CYBERCRIME: A CHALLENGE FOR THE TRADITIONAL MODEL OF LAW ENFORCEMENT

BY

SUSAN W. BRENNER[1]

[1] NCR Distinguished Professor of Law & Technology, University of Dayton School of Law, Dayton, Ohio. Email: Susan.Brenner@notes.udayton.edu Website: http://www.cybercrimes.net. A longer version of this paper is being published by the Rutgers Computer & Technology Law Journal.

I. Introduction

The proliferation of computer technology and attendant migration of human activities into cyberspace has had a negative effect upon our traditional model of law enforcement. As the next section explains, it is already clear that the traditional model is not an effective means of dealing with cybercrime.[2] As a result, an alternative approach to law enforcement, which emphasizes collaboration between the public and private sectors, is emerging. Section III explains how this evolving model functions and why it is emerging at this particular time and section IV offers a brief conclusion.

II. The Traditional Model of Law Enforcement

The traditional model of law enforcement evolved to deal with real-world crime; the essential components of the model were, for all intents and purposes, in place by the nineteenth century. Real-world crime is crime perpetrated in and via the real, physical world, that is, without the use of technology.

A. Real-world Crime

Because it is situated in a corporeal, physical environment, real-world crime has several defining characteristics. The sections below identify and examine the four characteristics that are the most significant for this discussion.

1. Proximity

The most fundamental characteristic of real-world crime is that the perpetrator and victim are physically proximate when an offense is committed or attempted. It is, for example, simply not possible to rape or attempt to rape someone if the rapist and victim are fifty miles apart; nor, in a non-technological world, is it possible to pick someone's pocket or take their property by force if the thief and victim are in different countries.

2. Scale

Real-world crime tends to be one-to-one crime, i.e., it involves one perpetrator and one victim. The "crime" commences when the victimization of the target is begun and ends when it has been concluded; during the event the perpetrator focuses all of his or her attention on the consummation of that "crime." When the "crime" is complete, the perpetrator is free to move onto another victim and another "crime." The one-to-one character of real-world crime derives from the constraints physical reality imposes upon human activity: A thief cannot pick more than one pocket at a time; an arsonist cannot set fire to more than one building at a time; and prior to the development of firearms and similar armament, it was exceedingly difficult for one bent upon homicide to cause the simultaneous deaths of more than one person.

[2] "Cybercrime" denotes the use of computer technology in an effort to achieve illegal ends. *See* Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), http://boalt.org/CCLR/v4/v4brenner.htm.

The one-to-one nature of real-world crime is more a default than an absolute; exceptions occur, especially as to the number of perpetrators. Rape, murder, theft, arson, forgery and many other crimes can involve multiple perpetrators; indeed, the aggregation of offenders and the rise of gangs and other types of "organized crime" is a tendency that has accelerated over the last several centuries. But while many-to-one deviations have occurred for centuries, one-to-many deviations were rare prior to the use of technology. In a world without computers, copiers and similar devices the forging of a document must be done by hand, which takes time and means that only a limited number of forgeries can be produced. Consequently, prior to say, 1800, forgery is almost inevitably a one-to-one crime.

3. Physical constraints

Real-world crime is subject to the physical constraints that govern all activities in the "real," physical world. Because we are accustomed to living our lives according to the dictates of these constraints, we do not appreciate how they enhance the complexity of criminal endeavors. Every "crime," even routinized crimes such as street-level drug dealing, requires a level of preparation, planning and considered implementation if it is to succeed; for real-world crime, these activities must be conducted in physical space.

One who decides to rob a bank must visit that bank to familiarize herself with its physical layout (entrances, teller windows, vault location), security (guards, surveillance cameras, visible alarm systems) and routine (when employees arrive and leave, times when the bank is likely to have the fewest customers, currency pickup and delivery). This exposes the putative robber to public scrutiny that can result in her being caught. The same is true of the robbery; once inside the bank, a robber can leave evidence or produce observations that can result in her being apprehended.[3] It is also true of the robber's flight once the robbery has been committed; here, too, she is exposed to public view and therefore runs the risk of being noticed and identified.[4] In addition to the risks of exposure that arise from planning and committing the "crime" itself, the robber will presumably need to secure a weapon and some type of disguise, and may need to find some way to launder the funds she takes from the bank. Like the processes involved in the robbery, each of these steps takes time and effort, incrementally augmenting the total exertion required for the commission of this "crime;" and like the robbery itself, each increases the likelihood that she will be identified and apprehended.

4. Patterns

With real-world crime, it becomes possible, over time, to identify the contours and incidence of the "crimes" committed within a society.[5] Real-world victimization tends to fall into demographic and geographic patterns for two reasons. One is that only a small

[3] *See, e.g.,* United States v. Morrison, 254 F.3d 679, 681 (7th Cir. 2001) (Morrison, who robbed a bank, left a shoe print on the teller's counter which was later used to link him to the robbery).

[4] *See, e.g.,* United States v. Morrison, 254 F.3d 679, 681 (7th Cir. 2001) (officers noticed the remnants of the bank's dye pack in a car used by Morrison, who robbed the bank).

[5] *See, e.g.,* U.S. Department of Justice – Bureau of Justice Statistics, Crime Victimization 2001: Changes 2001 with Trends 1993-2001 15 (2002), http://www.ojp.usdoj.gov/bjs/pub/pdf/cv01.pdf.

segment of a functioning society's populace will persistently engage in criminal activity. Those who fall into this category are apt to be from economically-deprived backgrounds and to reside in areas that share certain geographic and demographic characteristics, primarily those in which the less affluent members of that society reside. They will be inclined to focus their efforts on those with whom they share a degree of physical proximity because they are their most convenient victims. This means that much of the "crime" in a society will be concentrated in specific areas, such on the "West Side of Notown" or "South of 31st Street in Megalopolis."

The other reason "crime" falls into patterns is that each society has a repertoire of "crimes" -- of legal rules that proscribe a set of behaviors ranging from more to less serious in terms of the respective "harms" each inflicts.[6] The "harm" caused by a specific "crime" is encompassed by, and limited to, the definition of the offense: A rape produces the "harm" targeted by the "crime" of rape; a theft causes the "harm" inflicted by the "crime" of theft; a forgery yields the "harm" subsumed by the "crime" of forgery, and so on. In a functioning society, the more egregious "crimes" will occur much less often and may occur less predictably than the minor "crimes." Murder, for instance, is an extraordinary event in any society that is successfully maintaining social order and resisting chaos. Theft in its various forms is a far less extraordinary event; and, depending on the cultural mores of the society, drunkenness and/or prostitution may be quite common. Also, various "crimes" fall into localized patterns reflecting geography and particular types of victimization.

Because these characteristics are inevitable aspects of "crime" in the real-world, they shaped the traditional model of law enforcement that evolved to deal with this type of "crime." The next section explains how each characteristic contributed to the model.

B. Traditional Model of Law Enforcement

As noted above, real-world crime has four empirical characteristics: physical proximity of victim and victimizer; default one-to-one "crime"; the influence of physical constraints; and offender and "crime" patterns. As policing evolved, these aspects of real-world crime became embedded assumptions that shaped the traditional model of law enforcement and defined the way it approaches "crime" in general.

The first characteristic contributed a presumed dynamic to the model: victim-offender presence in the same general locale; victim-offender proximity and resulting victimization; offender's efforts to leave the locale or otherwise avoid apprehension and prosecution; investigation; identification, apprehension and prosecution of the offender. The dynamic reflects a time when life and crime were both parochial, when victims and offenders generally lived in the same village or in the same city neighborhood. If a victim and offender did not actually know each other, they were likely to share community ties; this facilitated the process of apprehending offenders because there was a good chance they could be identified by the victim, by witnesses and/or or by reputation. If the perpetrator and the victim did not share community ties, that is, if the perpetrator was a stranger, his alienness was likely to contribute to his being apprehended because the

[6] *See* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace,* 2002 UCLA J. L. & Tech. 3, 55-65 http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf.

local citizenry paid particular attention to those who "did not belong" in their portion of the physical world. Law enforcement dealt effectively with this type of crime because its parochial character meant investigations were limited in scope. The model therefore assumes that the investigation of a "crime" can focus upon a specific geographical area surrounding the site where the "crime" occurred.

The second characteristic contributed another element: The traditional model of law enforcement assumes one-to-one victimization and that assumption, in conjunction with an unrelated assumption, structures its conceptualization of the scale of "crime". The unrelated assumption is that incidents of criminal activity are, to a greater or lesser extent, extraordinary events in a society; the model assumes "crime" is a deviation from the law-abiding conduct that constitutes the prevailing pattern of behavior in a society. This assumption derives not from the physical characteristics of real-world crime but from the nature of criminal law: the function of the criminal law is to maintain an acceptable level of social order within a society.[7] It does this several ways – by defining what is and is not acceptable behavior; by specifying the consequences of engaging in unacceptable behavior; and by socializing the members of a society in such a way as to ensure that the prevailing pattern of conduct eschews unacceptable behavior. The presumptive result is that "crime" becomes a subset, generally a small subset, of the total behaviors in a societal population; consequently, law enforcement – which is charged with apprehending those who engage in unacceptable behavior -- can focus its efforts on a limited segment of the conduct within a given society.

The assumption that "crime" is committed by a small percent of the population is one element – the "offender element" -- structuring the model's conceptualization of the scale of "crime." The other element – the "offense element" – is the default assumption of one-to-one victimization. "Crimes" are defined in terms of the seriousness of the "harm" each inflicts. If one-to-one victimization is the norm, a completed "crime" inflicts a "harm" upon one victim; additive "harms" must be inflicted sequentially. So, while a serial killer can cause many deaths, each a distinct "harm," he necessarily does so consecutively, with each death representing a discrete "crime."

The conceptualization of scale derived from these assumptions posits that the incidence of victimization in a society will be relatively small both (a) in relationship to the size of the population and (b) in terms of the level of "harm" inflicted. The source of the first proposition is the assumption that only a small percentage of a society's population persistently engages in criminal activity. The derivation of the second proposition is more complex. The level of "harm" inflicted by the incidence of victimization in a society is a function of three variables: (1) the number of individuals engaged in committing "crimes"; (2) the number of discrete "crimes" these individuals commit in a given time period; and (3) the types of "harm" caused by the "crimes" these individuals commit. The operation of these variables is best illustrated by means of a hypothetical. Assume a society consists of 10,000,000 people, of whom 500,000 engage in criminal activity on a more or less regular basis. Assume that 200,000 of these 500,000 miscreants are incarcerated or are for other reasons not actively engaged in criminal activity during the time period at issue. This defines the first variable by giving us the basic pool of individuals who will commit "crimes" during this time period. Defining the remaining two variables is more problematic because they tend to interact. That is, it is difficult to set a

[7] *See, e.g.,* ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW 5 (3d ed. 1982).

generic number of “crimes” our 300,000 persistent offenders are likely to commit because the number of “crimes” an individual commits tends to be a function of the seriousness of the “crimes” at issue. A low-level drug dealer or a street prostitute may commit fifty or more “crimes” a week, but this will most certainly not be true of an arsonist or a career bank robber. As the seriousness of a “crime” increases, the frequency with which it is committed tends to decrease; most murderers, for example, kill only once. Crime statistics therefore indicate, and the traditional model assumes, that most of the “crimes” committed by a society’s persistent offenders – the 300,000 miscreants in our hypothetical – will be less serious “crimes,” i.e., “crimes” that do not involve the infliction of death, physical injury or massive property damage/loss.

Finally, as explained earlier, the traditional model’s conceptualization of scale incorporates the fourth characteristic of real-world crime, i.e., the premise that offenses and offenders fall into identifiable patterns. What this adds to the conceptualization of scale is the notion of localization. The traditional model’s conceptualization of the scale of real-world “crime” postulates that it will be limited in incidence and in the relative type of “harms” it inflicts on a populace. This final premise contributes the notion that an identifiable percentage of these real-world “crimes” will occur in geographically and demographically demarcated areas.

The traditional model, in other words, assumes real-world “crime.” It relies upon the empirical characteristics of real-world “crime” and certain extrapolations from these characteristics to structure its approach to “crime.” The model assumes that societal “crime:” (a) consists of discrete events – “crimes” – each of which is physically situated; (b) is subject to the constraints associated with activity in the physical world; (c) is qualitatively and quantitatively limited; and (d) falls into identifiable geographical and demographic patterns. These assumptions combine to generate the principle upon which the model’s approach to “crime” is based -- that it is a manageable phenomenon for law enforcement. The first two assumptions contribute the premise that discrete “crimes” necessarily leave information, evidence, in the real-world locale where they were committed. Extrapolating from this premise yields the conclusion that law enforcement personnel reacting to the report of a “crime” can locate this information, this evidence, and use it to apprehend the perpetrator of the offense. The model postulates that perpetrators remain in or near the area where the “crime” was committed, which will facilitate their being apprehended by the authorities. These two assumptions inferentially establish law enforcement’s ability to deal with specific “crimes,” which is necessary if “crime” is to be a manageable phenomenon. The last two assumptions add the premise that because real-world “crime” occurs on a modest scale and assumes certain patterns, law enforcement can mobilize its modest resources so as to deal with it effectively.

Each of these components of the model is based upon our historical experience with “crime”: We believe perpetrators will remain in the area where they commit their “crimes” because they have tended to do so on the past (more so, of course, prior to the proliferation of the automobile and other forms of motorized transportation). We believe the commission of a “crime” leaves information – such as weapons or trace evidence at the crime scene and witness observations of the perpetrator or victim – which the police can collect, analyze and use to apprehend and convict the perpetrator. We believe all this because it has been established practice at least for the last century, since the development of forensic science.

These beliefs are micro-components of the model; that is, they structure how it approaches discrete events, specific “crimes.” The model does have an over-arching conception of how law enforcement should deal with “crime” as a general phenomenon. This conception is historically derived; like the common law, the traditional model of law enforcement is a compilation of past practices that have been deemed to be effective in dealing with the phenomena it confronts. The model’s general strategy is one that has been in use since antiquity -- the reactive approach -- and remains the same as it was centuries ago, when law enforcement consisted of a constable or night watchman: A “crime” is committed and reported to the appropriate law enforcement personnel, who investigate the offense and, if the investigation is successful, apprehend the perpetrator, who is then formally charged with the “crime,” prosecuted, and presumably convicted.[8]

This reactive approach emerged millennia ago as a pragmatic solution to what was then very atypical behavior, i.e., the commission of a real-world “crime.” “Crime” is an unusual event in small, rural societies because the informal social control exerted by shared religious and other philosophies is sufficient to deter most would be offenders. When a “crime” does occur, it is relatively easy to address given the nature of the society in which it is committed. Identifying the perpetrator, who may literally be caught red-handed, is usually not difficult; the operation of the physical constraints discussed earlier is magnified, so it may be impossible for an offender to avoid observation and detection either in the process of committing the “crime” or in the process of fleeing from it. And the essential impossibility of “stranger danger” means that it is relatively easy to deduce who might have had the necessary motive and opportunity for the offense. The level of organizational development in the society determines who will actually be responsible for apprehending an identified perpetrator: In very simple societies, this task is assigned to the general citizenry; more developed systems allocate it to designated individuals, such as the common law’s sheriff or constable.

The reactive approach is a workable and appropriate means of addressing “crime” in the small, rural societies in which it evolved. It is a workable solution because societies such as this have neither the resources nor the organizational ability to field a force of designated law enforcement officers who might take a rather different approach, a proactive approach, to dealing with “crime.” Crime control is therefore a matter of responding to what has been done in a way that is presumed to prevent future such occurrences. The appropriate response take the form of retributive justice; at this stage of social development, societies tend to regard the commission of a “crime” and the “harm” it inflicts as a personal affront which requires an equivalent response, i.e., an eye for an eye.[9] This type of response is regarded as appropriate for at least two reasons: On a purely visceral level, it returns “harm” for “harm,” so that theft, for instance, may result in the thief’s losing the hand with which he committed the “crime.” On a more practical level, this type of response is regarded as an effective way of deterring the commission of future “crimes”; it is considered to accomplish this by ensuring that the apprehended offender does not engage in further criminal activity and by using him as an example to discourage other would-be offenders from doing so. The apprehended offender is nullified either by inflicting a level of pain that would deter a rational human

[8] *See, e.g.,* Mark H. Moore & George L. Kelling, *"To Serve and Protect": Learning from Police History*, 70 Pub. Interest 53 (1983).

[9] *See, e.g.,* Code of Hammurabi, The Avalon Project at Yale Law School, http://www.yale.edu/lawweb/avalon/medieval/hamframe.htm.

being from running the risk that it might be repeated or by taking his life; and retributive justice assumes that either result will be sufficient to deter others from following in his footsteps, especially if the punishment is publicly administered.

Although it evolved centuries ago to meet the demands of societies in which “crime” was rare and justice was retributive, the reactive model of law enforcement has persisted. It remains the prevailing model in countries around the world even though penal philosophies have increased in complexity and retributive justice has diminished in importance. Why has it endured? One reason, no doubt, is that we are accustomed to this model and the dynamic it incorporates; we expect law enforcement to respond when a “crime” is committed, and we assume that the apprehension, prosecution and eventual punishment of the offender will satisfactorily resolve things, returning “harm” for “harm” and deterring future “crimes.” Another reason is that societies are unwilling or unable to allocate the increased resources that are needed to implement a proactive model which emphasizes “crime” prevention as well as control-by-deterrence. Yet another reason is that it is still a workable means of dealing with real-world “crime”; it may not be the most effective means, but real-world “crime” still retains the characteristics described earlier and the persistence of those characteristics means the reactive model continues to be a viable strategy for addressing real-world “crime.” The open question is whether it is a viable strategy for cybercrime.

C. Cybercrime

While our experience with cybercrime is stilll in its infancy, it is already apparent that the traditional model of law enforcement is not an effective strategy for dealing with cybercrime. It cannot deal effectively with cybercrime because online crime possesses few, if any, of the essential characteristics of real-world “crime.”

1. Proximity

Perhaps the most critical difference between the two is that, unlike real-world “crime,” cybercrime does not require any degree of physical proximity between victim and victimizer at the moment the “crime” is committed. Cybercrime is unbounded crime, borderless crime. It can be committed by someone who is located anywhere in the world against a victim who is in another city, another state, another country. All the perpetrator requires is access to a computer that is linked to the Internet; with this, he can inflict “harm” upon someone directly, by attacking their computer, say, indirectly, by obtaining information that lets him assume their identity and use it commit fraud on a grand scale.

2. Scale

Cybercrime is not one-to-one “crime” because it is not corporeal crime, not terrestrial crime; consequently, the one-to-one scale of offense commission is by no means a viable default assumption for cybercrime. Much of cybercrime is already, in effect, “automated crime;” this trend will only accelerate. The phrase “automated crime” denotes an individual's ability to use technology to multiply the number of offenses she can carry out in a given period of time; a single perpetrator can commit thousands of cybercrimes in a short period of time. Indeed, with automated crime, a perpetrator can put the process of victimization into effect and turn his or her attention to other matters, letting automated systems carry out the process. This creates a problem for law enforcement operating under the traditional model, which dictates that officers will react to reports of "crimes," initiate an investigation, apprehend the perpetrator and thereby ensure that justice is done. The traditional model, however, assumes the commission of real-world crime and, in so doing, assumes that "crimes" will be committed on a manageable scale.

This is not true of cybercrime; computer technology acts as a force multiplier that vastly increases the number of "crimes" an individual can commit and the speed with which she can do so. The additive scale of cybercrime overwhelms law enforcement's ability to react because this ability is based on the assumption that "crime" is real-world "crime." Cybercrime violates this assumption in two ways: It is committed on a scale far surpassing that of real-world "crime;" and it represents an entirely new class of "crime" that is added to the real-world "crimes" with which law enforcement has traditionally dealt and with which it must continue to deal. As a result, law enforcement's ability to react to "crime" erodes because the resources which were adequate to deal with the incidence of real-world "crime" are inadequate to deal with real-world "crime" plus cybercrime.

3. Physical constraints

Perpetrators of cybercrime are not restricted by the constraints that govern action in the real-world. Cybercrimes can be committed instantaneously and require a rapid response; but law enforcement is accustomed to real-world "crimes," the investigation of which can proceed at a more deliberate pace. Another complication is that all, or substantially all, of the conduct involved in the commission of a cybercrime occurs in an electronic environment; since a perpetrator is not physically "present" when the "crime" is committed, one can no longer assume she will leave trace evidence at the crime scene. The transborder nature of cybercrime enhances the difficulties law enforcement officers face when they try to react to a reported offense because traditional assumptions about a perpetrator's being observed preparing for, committing or fleeing from an offense no longer hold.

And cyberspace lets perpetrators conceal their identities; cybercriminals can enjoy anonymity on a scale that is not possible in the real-world. In the real-world, an offender can wear a mask and perhaps take other efforts to conceal his identity, but certain characteristics -- such as height, weight, accent, age -- will still be apparent. In cyberspace, one can achieve perfect anonymity;[10] consequently, officers may have no way of identifying the person who victimized someone in their jurisdiction. As one report noted, "[t]he ability for criminals to remain anonymous on the Internet presents a huge challenge for police and policy makers. Anonymity is assisted by a proliferation of

[10] See, e.g., Jonathan I. Edelstein, Note, *Anonymity and International Law Enforcement in Cyberspace,* 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 231 (1996).

Internet cafes and web kiosks, the emergence of data havens, the availability of tools for ‘spoofing’ and the presence of anonymising services on the Internet”.[11]

Even if police can identify a perpetrator, gathering evidence of the crime can be difficult for various reasons. The country that hosts the cybercriminal and his activities may not define what he did as illegal and may therefore be unable to prosecute him or cooperate in his being extradited for prosecution elsewhere;[12] the host nation may not have agreements in effect with the victim nation which obligate it to assist in gathering evidence that can be used against the perpetrator; or the evidence may have been destroyed, advertently or because it was routine transactional data that was not retained by the Internet Service Provider which the offender used to commit his crime.

4. Patterns

Perhaps because cybercrime is such a new phenomenon, we cannot identify patterns comparable to those that exist for real-world crime. We are unable, as yet, anyway, empirically to derive conclusions as to how various types of cybercrime will manifest themselves geographically and demographically. Consequently, we cannot develop the type of crime maps law enforcement uses to allocate its resources in dealing with real-world crime.

One factor which may account for our inability to identify patterns in cybercrime is that it is not accurately documented; nations are not tracking the incidence of cybercrime in the same way they track real-world crime. There are several reasons for this lack of accurate cybercrime statistics: One is that countries have not defined what “cybercrime” is and how it differs from “crime.”[13] Another is that while law enforcement agencies do record reported cybercrimes, they do not break them out into a separate category; online fraud, for example, is recorded as “fraud.” Yet another reason is that it can be difficult to parse cybercrime into discrete offenses. Was the “Love Bug” virus which caused billions of dollars of damage in over twenty countries one crime or thousands of crimes? [14] Clearly, though, the most important reasons why we do not have accurate information about cybercrime are that (a) many cybercrimes go undetected and (b) many detected cybercrimes go unreported.[15]

But perhaps the lack of accurate statistics is not the real reason why we cannot identify patterns -- maybe the notion of “cybercrime patterns” is an oxymoron. The

[11] Barbara Etter, Critical Issues in High-Tech Crime, Australasian Centre for Policing Research 13 (2002), http://www.acpr.gov.au/pdf/Presentations/CIinHi-tech.pdf (footnote omitted).

[12] *See, e.g.,* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace, supra,* at 3-5.

[13] *See, e.g.,* Barbara Etter, Critical Issues in High-Tech Crime, Australasian Centre for Policing Research 9 (2002), http://www.acpr.gov.au/pdf/Presentations/CIinHi-tech.pdf.

[14] *See, e.g.,* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace, supra.*

[15] *See, e.g.,* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace, supra.*.

existence of patterns in real-world criminality is a function of the physical space in which real-world criminals operate: Economic forces dictate that most real-world "crime" is committed by individuals who suffer from varying levels of economic deprivation and are, therefore, apt to reside and function in economically-disadvantaged neighborhoods. These neighborhoods then generate offense and offender patterns because perpetrators tend to target victims of opportunity, i.e., those who are within some convenient zone of physical proximity.

Cyberspace makes physical space irrelevant: It becomes as easy to victimize someone who is halfway around the world as it is your next-door neighbor. Does this mean cybercrime will never assume patterns, either as to the location of the offense or the types of offenses being committed?

It is impossible to answer that question at this stage of our experience because all we know about this new type of crime is what we have seen so far. The apparent absence of cybercrime patterns may be a function either of the fact that they have not had time to develop or that they exist but we cannot identify them because they assume forms different from those we are accustomed to seeing in real-world crime. We cannot resolve this issue, but it may be helpful to speculate about whether patterns will evolve and, if so, how they might be useful in combating cybercrime.

It is useful to begin by considering the patterns that emerge in real-world crime and how law enforcement uses them to maximize its effectiveness. Real-world patterns reflect "crime"-categories and "crime"-locations. As to the former, the frequency with which real-world "crimes" are committed is in inverse proportion to the seriousness of the "crime"; less serious "crimes" are committed with greater frequency than more serious "crimes," such as murder. This means, among other things, that property "crimes" are committed much more often than crimes of violence and that the same is true of "crimes" involving traffic in societally-banned substances such as drugs and child pornography. "Crime"-category patterns are derived from compilations of data on reported offenses.[16] How does law enforcement use the patterns that appear in the commission of offenses? For one thing, they can be used to develop profiles of offenders; they can also be used to determine the best means of allocating limited police resources among various units. "Crime"-location patterns are also used to allocate resources; they let law enforcement agencies allocate officers to geographical areas where certain types of "crimes," at least, are committed with the greatest frequency.[17] Location patterns are derived both from data compilations concerning reported offenses and crime-mapping techniques.[18]

Since "crime"-category patterns are driven by human behavior more than by geography, it seems likely that category patterns will manifest themselves in cybercrime. Indeed, there is some evidence that they are already emerging. The current inadequacy of statistical data concerning the incidence of cybercrime makes it difficult to extrapolate

[16] *See, e.g.,* Summary of the Uniform Crime Reporting Program, Federal Bureau of Investigation: Crime in the United States 2001, http://www.fbi.gov/ucr/cius_01/01crime1.pdf.

[17] *See, e.g.,* Advanced Crime Mapping Topics 94-134, National Law Enforcement & Corrections Technology Center (2002), http://www.nlectc.org/cmap/cmap_adv_topics_symposium.pdf.

[18] *See, e.g.,* Advanced Crime Mapping Topics 94-134, National Law Enforcement & Corrections Technology Center (2002), http://www.nlectc.org/cmap/cmap_adv_topics_symposium.pdf.

as to the existence of offense patterns, but anecdotal evidence suggests that much of the contemporary cybercrime falls into three categories. One is hacking, which can be defined as gaining unauthorized access to a computer system either for the purpose of exploration or to cause damage once inside. Another is online fraud, which may exceed hacking in the frequency with which it is committed. The third category consists of child pornography and other crimes targeting minors, such as using the Internet to solicit children for sexual activity. Interestingly, the apparent frequency of these offenses is at least partially consistent with the proposition adduced above concerning the frequency of real-world crime; that is, in the real-world we can predict that property "crimes" (such as hacking and fraud) and trafficking in banned substances will be committed more often than, for example, "crimes" that involve the infliction of death, serious bodily injury or massive property damage.

What, if anything, does this mean for the development of offense patterns in the commission of cybercrimes? It could mean that the behaviors which shape the contours of real-world offense categories are constants in illicit human activities. That is, crime is finite: Because people commit "crimes" for specific, identifiable reasons, such as to enrich themselves, to take revenge, or to discharge psycho-sexual or other impulses, there is a fixed class of "crimes." If crime is finite, then we should see the same types of "crime" being committed in and via cyberspace and online "crime" will manifest itself in essentially the same ways as real-world "crime." All of this assumes, however, that we have seen humanity's entire repertoire of antisocial activity, an assumption which may very well be invalid. While it is reasonable to assume that our experience over the last several millennia has treated us to the gamut of motivations which prompt individuals to engage in antisocial activity, we need to remember that the way these motivations have manifested themselves so far has been the product of the physical constraints imposed by the real-world. We may well see traditional motivations generating antisocial activity that takes new and different forms in cyberspace, which would mean that real-world offense patterns will not recapitulate themselves in this new environment.

There is another possible explanation for the apparent recapitulation of real-world "crime" tends in cybercrime: It may be that we are so far only seeing the migration of real-world offense categories to cyberspace; that is, those who are currently using the Internet to commit "crimes" grew up with and were socialized by a climate in which the predominating mode of unlawful activity was real-world "crime," in its traditional guises. It would not be surprising, therefore, if they recapitulated the patterns they had observed with regard to real-world criminality online; they are, in other words, committing "crimes" and have not begun to imagine "cybercrime." Cyberspace, after all, not only erases the importance of geography; it also lets people do things they cannot do in real-space. So, we may see the emergence of new and as yet unexperienced varieties of "crime" (which will, of course, have to be defined as such). It is probably reasonable to anticipate that much of "crime" will continue to take the form of attempts at illicit self-enrichment; it is also probably reasonable to anticipate that the incidence of non-violent offenses will continue to exceed that of violent offenses. But beyond that, it is difficult to speculate; we will, for example, no doubt see the emergence of "collective crime," i.e., of automated mass victimization. If that occurs, we shall have to decide how to factor that into the way we categorize the "crimes" that were committed in a given time period: Is the automated victimization of 5,000 victims by one human offender using technology the commission of one "crime" or 5,000 "crimes"? And law enforcement will have to decide how to react to phenomena such as this. Should the allocation of resources continue to reflect the frequency with which certain types of "crime" are committed in an era when this process is automated, so that a few offenders can account for thousands and thousands of discrete “crimes”? Or should the allocation of resources be based on other criteria?

And what about the potential for mapping the location of cybercrimes? Is there any purpose in doing so? One difficulty that arises in this context is determining what is meant by the “location” of the “crime.” As was explained earlier, the traditional model of law enforcement assumes real-world “crime”; one characteristic of real-world “crime” is that the victim and victimizer must be in relatively close physical proximity at the time the “crime” is committed. Geography consequently assumes a great deal of importance in dealing with real-world “crime;” aside from anything else, focusing an investigation on the physical location of a “crime” offers police their best opportunity for identifying and apprehending the offender(s). But in cyberspace there is no “crime” scene, at least not in the traditional sense; for most cybercrimes, evidence is scattered over several locations, including the computer the perpetrator used, the victim’s computer and the intervening computers and computer servers the perpetrator used to accomplish the offense. So, if a woman in the Ukraine uses the Internet to defraud a man in Texas, where did the “crime” occur? If one assumes that the victim is the locus of a “crime,” then it occurred in Texas; but, of course, little evidence of the “crime” will be found in Texas, and the perpetrator will most certainly not be found there. Does this mean that “crime”-location patterns will be irrelevant in dealing with cybercrime? It is impossible to answer that question with any certainty. It might be useful to know where offenders are geographically located, assuming that can be ascertained; knowing the location of the offender is a primary goal of the traditional, reactive model of law enforcement.

But that raises the critical issue: While the apparent difficulty of identifying patterns in cybercrime does not itself sound the death knell for the traditional model of law enforcement, it demonstrates the difficulties that are involved in extrapolating this model to the world of online activity. It seems that we must come up with a better approach, which could involve either devising an entirely new model of law enforcement, one that is more suited for online crime, or modifying the traditional model so it becomes an effective means of addressing cybercrime. The next sections take up these issues.

III. An Alternative

The migration of human activity into cyberspace is already producing antisocial activity that does not exhibit the characteristics which shaped the traditional model of law enforcement. This trend will only accelerate, which means that the deficiencies in the traditional model will become ever more apparent and ever more problematic. We must, therefore, consider how we can improve law enforcement’s ability to address cybercrime without sacrificing the traditional model’s proven utility in dealing with real-world crime.

It is useful to begin this exercise by considering why the traditional model is not an effective means of addressing cybercrime. As § II explained, the traditional model is a reactive model: Its fundamental premise is that officers react to completed “crimes” by apprehending the perpetrators, who are prosecuted and punished; this renders them incapable of re-offending and ensures that their experience deters others from offending. This is a territorial approach to law enforcement; it assumes that perpetrators, victims and officers are all physically situated in a reasonable degree of proximity within a single territorial state. When these assumptions are valid, the model works; officers who know the area stand a good chance of being able to identify and apprehend perpetrators, and the local legal system stands a good chance of being able to convict and punish them. As § II explained, these assumptions do not hold for cybercrime; the use of cyberspace to commit "crimes" makes territory, and assumptions predicated on territory, irrelevant.

Does that mean we should abandon the traditional model for a new approach? The answer is "yes" and "no." We do need a new approach, particularly for cybercrime, because the traditional model is not a wholly workable solution for online crime. But this does not mean we should abandon the strategy responsible for the traditional model, i.e., that when a "crime" has been committed the law enforcement system reacts in an effort to bring the perpetrator to justice. However we decide to deal with cybercrime, we will always want law enforcement to react to some "crimes," certainly the more egregious "crimes," because of the benefits that derive from a society's reacting to and inflicting certain consequences upon offenders. The problem with applying the traditional model to cybercrime is not that there is anything wrong with this strategy; it is that the peculiar characteristics of crime in cyberspace make the application of this strategy sufficiently problematic that we can no longer rely upon it as our sole approach to dealing with criminal activity. We need to retain the traditional model but modify it to incorporate an additional strategy, one that is optimally focused upon dealing with criminal activity in cyberspace (and that can also be extrapolated to address some quantum of real-world crime).

Logically, there are two ways we can deal with crime: (1) React after a "crime" has been committed in order to incapacitate and punish the perpetrator(s); (2) prevent "crimes" from occurring. The two are not inconsistent; indeed, there has for the last century been an evolving emphasis upon preventing "crimes," though this still plays a small role in our overall approach to dealing with real-world crime. One reason why prevention is a small part of our current strategy is that it is resource-intensive; as long as we rely on law enforcement officers for crime prevention, increasing our efforts to prevent crime means we have to increase the number of officers who are available to patrol the streets of our communities, work with community members and otherwise create a climate in which the commission of "crime" is seen as a high-risk and therefore unattractive proposition. Since hiring, training and employing officers is costly, and since state and local governments have limited resources, crime prevention has been a minor part of our official law enforcement strategy.

But because prevention is an effective strategy, citizens turned to private sources for assistance in preventing their being victimized by real-world criminals.[19] This trend, which began in the latter part of the nineteenth century with the rise of private security services such as the Pinkerton Agency,[20] accelerated toward the end of the twentieth century as corporate and other commercial entities sought protection for their business endeavors and, often, for their officers and employees.[21] In a sense, it is a return to an older model, one that antedates Sir Robert Peel's creation of the modern police force in nineteenth century London;[22] until that time, security had been something of an ad hoc

[19] *See, e.g.,* David A. Sklansky, *The Private Police,* 46 UCLA L. Rev. 1165 , 1212-1221 (1999).

[20] *See, e.g.,* Brian Forst, *The Privatization and Civilianization of Policing,* 2 Criminal Justice 2000 at 21, http://www.ncjrs.org/criminal_justice2000/vol_2/02c2.pdf:

[21] *See, e.g.,* Sklansky, *The Private Police, supra,* 46 UCLA L. Rev. at 1220-1221.

[22] *See* Sklansky, *The Private Police, supra,* 46 UCLA L. Rev. at 1202-1203 (footnotes omitted).

affair, often consigned to private individuals and private arrangements.[23] Sir Robert's introduction of a modern, state-sponsored law enforcement organization led to the decline and ultimate disappearance of the prior model; consequently, for over a century, states have enjoyed a monopoly on the arrangements that govern internal security within their territories.

Cyberspace does not have "territories," which is one reason why the traditional model of law enforcement is not an effective means of dealing with cybercrime. The solution is to move from a model in which law enforcement is the exclusive province of the state to one in which it becomes the shared responsibility of the state and the private sector. The notion of allocating some responsibility for crime prevention, detection and response to the private sector is, as noted above, far from new. For decades, private security companies have protected corporate funds, facilities and employees. More recently, companies have supplemented these efforts by relying on private security agencies to help them discourage and – when that proves unsuccessful – investigate corporate espionage and other "business-related" crime.

These efforts, which primarily target real-world crime, tend to be substitutionary; that is, they generally involve the use of private security resources as an alternative to seeking assistance from law enforcement. Not surprisingly, this approach is being applied to cybercrime; companies are engaging the services of consultants and security firms in an effort to prevent their becoming victims of online crime. The private sector's use of commercial services to help secure their operations in cyberspace is novel only insofar as it involves cyberspace; as noted above, businesses have long relied upon private entities to protect them from real-world crime.

Another approach is evolving with regard to cybercrime, however, one that utilizes a very different strategy for dealing with criminal activity. It is predicated upon the collaboration of members of the public and private sectors both in preventing and in reacting to cybercrime. Under the traditional model, law enforcement was exclusively responsible for responding to completed crimes – the victim's role was limited to reporting a crime to the appropriate officials and then, if requested, assisting with their investigation. This aspect of the traditional model has not changed; the onus is still placed on victims to report their victimization to law enforcement and cooperate, to the best of their abilities, with an investigation conducted by law enforcement. What has changed are two aspects of how this model is implemented with regard to cybercrime.

One aspect that has changed is the way in which commercial victims report their victimization. The rise of cybercrime has aggravated a tendency that existed before, in at least certain areas of the private sector. It ha long been common knowledge among those in the banking industry that financial institutions tend to fire embezzlers instead of reporting them to the police and having them prosecuted for their crimes.[24] Historically, banks eschewed prosecution in all but the most egregious cases for fear that publicizing embezzlements would lead to a loss of confidence among the members of the banking

[23]

[?]*See, e.g.,* Forst, *The Privatization and Civilianization of Policing, supra,* 2 Criminal Justice 2000 at 26.

[24] *See, e.g.,* Richard Forno & Ronald Baklarz, The Art of Information Warfare 4 (1998), http://www.bookpump.com/upb/pdf-b/1128576b.pdf.

public. Similar tendencies have existed, no doubt, in other areas of the private sector, but the disinclination to report being victimized seems to be much more pronounced when cybercrime, rather than real-world crime, is involved. The annual cybercrime survey which the Computer Security Institute conducts in conjunction with the Federal Bureau of Investigation has consistently shown, for example, that only a very small percentage of cyberattacks on businesses are reported to law enforcement.[25]

The private sector's reluctance to report cybercrimes has caused great concern in the law enforcement community for various reasons. One is that if businesses do not report cybercrime, the perpetrator of an offense may return to re-victimize that business and/or use the same tactics to victimize other businesses. The net effect is similar to that which results when a bank discharges an embezzler instead of having her arrested and prosecuted; by letting her go, the victim bank gives her the opportunity to victimize other financial institutions. An article written by an attorney with the Department of Justice's Computer Crimes and Intellectual Property Section outlines two other reasons why it is important that victims report cybercrime:

> Specific deterrence is perhaps one of the most compelling reasons for a company to report an intrusion. When law enforcement catches and successfully prosecutes an intruder, that intruder is deterred from future assaults on the victim. This is a result that no technical fix to the network can duplicate with the same effectiveness. . . . [The general deterrence that criminal law enforcement provides also benefits victims and potential victims in the long run.[26]

This reluctance to report is a problem for the traditional model, which assumes victims report "crimes" to law enforcement; indeed, victim reporting is a primary driver of the model's approach to real-world crime. Since real-world victims tend to report their victimization, neither the traditional model of law enforcement nor the criminal law has had to consider how to deal with the failure to report "crimes"; clearly, though, some solution needs to be devised with regard to cybercrime.

Law enforcement is in the process of devising such a solution. It is part of a larger change in the working relationship between law enforcement and the citizens it is dedicated to serving, a change that holds out the promise of evolving into a new model of law enforcement. Since this approach is emerging from the relationship between law enforcement and the commercial sector, the remainder of this section deals only with how it functions in with regard to corporate victimization and corporate crime prevention.

A collaborative relationship is evolving, in the context of combating cybercrime, anyway, between law enforcement and commercial entities in the private sector. This collaborative relationship has several aspects: It emphasizes cybercrime-prevention by facilitating the sharing of information among members of the public and private sectors;

[25] *See, e.g.,* Cybercrime Bleeds U.S. Corporations, Survey Shows; Financial Losses from Attacks Climb for Third Year in a Row, Computer Security Institute (April 7, 2002), http://www.gocsi.com/press/20020407.html.

[26] *See, e.g.,* Richard P. Salgado,*Working with Victims of Computer Network Hacks,* U.S. Department of Justice – U.S. Attorney's Bulletin (March, 2001), http://www.usdoj.gov/criminal/cybercrime/usamarch2001_6.htm.

and by providing educational opportunities for both. These aspects of this new approach emphasize training and preparation as tactics businesses can use to frustrate the efforts of would-be criminals; aside from the fact that they focus on cybercrime, they are novel only with regard to the intensity and sophistication of the efforts involved. The novel aspects of this approach lie not in its efforts to prevent cybercrime but in how it structures the reaction to a completed cybercrime.

Like the traditional model, this approach assumes that aw enforcement reaction to a completed cybercrime is an essential requirement for maintaining social order. Both assume that law enforcement's investigating, identifying, apprehending and prosecuting perpetrators promotes the goal of maintaining order by incapacitating them, discouraging other, would-be perpetrators, satisfying society's desire for retribution and reinforcing the societal understanding of what is, and is not, acceptable behavior. Unlike the traditional model, however, this approach involves the private sector in the process of reacting to a completed "crime." So far, private sector involvement is limited to two aspects of this process, both of which are discussed below.

A. Reporting

The first aspect deals with the reporting of cybercrime. In an effort to encourage reporting by commercial victims, the collaborative approach gives them more options. Under the traditional model of law enforcement, victims report their victimization, law enforcement investigates, and the process is set in motion; victims can, and do, decline to cooperate in a prosecution, which can mean that no charges are brought against an offender. This is not uncommon in domestic violence cases, for example. In the civil justice system, no case is brought except at the behest of, and through the dedicated efforts of, the injured party, i.e., the plaintiff. In the civil system we leave the decision whether to seek redress entirely to the victim; the injury is regarded as a private matter, one in which the state has no interest. In the criminal justice system, on the other hand, once a victim reports a "crime" to the authorities, his or her role essentially becomes that of witness; the "harm" inflicted by the perpetrator is considered to be a "harm" against the state, and it is the state that chooses to seek redress.

How is this relevant to the way the collaborative approach deals with cybercrime? It is relevant because this approach changes the dynamic involved in "reporting" such a crime. Under the traditional model, a victim has two choices: report or do not report. As noted above, commercial cybercrime victims are often reluctant to report cybercrime for fear of the effects the publicity attendant upon an investigation and prosecution will have on their business operations. The collaborative approach addresses this by giving them another alternative. The alternative is predicated, as is the approach, upon establishing close working relationships between the law enforcement officers who are charged with responding to cybercrime and members of the local business community. One purpose of this relationship is to facilitate the educational processes described above; another is to foster a climate of trust in which commercial cybercrime victims can, in effect, consult with law enforcement about the circumstances of their victimization and what response is appropriate. An essential component of this relationship is that law enforcement agrees to hold the information that results from such a consultation in confidence, at least to some extent; the understanding between the two is that law enforcement will not initiate a "public" investigation heading toward prosecution without discussing the matter with the victim and, perhaps, obtaining the victim's consent to such action.

How does this consultative "reporting" arrangement benefit the parties to the relationship? The commercial victim can contact law enforcement, obtain its assistance in ensuring that the vulnerability which gave rise to the cybercrime has been addressed and discuss the possibility of prosecution with knowledgeable officers without, however, having to give up control over the decision as to whether or not a public prosecution will be brought. Law enforcement benefits because it obtains important information about the occurrence of a new cybercrime, including the nature and incidents of the offense; this can be used in responding to other, similar incidents. This information can also be used to prevent further incidents; law enforcement can, without identifying the "reporting" victim, notify other potential victims of the occurrence and details of this offense and encourage them to take measures to protect themselves from being victimized. This in effect achieves specific deterrence by preventing the individual who was responsible for the completed cybercrime from is cybercrime from victimizing others.

While this approach seems to resolve the reluctance commercial victims display to report cybercrime under the traditional model, it also raises some interesting policy issues. For one thing, it means that members of the private sector essentially control the decision whether or not an offender will be prosecuted for her crimes (assuming she can be apprehended). Of course, members of the private sector do precisely that, in a *de facto* sense, under the traditional mode when they decide whether or not to report a cybercrime. And what is undesirable about giving the victim of a cybercrime the ability to decide whether the perpetrator will be prosecuted? As noted above, we do precisely this in the civil justice system; no civil case arises unless an aggrieved party initiates it.

Requiring that criminal prosecutions be brought by the state instead of by victims assumes there are significant differences between the rationales for and circumstances addressed by the civil and criminal justice systems, respectively. If such differences exist, perhaps they go to the nature of the "harms" each system addresses: If someone who is injured in a traffic accident elects not to sue the driver of the other car, we regard that as a private matter between those individuals. But if someone uses an explosive device to injure another, we regard that as a matter of much greater societal import, one that is too important to be left to the individual victim's discretion.[27] But why do we treat the cases differently, when for centuries they were treated the same? If "harm" is the differentiating factor, how does the deliberate use of an explosive device to inflict injury produce a "harm" that sufficiently exceeds that resulting from an inadvertent injury to require action by the state? What, in other words, is the state's interest in the deliberate infliction, or the deliberate attempt to inflict, certain types of "harm?"

The state's interest lies neither in the magnitude of the "harm," as such, nor in the motivations for its infliction but in the potential the infliction of certain types of "harm" has for the maintenance of public order and safety. The function of criminal law is to maintain an acceptable level of order within a society. It does this by establishing prohibitions that are designed to maintain the integrity of certain vital interests: the safety of persons; the security of property; the stability of the government; and the sanctity of certain moral principles.[28] No society can survive if its constituents can without recourse harm each other, appropriate each other's property, undermine the political order and flout moral principles the citizens hold dear. Every society will therefore proscribe "crimes" against

[27] *See, e.g.,* IV William Blackstone, Commentaries on the Laws of England 5.

[28] *See, e.g.,* ANDREW ASHWORTH, PRINCIPLES OF CRIMINAL LAW 11 (1991).

persons (e.g., murder, rape); “crimes” against property (e.g., theft, arson); “crimes” against the state (e.g., treason, rioting); and “crimes” against morality (e.g., obscenity, defiling a place of worship). Every society will also seek the most effective means of enforcing these proscriptions.

For centuries, the enforcement of these proscriptions was left to the victim. By the mid-nineteenth century, the victim had been replaced by the state, which claimed the sole right to seek justice from those who violated its criminal law. Why did this shift occur? And what can it tell us about the future enforcement of criminal proscriptions?

In a thoughtful work, Philip Bobbitt traces the historical evolution of the “state” from the princely states that emerged in the fifteenth century through the appearance of the nation-state in the nineteenth century.[29] The evolutionary process that resulted in the appearance of the nation-state is far too complex even to be summarized here, but it is useful to note certain aspects of this process. One important element is territory; as states evolve in power and sophistication, territory assumes in increasing importance. Indeed, an essential characteristic of the more evolved forms of the state is that each claims exclusive authority over a particular geographical territory. This authority takes two forms: preserving the physical integrity of the territory against potential intrusions by other states; and preserving internal order within the territory. As to the latter, the evolving incarnations of the state each assume varying degrees of responsibility for maintaining internal order; the older systems of criminal justice in which the enforcement of criminal proscriptions was consigned to the victim reflect earlier conceptions of the state’s role with regard to this task. Each successive incarnation of the state assumes greater responsibility for maintaining internal order, a process that culminates with the rise of the nation-state in the nineteenth century. The defining characteristic of the nation-state is its commitment to guarantee the security and prosperity of its citizens; by making this commitment, the nation-state agrees to assume responsibility for the various tasks required to implement this guarantee.

This explains why a process that culminated in the nineteenth century resulted in shifting the responsibility for enforcing criminal proscriptions from the victim to the state. In pre-state forms of social organization, authority is relational, not institutional; members of such a society derive whatever authority they possess from the positions they occupy relative to other members of that society.[30] Since authority is decentralized, individuals must vindicate “harms” inflicted upon them by other members of the society; no central authority has emerged to assume this task. As the state evolves, authority becomes increasingly centralized; that process eventually culminates in the rise of the nation-state which, as part of asserting its authority over the territory it controls and those who reside therein, assumes total responsibility for maintaining internal order by enforcing criminal proscriptions.[31] This, then, accounts for the shift we have seen in the enforcement of the criminal law, from an older system in which enforcement lay entirely with the victim to the current system in which the state monopolizes the enforcement of local criminal law.

[29] *See* Philip Bobbitt, The Shield of Achilles: War, Peace, and the Course of History 75-205 (2002).

[30] *See* Bobbitt, The Shield of Achilles: War, Peace, and the Course of History, *supra*, at 75-95.

[31] *See* Bobbitt, The Shield of Achilles: War, Peace, and the Course of History, *supra*, at 144-204.

What, if anything, does all this tell us about the advisability of giving commercial victims of cybercrime the ability to decide whether or not an offender will be prosecuted? So far, all we have seen is two zero-sum systems, i.e., a victim-prosecution system and a state-prosecution system. Does this mean that the emerging collaborative approach to commercial cybercrime must evolve into a victim-prosecution system?

It does not, for reasons we can again derive from Professor Bobbitt's study of the evolution of the state. He asserts that we are seeing the decline of the nation-state due to the combined effects of various forces, including cyberspace, which make territorial boundaries irrelevant. [32] As territorial boundaries become irrelevant, nation-states can no longer protect their citizens from internal and external threats; since this is their basic reason for existing, nation-states disappear, to be replaced by a new, more adaptive form of the state – the market-state.[33] The market-state differs from the nation-state in various respects, one of which is particularly relevant to this discussion. According to Bobbitt, the market-state will emphasize public-private collaboration in discharging the various functions that have heretofore been monopolized by the state.[34]

This, therefore, explains why the collaborative approach described above has emerged as a strategy for combating cybercrime that is directed at commercial entities. It is the product of an implicit recognition that the traditional model of law enforcement, which is a product of the nation-state, cannot deal effectively with cybercrime and that a new model is needed. Like the model that came before, this model will evolve along with the new, market-state; and because this evolutionary process is still in its infancy, it is impossible to predict precisely what form the new model will take.

It is, however, possible to outline the general strategy it will employ, as aspects of the strategy are evidence in the collaborative approach described earlier. The primary difference between the model that will evolve from the collaborative approach and the traditional model of law enforcement is that, while the former will retain the practice of reacting to completed cybercrime, it will put primary emphasis on preventing cybercrime. Prevention assumes paramount importance because we can no longer routinely assume that an effective reaction to a completed cybercrime is possible. But prevention is not something that can be consigned exclusively or even primarily to law enforcement; if commercial cybercrime is to be prevented, businesses must assume the responsibility, alone and working in conjunction with law enforcement, to make their computer systems and operations as secure as possible. And a critical part of this process is the sharing of information about consummated attacks, i.e., completed cybercrimes; once they learn the details of how another business was victimized, companies can take steps to prevent the same tactics from being used against them. This is a new form of reacting to crime, one that is undertaken primarily by the victim, rather than by law enforcement. But law enforcement also plays a role in this process. Companies are reluctant to publicize their victimization by cybercriminals for fear of the impact this information will have upon their respective clienteles; the collaborative approach addresses this by letting them share the information with law enforcement on the condition that it not be made public without their consent. Only law enforcement can share this information with other businesses,

[32] *See* Bobbitt, The Shield of Achilles: War, Peace, and the Course of History, *supra*, at 213-228.

[33] *See* Bobbitt, The Shield of Achilles: War, Peace, and the Course of History, *supra*, at 228-242.

[34] *See id.* at 235-238.

suitably anonymized, if this is necessary to alleviate the victim company's fears that its competitors might utilize the information to its detriment or that it might otherwise harm the company's interests.

In sum, there is no logical or doctrinal reason why victims of cybercrime cannot be given the power to decide whether or not the offense committed against them should result in a formal prosecution. Victim-driven prosecution was established practice not so long ago; giving cybercrime victims this power does not, however, mean a return to the days when victims were solely responsible for investigating an offense, apprehending the perpetrator and funding the costs of prosecution. It means we adopt a new, more flexible system that is responsive to the distinct issues commercial cybercrime presents. Giving these victims control over (or input into) the decision to prosecute promotes information-sharing and cooperation among businesses and between business and law enforcement, both for the purposes of preventing cybercrime and reacting (formally and informally) to completed cybercrimes. Giving them this power also fosters a relationship between the groups that can result in other forms of collaboration in the battle against cybercrime.

B. Assisting

As noted above, the collaborative approach, which seems to represent a new model of law enforcement, so far includes private sector involvement in two aspects of the process of reacting to cybercrime. One is the reporting of cybercrimes. The other is the investigative process that has heretofore been conducted by law enforcement.

Of the two, private sector involvement in the investigative process is the least problematic, since it does not require re-evaluating a basic assumption of the criminal justice process. One form this involvement takes is that a commercial entity that has been victimized by cybercriminal assists law enforcement officers with their investigation of that offense. A victim company might, for instance, provide law enforcement officers with the computer hardware, software or even technical expertise they need to execute a computer search warrant. There is nothing novel in the notion that law enforcement can seek technical expertise from members of the private sector. Federal and state statutes specifically authorize this,[35] and courts have approved of the practice.[36]

Legal issues might, however, arise with regard to seeking such assistance from the victim of the crime being investigated. The statutes noted earlier, and much of the case law in this area, all antedate the rise of cybercrime and therefore contemplate private assistance of a type unlike that described above. For the most part, these authorities assume that the police should be allowed to call upon those having special expertise to assist them in executing a search warrant. A classic example is law enforcement's seeking assistance from employees of a telephone company to install a pen register or wiretap.[37] As this example suggests, what is common in most of these cases is that they involve law enforcement's obtaining assistance from a disinterested

[35] *See* 18 U.S. Code § 3105. *See also* Va. Code § 19.2 – 56.

[36] *See, e.g.,* United States v. Clouston, 623 F.2d 485, 486 (6th Cir. 1980).

[37] *See, e.g.,* United States v. Guglielmo, 245 F. Supp. 534, 535 (N.D. Ill. 1965).

third party with particular expertise. Depending on the facts at issue, the target of a search warrant that was executed with assistance provided by the victim of a cybercrime might claim that the search was invalid because the victim's agents deliberately exceeded the scope of the warrant, perhaps in an effort to locate proprietary information that could be of use to the victim company or to find evidence of unlawful activity not encompassed by the warrant. The target of such a search might also contend that involving a victim or victim's agents in executing a warrant against a rival company represents, in effect, a conflict of interest and should not be allowed.[38] It remains to be seen how a court would resolve claims such as these. It is clear, though, that merely involving the victim in the execution of a search warrant does not, per se, render the search unlawful.[39] Indeed, the practice of involving the victim dates back to common law, when officers were required to bring the victim of a theft along to identify her stolen goods.[40]

Providing assistance with the execution of search warrants does not exhaust the private sector's involvement in investigating cybercrimes. Businesses routinely conduct internal investigations into suspicious activity; if these investigations are conducted for the purpose of determining the propriety of an employee's actions as an employee, they do not trigger the constitutional standards that govern the actions of law enforcement officers. They do not, for instance, trigger the application of the Miranda doctrine or the Fourth Amendment's prohibition on unreasonable searches and seizures.[41] These and other constitutional protections only apply to the actions of law enforcement officers *or* to the actions of private citizens who are acting as agents of law enforcement.[42] This is where the potential difficulty can arise: If a company becomes aware that an employee may be using its computer facilities for illegal purposes, it will investigate the employee's actions. If, as noted above, the investigation is conducted purely as an internal matter, i.e., to determine whether the employee should be discharged or even, perhaps, civilly sued for the damage he has caused, this would not trigger the constitutional principles that govern the conduct of official, criminal investigations. But if the company, at the beginning of the investigation or while it is still in progress, decides it will gather evidence which it will give to the police so that the employee will be prosecuted, the company may be acting as an agent of the state and constitutional doctrines may apply.[43] If the company is deemed to have been acting as an agent of the state and, while so doing, violated, say, the Fourth Amendment in the process of gathering evidence, that evidence will be suppressed, which may well mean that a perpetrator goes free, to paraphrase Judge Cardozo, because the "employer blundered."[44]

[38] *See, e.g.,* People v. Superior Court (Meyers), 25 Cal.3d 67, 76, 598 P.2d 877, 157 Cal. Rptr. 716, 722 (Cal. 1979).

[39] *See, e.g.,* United States v. Clouston, 623 F.2d 485, 486 (6th Cir. 1980).

[40] *See, e.g.,* Wilson v. Layne, 526 U.S. 603, 611-612 (1999).

[41] *See, e.g.,* State v. Roush, 150 N.C. App. 440, 563 S.E.2d 642 (N.C. App. 2002).

[42] *See, e.g.,* United States v. Douglas, 947 F.2d 951, 1991 WL 216963 *1 (9tth Cir. 199).

[43] *See, e.g.,* United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000).

[44] *See* People v. DeFore, 242 N.Y. 13, 21, 150 N.E. 585, 587 (1926).

The collaborative approach is still in its infancy, even with regard to cybercrimes directed at commercial entities. The rules we have developed, particularly over the last century, to govern the conduct of criminal investigations by law enforcement officers will have to evolve as this new approach evolves. This is not to say that this new approach will or should result in an erosion of the protections against excessive or arbitrary state action that were so carefully and thoughtfully crafted by courts during the twentieth century. We will, though, have to confront many difficult issues as we move toward what might be characterized as a "blended" approach to cyber-security and cybercrime investigations.

V. Conclusion

Cyberspace presents many challenges for the law, both civil and criminal. One of the most critical challenges the law faces is ensuring the enforcement of criminal law in cyberspace. As earlier sections of this article explained, cybercrime differs in several fundamental respects from real-world crime, the type of crime which our existing model of law enforcement was developed to address. As a result, the traditional model is not an effective means of dealing with cybercrime.

There is good reason to believe that we are witnessing the emergence of a new model of law enforcement, at least with regard to cybercrime. While it is far too early to speculate with any specificity as to the eventual form this model will take, it is possible to note several characteristics which will most certainly persist. Because it is the product of an evolutionary process that is changing our basic social order, from the nation-state to the market-state, the new model will necessarily de-emphasize the state's guaranteeing certain rights and protections to its citizens. It will emphasize citizen opportunities and obligations; for cybercrime, this means that we will see the evolution of a system in which citizens and law enforcement officers work together to ensure our collective security from crime, particularly cybercrime.