern criminal law or the criminal justice system. According to many scholars, the problem of computer crime can be best addressed by looking beyond criminal law. Cybercrime demands a new model of law enforcement, the thinking goes; the traditional mechanisms of criminal investigation and prosecution cannot deter computer-related crime effectively.[1] The law must turn to alternative approaches that regulate social norms, code, and civil liability to alter incentives *ex ante* without recourse to the criminal justice system.[2]

This essay critiques three of the most prominent proposals to deter computer crime outside of criminal law. The first proposal, self-help, would allow victims of hacking and denial-of-service attacks to defend

[*] Associate Professor, George Washington University Law School. Thanks to Dan Hunter, Neal Katyal, Doug Lichtman, Dan Markel, Michael O'Neill, and Daniel Solove for their comments on an earlier draft. This essay was prepared for a symposium "Property Rights on the Frontier: The Economics of Self-Defense and Self-Help in Cyberspace" hosted by the *Journal of Law, Economics and Policy.* Thanks to Noah Falk for excellent research assistance, and to the editors of the *Journal of Law, Economics and Policy* for their gracious invitation to speak at the *Journal*'s first symposium.

[1] *See, e.g.,* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier,* 11 S. CAL. INTERDISC. L. J. 63 (2001) (arguing that "criminal law is an inadequate institution of social control against cybercrime," and that there is a "greater role for private 'cybercops' to punish and control cybercrime to close the enforcement gap"); Stevan D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response,* 11 HARV. J. LAW & TECH. 699, 706-708 & fn. 14, 15 (1998) (discussing the need for public private partnerships in the deterrence of computer crimes); Susan W. Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security,* 10 B.U.J. SCI. & TECH. L. 1 (2004) (arguing that cybercrime demands a new model of law enforcement); Nimrod Kozlovski, *Designing Accountable Online Policing, available at* http://islandia.law.yale.edu/isp/digital%20cops/papers/kozlovski_paper.pdf ("The online crime scene introduces complex challenges to law enforcement that inevitably lead to the emergence of a new policing model . . . derive[d] from employing alternative strategies of law enforcement."); AMITAI AVIRAM, *Network Responses to Network Threats: The Evolution Into Private Cyber-Security Associations,* in THE LAW & ECONOMICS OF CYBER-SECURITY (Cambridge University Press; forthcoming 2005); Brent Wible, Note, *A Site Where Hackers Are Welcome: Using Hack-in Contests to Shape Preferences and Deter Computer Crime,* 112 YALE L.J. 1577, 1577 (2003) ("With the failure of traditional law enforcement methods to deal with [the threat of computer crime], computer crime requires a new approach to thinking about deterrence."). *See also infra* notes 3-5.

[2] *See infra* notes 3-5.

themselves by counterattacking and disabling intruders.[3] The concept animating offensive self-help or "hack back" proposals is that private parties may be able to deter and prevent computer crimes through private action more effectively and efficiently than through government action. The second proposal, architecture regulation, was offered recently in an essay by Professor Neal Katyal.[4] Professor Katyal contends that computer crime can be deterred by redesigning the architecture of cyberspace in ways that mirror how architects design physical spaces to deter traditional crime. The third proposal, civil liability, seeks to impose liability on third-party intermediaries such as ISPs for the cost of criminal activity.[5] Although many variations of this proposal exist, my specific interest is on the use of civil liability to encourage ISPs to monitor and deter crime attempted by their subscribers.

This essay offers a skeptical view of the three proposals. I agree that responses to computer crime must look at least in part beyond criminal law. Criminal law addresses only a small piece of the broader puzzle of how to deter misconduct, and that is just as true online as it is offline.[6] At the same

[3] *See* Michael E. O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237 (2000); Curtis E. A. Karnow, *Launch on Warning - Aggressive Defense of Computer Systems*, *available at* http://islandia.law.yale.edu/isp/digital%20cops/papers/karnow_newcops.pdf; Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171 (2000); Bruce Smith, *Hacking, Poaching, and Counterattacking*, 1 J.L. ECON. & POL'Y (forthcoming 2005). *Cf.* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207 (2002) (discussing self-help measures under the rules of war).

[4] Neal Kumar Katyal, Essay, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261 (2003).

[5] *See, e.g.*, Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, SUP. CT. ECON. REV. (forthcoming 2005); Assaf Hamdani, *Who is Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002); Stephen E. Henderson & Matthew E. Yarborough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N. M.L. REV. 11 (2002); Rustad, *supra* note 1; Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1009 (2001); Calkins, *supra* note 3, at 219-224; Robin A. Brooks, Note, *Deterring the Spread of Viruses Online: Can Tort Law Tighten the 'Net'?*, 17 REV. LITIG. 343 (1998); David L. Gripman, Comment, *The Doors Are Locked but the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMP. & INFO. L. 167 (1997); Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213 (1995); Susan C. Lyman, *Civil Remedies for the Victims of Computer Viruses*, 21 SW. U.L. REV. 1169, 1172 (1992); Cheryl S. Massingale & A. Faye Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. NEW ENG. L. REV. 167, 185 (1990); Anne Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 30-37 (1990); Agranoff, *Curb on Technology: Liability for Failure to Protect Computerized Data Against Unauthorized Access*, 5 SANTA CLARA COMPUTER & HIGH TECH. L.J. 263, 268 (1989).

[6] In the case of traditional crimes, no one would think to argue that criminal law should be the *only* mechanism to prevent crime. No one keeps their doors unlocked at night in the hope that burglars will break in, get caught, and then be prosecuted so as to deter future burglary attempts. Instead, we lock our doors. Conversely, few would argue seriously that there should be no criminal punishment at

time, the three proposals reflect in varying degrees a common conceptual mistake: over reliance on the metaphor of the Internet as a virtual "place." The proposals tend to envision the Internet as a virtual world of cyberspace with virtual streets and virtual management, and use this virtual model to generate assumptions about what kind of legal rules and practices are likely to generate particular results. These assumptions are valid in some circumstances, but they are not valid in many others. As a result, heavy reliance on virtual metaphors risks incorporating assumptions from the physical world that break down when applied to the Internet. When this occurs, virtual metaphors will obscure rather than illuminate the dynamics of computer crime.

This essay argues that responding to computer crime requires confronting the physical reality of what the Internet is and how it works. Both virtual and physical perspectives of the Internet can offer important lessons, but any strategy to deter computer crime must look viable given the physical reality of the network. Strategies that rely too heavily on the virtual metaphors of cyberspace are likely to rely on assumptions drawn from the physical world that do not apply to the Internet; the process of importing concepts from physical space to the virtual world of cyberspace will introduce errors. Over reliance on virtual metaphors will often misrepresent how online crime occurs and thus how it can be deterred. Where virtual metaphors govern, proposals to deter computer crime through civil liability and social norms will prove less effective in practice than they may first appear in theory.

I begin my argument by exploring the tension within Internet law between modeling the Internet using virtual reality and physical reality, with a special emphasis on what this tension means for developing arguments about deterrence and computer crime. The analysis explains that a physical description of the Internet differs dramatically from a virtual description of Internet applications, and argues that any effective model for deterring computer crime must be rooted in the former rather than the latter. In the remaining parts of the paper, I apply this insight to critique the three proposals. I begin with offensive self-help, focusing on Michael O'Neill's article *Old Crime in New Bottles: Sanctioning Cybercrime*; turn next to architecture regulation, focusing on Neal Katyal's essay *Digital Architecture as Crime Control*; and conclude by studying proposals that would impose civil liability on third-party computer operators. In each case, I identify how over reliance on virtual metaphors can frustrate efforts to deter computer crime.

all for burglary. We recognize that the criminal justice system offers a marginal deterrent value against burglary and serves important retributive ends as well. The basic regulatory strategy is to combine criminal law with other mechanisms to best deter crime while minimizing other social costs. I submit that this basic approach will likely prove the most effective strategy to deter and punish computer crime, as well.

I. PHYSICAL AND VIRTUAL APPROACHES TO DETERRING COMPUTER CRIME

There are two basic ways to model the Internet: from the perspective of physical reality and the perspective of virtual reality.[7] From a virtual perspective, the Internet can be understood as the home of a virtual world of cyberspace that is roughly analogous to the physical world. A user can utilize his keyboard and mouse to go shopping, participate in online communities, and do anything else that he finds online much like he could in the physical world. The Internet is cyberspace, a virtual world with virtual streets and virtual stores, virtual perils and virtual promise that echo the physical world.[8] The physical perspective of the Internet is very different. From a physical perspective, "the Internet" is a name attached to the sprawling and decentralized international network of networks including millions of computer servers and hundreds of millions of miles of cables. The hardware sends, stores, and receives trillions of digits of data every day using a series of common protocols. Many of the computers connected to this network of networks are located outside the United States, along with the majority of its users. Keyboards provide sources of input to the network, and monitors provide destinations for output. From the standpoint of physical reality, the virtual world of cyberspace is just a convenient metaphor. Internet users may decide to use that metaphor to more easily understand particular software applications available via the Internet. But what matters is the physical reality of the network, the actual bits and bytes, rather than the virtual world a user might imagine.

Understanding the distinction between physical and virtual descriptions of the Internet is critical to understand how law can help deter computer crime. The distinction between physical and virtual leads to two basic approaches to deterring cybercrime. From a virtual perspective, the natural starting point for regulating cyberspace is to translate the ways that the law regulates the physical world. If a problem from the physical world carries over into cyberspace, the solution from physical space should be harnessed, modified as necessary, and then applied to cyberspace. In the specific context of computer crime, the virtual perspective suggests that legislatures should study crime prevention strategies that have worked in physical space, and apply a virtual version of that solution to cyberspace. In a sense, computer crime is nothing new: it's just a cyberspace version of old-fashioned physical crime. The switch from physical to virtual may create

[7] *See generally* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91, GEO. L.J. 357 (2003).

[8] *Cf.* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 524 (2003) ("Even if we understand somewhere in the back of our minds that we are not really going anywhere, perhaps when we access the Internet it seems so much like we are in a different physical space that we accept cyberspace as a "real" or physical place.").

some new wrinkles, but the basic problem can draw from solutions already applied in the physical world.

From a physical perspective, computer crime is a different problem and calls for different solutions than you might see from a virtual perspective. The physical perspective teaches that online crimes involve users sending and receiving data in ways that the law seeks to prohibit. Perhaps the data is contraband, such as an image of child pornography. Perhaps the law prohibits the transmission or use of data because particular data is private and belongs to some one else, such as private files exposed by a hacker. Perhaps the data is copyrighted and cannot be distributed without permission. Or perhaps the transmission of data blocks others from being able to access their computers, such as might occur with a denial of service attack. In all of these cases, computer crime law attempts to regulate the transmission of data to avoid identified social harms. To deter computer crime, solutions either must block the transmission by code-based restrictions or else persuade users not to act in ways the law recognizes as harmful.

The distinction between physical and virtual is critical because solutions that appear promising from a virtual perspective might not appear promising from a physical perspective, and vice versa. Consider the example of "broken windows" policing.[9] In the physical world, individuals considering whether to engage in criminal activity often take clues from their physical environment.[10] Visible disorder can undermine law-abiding norms.[11] Tolerance of low-level criminal activity in a neighborhood can signal tolerance of higher-level activity, and may lead to more serious crime. "Broken windows" policing attempts to reverse that process. The visible enforcement of low-level activity signals to wrongdoers that higher level activity will not be tolerated; the hope is that perception of obedience to the law based on observable enforcement of the law helps generate norms of obedience and discourages crime.[12]

Does broken windows policing teach us anything useful about deterring computer crime? From the virtual perspective, the answer might appear to be "yes." Enforcement policies might place a priority on fixing broken "cyber windows," if you will, encouraging the visible enforcement of the law in one region of cyberspace to help generate norms of obedience to law in that region. Visible signs that the law is enforced in one cy-

[9] *See generally* GEORGE L. KELLING & CATHERINE M. COLES, FIXING BROKEN WINDOWS: RESTORING ORDER AND REDUCING CRIME IN OUR COMMUNITIES (1996).

[10] *See generally* Robert J. Sampson & Jacqueline Cohen, *Deterrent Effects of the Police on Crime: A Replication and Theoretical Extension*, 22 LAW & SOC'Y REV. 163 (1988).

[11] Dan M. Kahan, *A Colloquium on Community Policing: Reciprocity, Collective Action, and Community Policing*, 90 CAL. L. REV. 1513, 1527-30 (2002).

[12] *See id. But see* BERNARD E. HARCOURT, ILLUSION OF ORDER: THE FALSE PROMISE OF BROKEN WINDOWS POLICING (2001).

berneighborhood might send signals to cybercriminals that they should look elsewhere. From a virtual perspective, it seems plausible to look for ways to signal to potential cybercriminals that the cyber-community will not tolerate criminal activity in a particular corner of cyberspace.[13]

From a physical perspective, however, the answer appears to be "no." The notion of fixing windows in cyberspace makes little sense. Cyberspace is just a metaphor, not an actual place. Applying real-space approaches to "cyberspace" works only if the way that the approach applies to physical space happens to be replicated within the metaphorical understanding of cyberspace. This does not seem to occur in the case of broken windows policing. In the physical world, broken windows policing may work because there is an observable correlation between the visual appearance of a place and whether crime will be tolerated there. Visual appearance communicates information about law enforcement practices, and a potential wrongdoer can factor that into his decision whether to commit an offense.

The same linkage does not apply online. The visual appearance of a "site" on the Internet is merely a string of zeros and ones that the computer has been programmed to send to the user for reassembly and display. The string of zeros and ones does not reflect the social practices, priorities, or condition of the computer or its users. Whether the police pay attention to low-level criminal activity generally will not change the visual appearance of anything. Even if it did, the appearance of a site is known by wrongdoers to be merely a graphic overlay, not a signal of social norms or law enforcement practices. The homepage of a webserver looks the same regardless of whether the server is secure or is riddled with holes. Online intruders get a sense of the security practices used at a potential victim computer not by viewing the homepage of its webserver, but by remotely scanning the computer to determine its software, open ports, and vulnerabilities.[14] The dynamic underlying "broken windows" policing does not seem to apply to crimes involving the transmission of data from computer to computer. As a result, the strategy has little relevance in the context of computer crimes.

This example points to broader lesson about the role of physical and virtual perspectives in the formulation of cybercrime deterrence strategies. While both virtual and physical perspectives of the Internet can offer important lessons, any strategy to deter computer crime must look viable from a physical perspective. Strategies that rely too heavily on the virtual perspective of the Internet are likely to rely on assumptions drawn from the physical world that do not apply to the Internet. The process of importing

[13] *See* Katyal, *supra* note 5, at 1110 (suggesting that an application of the complementarity of crime underlying broken windows policing should lead to the swift and harsh punishment of computer virus authors to avoid copycat crimes).

[14] *See* Ofir Arkin, *Network Scanning Techniques: Understanding How It Is Done, available at* http://www.totse.com/en/hack/introduction_to_hacking/162026.html.

concepts from physical space to the virtual world of cyberspace risks importing too much. It threatens to let virtual metaphors get the best of us, and may point us in directions that do not actually work given the physical reality of the Internet. To ensure effective deterrence, care must be taken to make sure that no unwarranted assumptions are embedded in those strategies when they are transferred to the Internet.

This does not mean that metaphors are never useful, of course.[15] Metaphors harness existing similarities. When a new problem is similar in a relevant way to an old one, metaphors can illuminate how solutions from the old problem might apply to the new. The difficulty arises when one set of similarities generates a metaphor, and the metaphor is then used in other contexts where no relevant similarities exist. Consider e-mail and traditional postal letters. As a communications mechanism, e-mail is akin to traditional postal mail: e-mail is used to send and receive messages much like postal mail. When evaluating legal rules to regulate postal mail as a communications mechanism, it makes sense to invoke the virtual metaphor and begin by considering the legal rules used to regulate postal mail.

But this doesn't mean that snail mail and e-mail always should be treated alike. The fact that they are similar in some ways does not mean that they are identical in every way. For example, the existence of the United States Postal Service to deliver physical letters does not mean a centralized virtual Postal Service is needed to deliver e-mail. The fact that stamps are required to send postal mail doesn't mean stamps are needed to send e-mail. While postal letters and e-mail are alike in some ways, their delivery mechanisms are quite different. We cannot simply declare e-mail the virtual equivalent of physical mail and assume that every legal regulation of the latter should apply to the former. A more nuanced approach is required that looks carefully at the specific ways in which virtual and physical are similar and different.

The remainder of this essay will apply this critique to three sets of proposals that would attempt to deter computer crime outside of criminal law. I will begin with offensive self-help strategies, turn next to architecture regulation, and finish with civil liability for third-party computer operators. In each case, I argue that over reliance on the cyberspace metaphor weakens the analytical framework of the proposals. Excessive use of virtual metaphors creates unwarranted assumptions, and unwarranted assumptions leads to misunderstandings of how the law can deter computer crime.

[15] *See generally* Kerr, *supra* note 7, at 389-405 (offering a normative framework for when law should adopt a virtual versus a physical perspective of computers and the Internet).

II. OFFENSIVE SELF-HELP

Should the law permit victims of computer hacking attacks to counterattack and disable intruders? A number of scholars have suggested that the answer is yes.[16] Professor Michael O'Neill has developed the most prominent proposal.[17] According to Professor O'Neill, traditional mechanisms of criminal investigation and prosecution do not sufficiently deter crime involving the Internet: there are too few cybercops, cybercriminals are too hard to catch, and jurisdictional hurdles often get in the way.[18] As an alternative, O'Neill proposes a regime of offensive self-help, or cyber-vigilantism. Allow victims of computer crimes to hack-back against those that hacked them. The threat of being hacked back will deter the initial round of hacking, O'Neill contends: potential attackers will know that an attack may lead to them being made the next victims, resulting in deterrence akin to a cyber-version of mutual assured destruction.

Professor O'Neill relies explicitly on virtual metaphors to explain and justify his proposal. He writes: "[J]ust as settlers in the American West could not reliably count on the local sheriff to protect them, and instead kept a weapon handy to stymie potential aggressors, Internet users may need to protect themselves."[19] "[C]yberspace is our new frontier,"[20] he adds, and private companies have the virtual firepower to keep "virtual streets"[21] safe. "Just as a homeowner may defend his house, . . . computer companies ought to not only be permitted, but encouraged, to unleash their considerable talents to launch countermeasures against cyber-criminals."[22] O'Neill appears to envision the Internet as a virtual Wild West, with cyber-settlers carrying virtual guns and mounting cyberdefenses against virtual bandits. Just as packing a weapon in the Wild West might deter wrongdoers, so can the threat of a cyberattack deter wrongdoers in cyberspace.

The image is a memorable one, but note the assumption embedded in the virtual metaphor. Use of the virtual metaphor presumes that victims of an attack can find out easily who is attacking them. This was often true in the Wild West, or at least in movies about the Wild West. If Bad Guy wants to attack Good Guy with a six-shooter, he needs to be close enough to see him and have a good chance of hitting him. At that very short dis-

[16] *See supra* note 3. There is a great deal of commentary on a related question of whether the law should allow similar self-help measures by copyright owners to disable computer-facilitated copyright infringement. For the sake of simplicity, however, I will limit my discussion to self-help designed to prevent and deter unauthorized access to computers.

[17] *See* O'Neill, *supra* note 3.

[18] *See id.* at 275-77.

[19] *Id.* at 277.

[20] *Id.* at 279.

[21] *Id.*

[22] *Id.* at 280.

tance, Good Guy can see Bad Guy, too. If Good Guy has the same gun that Bad Guy has and there is no element of surprise, Good Guy and Bad Guy are on equal footing. My sense is that Professor O'Neill's proposal presupposes such a dynamic. Let's assume that Bad Guy is a rational actor. He will decide to kill Bad Guy if the benefit from attacking good guy exceeds the harm to himself. To throw in some unnecessary math, we can say that Bad Guy will attack when

> (Chance initial attack will succeed) * (Benefit to Bad Guy if initial attack succeeds) > (Chance Good guy will attempt a counterattack) * (chance counterattack will succeed) * (harm to Bad Guy if counterattack succeeds)

My sense is that O'Neill assumes that the chance that the counter attack will succeed is on par with the chance that the initial attack will succeed. The deterrence dynamic O'Neill seeks to harness is based on a type of ricochet effect; the likelihood that an attack will lead to a successful counterattack deters the initial attack.

Applying this regime to the Internet creates a significant problem, however. It is very easy to disguise the source of an Internet attack. Internet packets do not indicate their original source. Rather, they indicate the source of their most immediate hop. Imagine I have an account from computer *A*, and that I want to attack computer *D*. I will direct my attack from computer *A* to computer *B*, from *B* to computer *C*, and from *C* to computer *D*. The victim at computer *D* will have no idea that the attack is originating at *A*. He will see an attack coming from computer *C*. Further, the use of a proxy server or anonymizer can easily disguise the actual source of attack. These services route traffic for other computers, and make it appear to a downstream victim as if the attack were coming from a different source.

As a result, the chance that a victim of a cyber attack can quickly and accurately identify where the attack originates is quite small. By corollary, the chance that an initial attacker would be identified by his victim and could be attacked back successfully is also quite small. Further, if the law actually encouraged victims of computer crime to attack back at their attackers, it would create an obvious incentive for attackers to be extra careful to disguise their location or use someone else's computer to launch the attack. In this environment, rules encouraging offensive self-help will not deter online attacks. A reasonably knowledgeable cracker can be confident that he can attack all day with little chance of being hit back. The assumption that an attacker can be identified and targeted may have been true in the Wild West, but tends not to be true for an Internet attack.

Legalizing self-help would also encourage foul play designed to harness the new privileges. One possibility is the bankshot attack: If I want a computer to be attacked, I can route attacks through that one computer towards a series of victims, and then wait for the victims to attack back at that computer because they believe the computer is the source of the attack. By harnessing the ability to disguise the origin of attack, a wrongdoer can get one innocent party to attack another. Indeed, any wrongdoer can act as a catalyst to a chain reaction of hacking back and forth among innocent parties. Imagine that I don't like two businesses, *A* and *B*. I can launch a denial-of-service attack at the computers of *A* disguised to look like it originates from the computers at *B*. The incentives of self-help will do the rest. *A* will defend itself by launching a counterattack at *B*'s computers. *B*, thinking it is under attack from *A*, will then launch an attack back at *A*. *A* will respond back at *B*; *B* back at *A*; and so on. As these examples suggest, basing a self-help strategy on the virtual model of the Wild West does not reflect a realistic picture of the Internet. Self-help in cyberspace would almost certainly lead to more computer misuse, not less.

To be fair, it is possible to generate a self-help proposal that does not rely on virtual metaphors. A proponent of the idea could restate it using physical rather than virtual descriptions of the Internet. In my experience, however, the persuasiveness of the self-help argument draws heavily on the virtual metaphor. The model of an online counterattack as a "virtual punch" or "virtual bullet" situates the proposal in a familiar physical setting, and supports the necessary but false assumption that an online victim can successfully disable his attacker much like a physical victim can disable a physical attacker. The virtual model incorporates assumptions that hold in the physical world but tends to hide the very different dynamics at work in the case of Internet attacks.

III. ARCHITECTURE REGULATION

Over reliance on virtual metaphors also blunts the effectiveness of architectural approaches to computer crime. In an interesting essay entitled *Digital Architecture as Crime Control,* Professor Neal Katyal contends that one answer to the problem of computer crime is to apply realspace notions of architecture regulation to cyberspace.[23] Katyal reasons that the "metaphorical synergy" between physical space and cyberspace justifies "a new generation of work" in which scholars apply "the lessons of realspace study . . . to the cybernetic realm."[24] Professor Katyal notes that in the physical world, architects can help deter crime by designing open and well-lit spaces,[25] by fostering notions of terroritoriality that signal stewardship of property,[26] and by fostering a sense of community.[27] Katyal proposes "reverse-engineering the realspace analysis of architecture . . . to cyber-

[23] Katyal, *supra* note 4.

[24] *Id.* at 2261.

[25] *Id.* at 2264-67.

[26] *See id.* at 2268-72.

[27] *See id.* at 2272-79.

space"[28] to "help develop the types of digital bricks and mortar that can both reduce crime and build community" online.[29] If architecture regulation helps prevent crime in physical space, Katyal suggests, it also can help prevent crime in cyberspace.

Katyal relies heavily on virtual metaphors to frame his proposals. He suggests that the very idea of distinguishing between real space and cyberspace has a limited future: "the divide between realspace and cyberspace [is] erod[ing],"[30] Katyal contends. "With wireless networking, omnipresent cameras, and ubiquitous access to data, these two realms are heading toward merger."[31] According to Professor Katyal, architectural concepts "offer a vantage point from which to view this coming collision"[32] between real space and cyberspace.

But does the architectural approach shed light on deterring computer crime? An important difficulty lurks within Katyal's approach. Architecture can deter crime in physical space because architecture defines the properties of the space. Physical space follows immutable rules of physics; by changing the space, architects can change the likelihood that an attempted criminal act in that space will succeed and communicate that to potential perpetrators of criminal activity *ex ante*. Cyberspace is only a metaphor, however. It offers a way to understand the experience of using some Internet applications, but does not create an environment with a universal set of rules that govern all interactions with particular people or things. Any perception of "cyberspace" generally rests on a superficial visual facade over the real network, and a typical cybercriminal will be focused on the real network rather than the facade.

The fact that cyberspace is only a metaphor makes it difficult for architectural insights to advance the debate over strategies to deter computer crime. Users' impressions of the virtual metaphor play little to no role in their decisions to engage in misconduct. In all but a few cases, a potential perpetrator of a computer crime does not enter a "space" that signals the likelihood that a crime would be detected, or that a crime would succeed.[33] Cybercriminals tend to focus on the physical perspective, not virtual ones. They want to hack the network to get the machine to send and receive the information they want. Their focus is code, not the visual overlay. As a result, efforts to deter crime by influencing users' perceptions of the properties of cyberspace will tend to have little effect on computer crime.

I think we can see these difficulties in Professor Katyal's attempt to explain why architectural insights should trigger a new generation of think-

[28] *Id.* at 2288.

[29] Katyal, *supra* note 4, at 2289.

[30] *Id.* at 2262.

[31] *Id.*

[32] *Id.*

[33] Internet chat rooms are one obvious exception.

ing about cybercrime deterrence. Although Katyal's proposals are described as architectural, most have only a tenuous connection to architectural concepts. The inherent difficulty of architecting a metaphor encourages attention to be focused elsewhere. Consider the case of "natural surveillance" design principles. In the physical world, architects can design spaces to be well-lit and open; this raises the chances of detection, raises the cost of crime, and therefore helps deter that crime. Katyal's attempt to apply this to cyberspace leads him to conclude that open source software is preferable to closed source software.[34] More people can see the code underlying open source programs, Katyal notes; the code is "open." According to Katyal, the principles of natural surveillance teach that greater exposure facilitates greater attention, and greater attention to code among computer security experts can lead to the identification and correction of security defects.[35] As a result, open source software should lead to more secure code than closed source software.

While it may be right that open source software tends to have fewer defects than closed source software – the technical community generally believes this, and I have no reason to disagree – this insight is not related to natural surveillance. Natural surveillance can be used to deter crime by fostering a sense among potential offenders that an attempted crime is unlikely to succeed; a space is "open" in the sense that it any conduct can be observed by other people who can report the crime. Natural surveillance increases the chance of detection, raising the cost of crime to the wrongdoer. Debates about open source software concern a different question. In those debates, the issue is how to create incentives for software designers to identify and correct security vulnerabilities. The goal is not to dissuade attempted wrongdoing based on fear of detection, but to make code impervious to attack when wrongdoing occurs. Software is "open" not in the sense of being visible to wrongdoers, but in the sense that programmers can obtain copies to review for defects. Despite the superficial connection between the two, natural surveillance principles do not appear to relate to or shed light on the open source debate.

A similar difficulty exists with Katyal's views of how notions of territoriality should impact Internet design. Katyal explains that real space architects can design space to foster a sense of territoriality and responsibility for enclosed and private regions. The use of archways and open gates can create a sense of ownership and private property that can encourage others to stay away.[36] By controlling how people perceive whether there are welcome in particular spaces, architecture can help determine the likelihood that crime will occur there. Katyal contends that cyberspace architects can apply this principle to the Internet by designing systems that facilitate

[34] *See id.* at 2264-65.

[35] *See id.*

[36] *See* Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039, 1058-59 (2002).

traceability. He focuses on the strengths and limitations of different privacy rules and practices, ranging from logging IP addresses to allowing content owners to subpoena ISPs for subscriber information.

Whatever the merits of these different rules and practices, however, the connection between them and realspace notions of territoriality is indirect at best. Territoriality rests on the perception that a space is someone's property; traceability rests on the idea that it should be possible to connect an individual's conduct to their person. The former deals with shaping attitudes about ownership and property rights *ex ante*; the latter concerns investigating crime *ex post*. To be fair, the two share a common theme of responsibility. In addition, traceability *ex post* can create disincentives to commit crime *ex ante*. At the same time, the fact that territoriality can be used in realspace design does not appear to shed light on the complex tradeoffs among different privacy rules and practices.[37] The connection is too indirect for the former to generate useful insights about the latter.

Finally, Katyal's proposals on community building appear to suffer from the same difficulty. In physical space, architects can design space to facilitate easy interaction and encourage a sense of community and common identity. They can put houses close together, and use public parks as common meeting places. According to Katyal, applying this insight to the Internet suggests that we should embrace (within limits) the end-to-end principle of network design.[38] The end-to-end argument is that the brains of a network operation should be at the ends of the network, rather than the middle; the network should be open to all types of different traffic and let the applications at the end point figure out what to do with them.

Lawrence Lessig and Mark Lemley have argued powerfully that end-to-end design is an important part of the Internet's architecture, and that facilitating future innovation depends on it.[39] They explain that end-to-end design ensures that the network remains open to technological change because the network does not discriminate among old and new types of communications. Katyal contends that the interest in community building also

[37] This is not to say that territoriality is irrelevant. Code-based restrictions can create a sense of territoriality, and I have argued elsewhere that such restrictions should be used to draw the line between legality and illegality in the case of unauthorized access statutes. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

[38] The end-to-end principle has been latent in the design of the Internet since its inception but was first explored systematically by Jerome Saltzer, David Reed, and David Clark in 1981. *See* Jerome H. Saltzer, David P. Reed, and David D. Clark, *End-to-End Arguments in System Design*, Second International Conference on Distributed Computing Systems (April 8-10, 1981) pages 509-512.

[39] *See* Mark A. Lemley & Lawrence Lessig, *The End Of End-To-End: Preserving The Architecture Of The Internet In The Broadband Era*, 48 U.C.L.A. L. REV. 925, 930-33 (2001). *See also* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 120-22 (1st ed. 2001).

supports end-to-end design.[40] An architect of the Internet would want easy interaction and reciprocity among computers much like a traditional architect would value easy interaction and reciprocity among people in physical space.[41] Because end-to-end facilitates interoperability among programs, the architectural insights of community building suggest the need for end-to-end design.[42]

The difficulty with this analogy is that computers are not people, and the comparison rests on attributes that humans have but Internet applications don't. Reciprocity and interaction can deter crime in physical space because community building creates a notion of shared responsibility. Shared responsibility fosters a willingness to look out for and respond to criminal activity. Reciprocity and interaction among computers generally is a good thing, but it is not clear how it relates to deterrence. Computers do not feel responsibility; they only look out for crime if they are programmed to do so. If there is a connection between end-to-end design and deterring computer crime, it is left unexplained.

To be clear, I share many of Professor Katyal's instincts on the merits. I share his sense that open source has advantages over closed source software, his interest in accountability, and his general agreement with end-to-end design. But labels matter, I think, and in this context architectural labels appear to hide the key questions rather than expose them. The core difficulty is that if the architectural approach is applied uncritically, any proposal can be justified as the application of one or more architectural theories. Every proposal opens law or code to more scrutiny, less scrutiny, or both. Under the architectural approach, however, any proposal that opens law or code to more scrutiny and interaction can be justified as an application of natural surveillance or community building principles. Conversely, any proposal that leads to law or code being less scrutinized can be justified as an application of territoriality principles. The virtual metaphor of cyberspace architecture is too flexible to be of much help in the design of strategies to deter computer crime.

IV. THIRD-PARTY CIVIL LIABILITY

Over reliance on virtual metaphors also undergirds a number of proposals to impose civil liability on third-parties for the costs of criminal activity. Here my critique is relatively narrow and cautious, in part because the literature is extensive and diverse. Scholarly discussion of third-party civil liability for computer crime dates back to the 1970s, and the relevant

[40] *See* Katyal, *Digital Architecture, supra* note 4, at 2272-73.

[41] *See id.* at 2273 ("Generally speaking, both online and offline, open networks for communication and transportation promote growth, opportunity, and interconnectivity.").

[42] *See id.*

body of work includes dozens of different proposals.[43] For the sake of simplicity, I will focus on just one subset of this literature: ISP liability for subscriber misconduct. In recent years, a number of scholars have explored whether Reinier Kraakman's insights about the benefits of third-party enforcement can be applied to ISPs.[44] ISPs may be better equipped to deter crime than public law enforcement, the thinking goes. ISPs can monitor their subscribers for signs that they are engaging in computer hacking or distributing viruses, and then disable the accounts or take other action to block the misconduct.[45] By imposing liability on ISPs for the wrongs of their subscribers, the law may be able to create incentives for ISPs to deter the subscribers' criminal activity.

My interest in these proposals concerns the assumptions they make about the powers and capacities of ISPs. The proposals tend to assume that ISPs can monitor and control their property much like a physical property owner can monitor and control physical property. In effect, each computer is like a small patch of cyberspace: its owner should be able to see what is going on in that area of cyberspace much like an employer can watch what is going on in the workplace. The owner can also control what he sees and take action to address problems and eliminate sources of wrongdoing. ISPs can act like chaperones at a high school dance, ferreting out untoward conduct and requiring the offenders to leave.[46] Or perhaps ISPs can develop hacker profiles of characteristic hacker activity; when an account is used in a way common to what a hacker would do, the ISP can study that account closely for signs of illegal activity.[47] The common theme is that computer owners can know and control what is happening within their networks; civil liability can lead to less crime because computer owners have the power (and, with civil liability, the incentive) to minimize criminal activity.

But is this assumption valid? There are good reasons to think the answer is "no." In the context of physical space, third-party monitoring generally refers to visual observation. Visual observation can provide a remarkably efficient surveillance tool to identify wrongdoing. A chaperone

[43] *See supra* note 5. For an early article on the role of civil liability see Susan Nycum, *Liability for Malfunction of a Computer Program*, 7 RUTGERS COMPUTER & TECH. L.J. 1, 1-22 (1979) (considering the prospect of civil liability for creators of software programs).

[44] *See* Reinier Kraakman, *Gatekeepers: The Anatomy of a Third Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 100-101 (1986). For applications of Kraakman's idea to ISP monitoring, *see, e.g.*, Katyal, *supra* note 5, at 1095-97; Hamdani, *supra* note 5, at 910-12; O'Neill, *supra* note 3, at 282-84.

[45] *See* Posner & Lichtman, *supra* note 5, at 18-20; Katyal, *supra* note 4 at 2284-85; O'Neill, *supra* note 3, at 282-84.

[46] *See* O'Neill, *supra* note 3, at 283-84. *See* Katyal, *Criminal Law in Cyberspace*, *supra* note 5, at 1096.

[47] *See* Katyal, *supra* note 5, at 1096 ("ISPs could also develop sophisticated hacker profiles that permit them to survey large numbers of users and pick out those who look suspicious because they repeatedly try to enter certain sites.").

at a high school dance can look at the dancers and easily tell if they are acting inappropriately. Visual observation is powerful; our eyes are trained to identify subtle patterns and reach quick conclusions. When proponents of ISP liability discuss ISP monitoring, they tend to draw from our instinct that computer monitoring must be something like visual monitoring. The word "monitoring" generally is used in an abstract way to suggest a virtual form of visual observation.

The virtual metaphor papers over the technical details, however, and those technical details indicate important limitations on ISP abilities. When you look more carefully at the technical problems, a different picture of ISP abilities emerges. Most obviously, ISPs cannot actually "see" accounts. They can only monitor accounts in ways that computer code allows, and that monitoring typically involves some form of wiretapping. Consider rules of liability that would encourage ISPs to determine when a customer is engaging in wrongdoing. How can an ISP know what a customer is doing? The most obvious approach would be to wiretap the customer's account; the ISP could install a surveillance device that taps into and records the user's line of traffic. As a technical matter, however, it is quite difficult to go from a stream of Internet traffic to a conclusion that a particular person was responsible for particular conduct. The data stream does not tell you who is using the account, or in what context. The ISP may be able to identify whether a user's account sent out a particular piece of malicious code, but it lacks the ready means to identify who sent it, or whether it was sent knowingly or unknowingly.

Unless an ISP wants to devote a full-time employee to following the conduct of a few accounts – quite a costly proposition given that ISPs can have millions of customers – the most viable monitoring tactic is "dumb" monitoring that can only look for particular bits and bytes of known code or trends in usage. Dumb monitoring has a high error rate, however, and is relatively easy to defeat. Consider our experience with spam filters. Spam filters monitor and attempt to identify incoming spam in much the same way that an ISP might try to monitor outgoing communications to identify malicious code. As anyone with an e-mail account will attest, spam filters never work perfectly: they only detect a proportion of spam, and occasionally block mail that is not spam. Ease of circumvention is also critical. If a person knows his ISP is monitoring his outgoing traffic to look for malicious code, he can take simple steps to ensure that his code evades the monitoring. He can encrypt the code, or send it in parts, effectively defeating the ISP's filters. In short, comprehensive ISP monitoring appears to be extremely difficult, even putting aside the very important privacy questions it raises. ISPs can have hundreds of thousands or even millions of customers; it is very difficult and time consuming for an ISP to watch just one or two customers in a comprehensive way; and it is easy for any customer to circumvent or defeat ISP monitoring.

Even proposals not reliant on virtual metaphors can be weakened by lack of attention to technical detail, leading to an unwarranted confidence in ISP monitoring abilities. For example, Doug Lichtman and Eric Posner suggest that ISPs may be able to program their computers to create a profile for each user, and then regularly compare that profile to usage patterns.[48] They write:

> [An] ISP can detect criminal behavior by analyzing patterns of use, much as a bank can detect credit card theft by monitoring a customer's pattern of purchases. Some patterns of use are intrinsically suspicious, for instance a continuous stream of communications from a home user. Other patterns are suspicious because they represent a radical departure from the user's ordinary behavior. If an ISP programs its computers to create a profile for each user, and then regularly compares the user's current patterns with that historic profile, the ISP should be able to detect this genre of unauthorized usage and intervene.[49]

While this may sound promising at first, it is worth pointing out the major differences between credit card account monitoring and the kind of ISP monitoring Lichtman and Posner suggest. Credit cards are used to purchase goods and services, and sellers must be registered and report every purchase immediately. Patterns of misuse are easy to identify; a credit card thief typically will attempt to run up as many purchases as the card will handle before a purchase is rejected. An attempt to max out the card will invite suspicion, and it is easy to program a computer to detect when that attempt occurs.

But what are the similar patterns for detecting criminal behavior in the case of an Internet account? Computers connected to the Internet can be used in an infinite number of ways to do an infinite number of things. The diverse range of Internet applications and uses for them makes it difficult (if not impossible) to identify a reliable marker that correlates with criminal activity. Lichtman and Posner suggest that a continuous stream of communications from a home user could signal criminality. But a continuous stream of communications could mean many things. Perhaps the user is merely uploading a large file; perhaps he is using a peer-to-peer networks to distribute files (whether copyrighted or not); perhaps the user has installed software allowing his computer to host Internet relay chat channels; perhaps he is sending e-mails with very large attachments. The transfer of data from a home user does not correlate sufficiently closely with criminal activity to warrant ISP investigation.

These difficulties do not mean that civil liability on third-party providers is necessarily a bad idea. But I think they provide reason for caution. Before the law adopts such a strategy, care should be taken to ensure that they do not rest in part on assumptions carried over from physical world dynamics that may not apply to the Internet.

[48] *See* Lichtman & Posner, *supra* note 5, at 18.

[49] *Id.*

CONCLUSION

The cyberspace metaphor is a powerful tool. It provides insights that help us understand our online interactions and their social meaning. At the same time, reliance on the virtual metaphor of cyberspace carries considerable dangers. At its worst, the virtual metaphor blinds us to how the Internet works; it substitutes metaphors from physical space instead of the reality of the Internet's dynamics. Deterring computer crime requires more focus on the reality of the network and less on metaphors of virtual worlds. A focus on the physical perspective of the Internet can ensure that concepts of deterrence that sound plausible in theory are also realistic in practice.