ARTICLE

TOWARD A CRIMINAL LAW FOR CYBERSPACE: DISTRIBUTED SECURITY

SUSAN W. BRENNER*

TABLE OF CONTENTS

* NCR Distinguished Professor of Law & Technology, University of Dayton School of Law. Email: Susan.Brenner@notes.udayton.edu Website: http://www.cybercrimes.net. The author gratefully acknowledges the contributions to this article made by John Lightfoot, Special Assistant to the Deputy Director of the Federal Bureau of Investigation's Counterterrorism Division. The focus on using assumption of risk to shift the obligation to prevent cybercrime to the users of computer technology arose from a conversation the author had with Mr. Lightfoot in which he cogently argued for the use of such a principle.

I. INTRODUCTION

A set of rules and constraints that shape human action through inducing a particular pattern of human behavior. . . .[1]

Why "a criminal law for cyberspace"? Should cyberspace have its own criminal law? What is it about cyberspace that requires the articulation of a set of distinctive principles governing the imposition of criminal liability?

The simple answer is that cybercrime[2] creates challenges for the extant

---

[1] GRAHAME F. THOMPSON, BETWEEN HIERARCHIES & MARKETS: THE LOGIC AND LIMITS OF NETWORK FORMS OF ORGANIZATION 120 (2003) (listing the features of an "institution").

[2] "Cybercrime" is not a type distinct type of crime, such as rape or murder; "cybercrime" denotes the use of computer technology to achieve illegal ends. *See* Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 CAL. CRIM. L. REV.1 ¶ 12 (2001), *available at* http://boalt.org/CCLR/v4/v4brenner.htm [hereinafter *Virtual Crime*]. "Cybercrime" essentially encompasses two types of unlawful activity. The first consists of conduct that targets a computer or a computer system. Attacks on networks, including hacking, denial of service attacks, and virus dissemination, fall into this category. *See* Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J. L. & TECH. 465, 468-69 (1997). Conduct of this type is usually the subject of "new" criminal prohibitions, even though it is for the most part functionally analogous to prohibited conduct found in the real, physical world. *See Virtual Crime*, *supra*, ¶4.

The second type "cybercrime" consists of using technology to commit traditional crimes such as theft, fraud, and forgery. Here, the perpetrator uses the computer as a tool, in the same way criminals use guns or motor vehicles. *See*, *e.g.*, *Virtual Crime, supra*, ¶12; *see also* Goodman, *supra.*

"Cybercrime" can also denote a third use of computer technology: Computers can play an incidental role in the commission of a traditional offense, such as when a blackmailer uses a computer to generate blackmail letters (or e-mails) or a drug dealer uses a spreadsheet program to track his drug purchases and sales. *See also* Goodman, *supra*. Though scenarios such as these do not represent "true" varieties of cybercrime, they do pose challenges for law enforcement. If nothing else, they contribute to the enormous amount of investigative

model of law enforcement[3] that are already of a severity sufficient to require the development of a new model, one that can address these challenges.[4] Like all models of law enforcement, the current model[5] combines a set of legal principles ("the criminal law") with a repertoire of operational procedures ("police practices") to create the device a society uses in an effort to maintain "order," a concept discussed below.[6]

Because the extant model of law enforcement evolved within a specific historical context, it incorporates certain assumptions about the modes and methods of criminal behavior law enforcement agents will encounter in a given

work that will eventually become part of most, if not all, criminal cases. *See infra* Part III.

[3] As used in this article, "a model of law enforcement" denotes the institutions and processes employed to enforce the criminal law in place in a social system. *See infra* note 6. *See also infra* Parts II(A)(2)(c) and II(B)(2).

[4] *See infra* Parts II and III.

[5] *See infra* Part II.

[6] For an explanation of "order," see *infra* Part II.A.1.

> Any criminal justice system is an apparatus society uses to enforce the standards of conduct necessary to protect individuals and the community. It operates by apprehending, prosecuting, convicting, and sentencing those members of the community who violate the basic rules of group existence. The action taken against lawbreakers is designed to serve three purposes. . . . It removes dangerous people from the community; it deters others from criminal behavior; and it gives society an opportunity to attempt to transform lawbreakers into law-abiding citizens.

THE PRESIDENT'S COMM'N ON LAW ENFORCEMENT AND ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 7 (1967) [hereinafter THE PRESIDENT'S COMM'N].

> [P]olice, prosecutors, courts, and correctional agencies [are] constituent parts of a criminal justice system. . . . [T]heir operations are linked in a specific process: the handling of criminal cases. The process begins with the allegation of a criminal offense, proceeds through an investigation to the arrest of suspects, progresses to the formal charging and prosecution of those arrested, and . . . concludes with the adjudication and disposition of the cases. . . .
>
> This view of the police as the crucial first step . . . meshes . . . with . . . the 'professional law enforcement model' of policing . . . . [T]he fundamental goal of the police is to reduce crime by enforcing the criminal law. They do so largely by arresting . . . offenders. To . . . produce arrests, they rely on three key operations: (1) patrolling public spaces, (2) responding to calls from citizens, and (3) investigating crimes.

Mark H. Moore & Margaret Poethig, *The Police as an Agency of Municipal Government: Implications for Measuring Police Effectiveness*, *in* Measuring What Matters: Proceedings from the Policing Research Institute 151 (Robert H. Langworthy ed., 1999), *available at* http://www.ncjrs.org/txtfiles1/170610-3.txt.

The excerpts demonstrate that a "model of law enforcement" can include not only the processes used to investigate "crimes" and apprehend criminals, but also those used to adjudicate guilt and impose sanctions. The "model of law enforcement" used in this article focuses only on (a) the rules that define behaviors as "criminal" and (b) the processes law enforcement officers use to prevent "crimes" and to pursue and apprehend criminals.

society.[7] Because these assumptions are historically derived, they can diverge from the social realities law enforcement officers actually encounter at a particular moment in time. As the disconnect between one or more of these basic assumptions and experiential reality becomes increasingly apparent, law enforcement personnel will endeavor to have their model updated by incorporating new or revised assumptions, but this can be a slow process.[8] Consequently, the deviation between embedded assumptions and empirical reality is particularly profound when a society is undergoing rapid, pronounced social and cultural changes.[9]

The rise and proliferation of cybercrime is revealing a profound, irreparable deviation between fundamental assumptions that configured the current model of law enforcement and the emerging texture of social reality in the twenty-first century.[10] The deviation is profound because several already apparent characteristics of cybercrime are inconsistent with assumptions that shaped the model's basic operating premises.[11] It is irreparable because these premises

[7] *See infra* Part II.

[8] *See*, *e.g.*, THE PRESIDENT'S COMM'N, *supra* note 6, at 7 ("For example, the American system was not designed with Cosa Nostra-type criminal organizations in mind, and it has been notably unsuccessful to date in preventing such organizations from preying on society")*; see generally infra* Part II.

[9] *See*, *e.g.*, Ken Gormley, *One Hundred Years of Privacy,* 1992 WIS. L. REV. 1335 (1992) (arguing that United States law has employed five different conceptions of "privacy" "with historical jolts or 'catalysts' producing new brands of privacy when existing law is incapable of dealing with unexpected societal and technological changes.").

[10] *See infra* Part III. "Social reality" is the "humanly produced, constructed objectivity" which the members of a given society experience as "real"; s*ee* PETER BERGER & THOMAS LUCKMANN, THE SOCIAL CONSTRUCTION OF REALITY: A TREATISE IN THE SOCIOLOGY OF KNOWLEDGE 51-55 (1966)*; see also infra* Part II.A.2.

This article focuses on the challenges cybercrime poses for law enforcement because cybercrime is, so far, the most commonly encountered variety of technologically mediated crime, i.e., crime that exploits the technologies that are proliferating and/or emerging in the twenty-first century. It is true that many technologies antedate the twenty-first century, and it is equally true that these technologies can be, and have been, exploited for illegal purposes. Telephone fraud, for instance, is a type of technologically mediated crime but neither telephone fraud nor criminal activity exploiting other older types of technology creates the kind of challenges that result from the use of these new technologies. *See infra* Part III.

While the unlawful exploitation of other technologies is in its infancy, it is reasonable to infer that other varieties of techno-crime will create challenges similar to those produced by the use of computer technology. *See infra* Part III. It is, therefore, also reasonable to infer that much of the analysis presented in the text will apply with equal force to as-yet-to-emerge varieties of techno-crime.

[11] *See*, *e.g.*, Susan W. Brenner, *Toward A Criminal Law for Cyberspace: A New Model of Law Enforcement, 30* RUTGERS COMPUTER & TECH. L.J. (forthcoming 2004) [hereinafter *A*

cannot be modified to adapt the current model so it can deal effectively with these aspects of cybercrime.[12] What is needed is a new model of law enforcement, one that is specifically designed to address the challenges of cybercrime.[13]

This is where a "criminal law for cyberspace" comes in. Given the nature of the challenges cybercrime poses for the traditional model of law enforcement, developing a new, cybercrime-adequate model is not simply a matter of devising new police practices. As noted earlier, any model, of law enforcement is based on an array of police practices and a set of legal principles.[14] Devising new police practices is therefore part of the calculus involved in creating a new model, but legal principles which reinforce and implement the approach it takes to wrongdoing must support the model.[15]

Articulating the precise contours of this new, cybercrime-specific model of law enforcement is an undertaking that is quite beyond the scope or ambitions of this article. The article has two goals: to explain how the current model of law enforcement evolved and why a new model is needed; and to outline this new model and explain how criminal law doctrines can be used to implement it. Sections II and III trace the evolution of the current model and describe its limitations as to cybercrime; Section IV sketches the contours of the new model and explains the role "a criminal law for cyberspace" plays in its

---

New Model of Law Enforcement]. This proposition is developed in more detail, *infra* Part III. As Part III explains, a new approach is required for dealing with cybercrime; the current model works satisfactorily with regard to traditional, real-world crime.

[12] *See infra* Part III.

[13] The new model should, with some modifications, be able to address the operational challenges resulting from the exploitation of other new technologies for unlawful ends. *See supra* note 10 and accompanying text.

[14] *See supra* note 6 and accompanying text.

[15] As an example, the model in effect until roughly the middle of the nineteenth century did not include "police practices" because it consigned law enforcement to private citizens.

> Law enforcement in the Founders' time was a *duty* of every citizen. Citizens were expected to be armed and equipped to chase suspects on foot, on horse, or with wagon whenever summoned. And when called upon to enforce the laws of the state, citizens were to respond 'not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities [were] convenient and at hand.' Any person could act in the capacity of a constable without being one . . . . The Founders could not have envisioned 'police' officers as we know them today. The term 'police' . . . was generally used as a verb and meant to watch over or monitor the public health and safety . . . . Only in the mid-nineteenth century did the term 'police' begin to take on the persona of a uniformed state law enforcer.

Roger Roots, *Are Cops Constitutional?,* 11 SETON HALL CONST. L.J. 685, 692-93 (2001) (footnotes omitted) (quoting Barrington v. Yellow Taxi Corp., 250 N.Y. 14, 164 N.E. 726, 727 (N.Y. 1928)); *see also infra* Part III. The law in effect in the colonies and in the early American Republic imposed duties on citizens that derived from an older system, which is described *infra* Part II(B)(2)(b).

implementation. Finally, Section IV presents a brief conclusion.

II. EVOLUTION OF THE CURRENT MODEL

[W]here . . . men live without other security than what their own strength . . . shall furnish them . . . there is no place for industry, . . . no culture of the earth, . . . no arts, no letters, no society . . . .[16]

The current model of law enforcement, like all the antecedent models, is intended to provide a baseline of security in a society, a framework within which human activities, especially those that are essential to the survival and perpetuation of the species, can be conducted confidently and predictably. A law enforcement model is an extrapolation, an operationalization, of a criminal law. The function of criminal law is to maintain an acceptable level of "order" within a society.[17] This is accomplished by defining certain types of behavior, behaviors which threaten essential interests, as intolerable.[18] Merely defining behaviors as intolerable is not, however, sufficient to eliminate them; there must also be processes in place that discourage individuals from engaging in these outlawed behaviors.[19] The sections below consider these two aspects of a law enforcement model – "rules" and "process" – in more detail.

A. Rules

[C]riminal law defines the boundaries of permissible and impermissible conduct for all members of a society governed by the law's geographic jurisdiction . . . .[20]

Criminal law, like all law, is a set of rules.[21] A rule is a compulsory

---

[16] THOMAS HOBBES, OF MAN, BEING THE FIRST PART OF LEVIATHAN, ch. XIII ¶ 9 (1909), *available at* http://www.bartleby.com/34/5/13.html (last visited Nov. 30, 2003).

[17] *See*, *e.g.*, Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace,* 2002 UCLA J. L. & TECH. 3, 56, *available at* http://lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *see also* ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW 5 (3d ed. 1982).

[18] *See*, *e.g.*, Goodman & Brenner, *supra* note 17, at 56. For a discussion of what a social system must do to maintain an acceptable level of internal order, *see infra* Part II(A)(2)(c).

[19] *See infra* Part II(B)(2).

[20] New York CITY CRIMINAL JUSTICE AGENCY, TRENDS IN CASE AND DEFENDANT CHARACTERISTICS, AND CRIMINAL COURT PROCESSING AND OUTCOMES, OF PROSECUTED ARRESTS FOR MISDEMEANOR AND LESSER-SEVERITY OFFENSES IN NEW YORK CITY 1 (2001), *at* http://www.nycja.org/research/reports/fnrpt.pdf.

[21] *See*, *e.g.*, JEROME HALL, GENERAL PRINCIPLES OF CRIMINAL LAW 17 (2d ed.1960)*; see also* BLACK'S LAW DICTIONARY 1028 (rev. 4th ed. 1968) (defining "law" as "[a] rule or method according which phenomena or actions co-exist or follow each other"); *see also infra* note 22.

principle that governs action and inaction;[22] a rule specifies which actions are allowable and which are not.[23] All natural systems – social, biological, physical – operate according a discrete set of rules,[24] and rules are also a constitutive element of artificial systems such as software programs and games.[25] Legal rules differ from other rules found in the natural world in certain respects, one of which is that they have been consciously established according to some process in place in a human society; they are therefore calculated and mutable.[26] Functionally, however, legal rules are analogous to the rules that are the basic component of order in all self-organizing collective systems, whether populated by insects, animals, humans or artificial entities (such as software routines).[27]

---

[22] *See*, *e.g.*, BLACK'S LAW DICTIONARY, *supra* note 21, at 1496 (defining "rule" as "a principle or regulation prescribing or directing action or forbearance").

[23] *See*, *e.g.*, Hugh Baxter, *Autopoiesis and the "Relative Autonomy" of Law,* 19 CARDOZO L. REV. 1987, 2007-08 (1998) (German sociologist Niklas Luhmann describes the legal system as a binary code specifying positive and negative values, i.e., "legal" and "illegal" actions).

[24] *See*, *e.g.*, STEVEN JOHNSON, EMERGENCE: THE CONNECTED LIVES OF ANTS, BRAINS, CITIES AND SOFTWARE 29-40, 53-57 (2001); JOHN H. HOLLAND, EMERGENCE: FROM CHAOS TO ORDER 1-2 (1998); JOHN T. BONNER, THE EVOLUTION OF CULTURE IN ANIMALS 72-92 (1980).

[25] *See*, *e.g.*, JOHNSON, *supra* note 24, at 53-57 (discussing pattern recognition software); Holland, *supra* note 24, at 53-80 (discussing checkers). Some games, like simple board games, do not really conform to the model of self-organizing collective systems advanced in the text above, since they generally only involve a few participants and since each discrete system (each "game") only last for a very short period of time. Structurally, however, more complex games do begin to resemble the model; many online games, for example, involve thousands of players and continue for months or years. *See, e.g.,* Ultima Online, *at* http://www.uo.com/ (online game) (n.d.); Origin Systems, Inc., *at* http://www.origin.ea.com/ (four years after it was launched, Ultima Online has 225,000 players from countries around the world) (n.d.).

[26] *See, e.g.,* ROBERT AXELROD, THE COMPLEXITY OF COOPERATION: AGENT-BASED MODELS OF COMPETITION AND COLLABORATION (1997) (noting evolution from informal norms to formal laws).

[27] *See*, *e.g.*, JOHNSON, *supra* note 24, at 29-40, 53-57 (discussing ants, human cities, software). The concept of self-organizing systems emerged in biology to describe structure, such as ant colonies and schools of fish, in which "pattern and organization develop through interactions internal to the system, that is, without the intervention of external influences such as a 'leader' who directs or oversees the process." See also Scott Camazine, *Self-Organizing Systems*, *in* ENCYCLOPEDIA OF COGNITIVE SCIENCES (n.d.), http://www.cognitivescience.net/s00644.pdf; JOHNSON, *supra* note 24, at 17-20.

> Consider the collective movement of a school of fish. The school snakes through the water like a single entity, turning in unison, waves of activity flashing across the shoal. This group-level behavior is not encoded within each individual, nor is there a leader or small group of individuals directing the movement of the school. It is a process

> whereby individual fish react to movements of their immediate neighbors, and, as a result of such local interactions, the group level pattern of activity emerges spontaneously . . . in short, the school is self-organized.

Carl Anderson, *Self-Organization in Relation to Several Similar Concepts: Are the Boundaries to Self-Organization Indistinct?,* 202 BIOL. BULL. 248 (2002), *at* http://www.isye.gatech.edu/~carl/papers/BoundariestoSO.pdf. The principle of self-organization (or "emergent behavior) has since evolved to encompass a variety of systems, including human societies and organizations.

> What features do all these systems share? . . . They are bottom-up systems, not top-down . . . . [T]hey are complex adaptive systems that display emergent behavior . . . . [A]gents residing on one scale start producing behavior that lies one scale above them: ants create colonies; urbanites create neighborhoods; simple pattern-recognition software learns how to recommend new books. The movement from low-level rules to higher-level sophistication is . . . l emergence.

JOHNSON, *supra* note 24, at 18. *See also* THOMPSON, *supra* note 1, at 129-35. This Article uses the phrase "self-organizing *collective* systems" to emphasize its focus on systems that are made up of many (tens, hundreds, thousands, millions of) discrete parts, each of which has the ability to act autonomously, at least within certain boundaries. *See generally* M. Luck, et al., *Autonomy: Variable and Generative, in* AGENT AUTONOMY 9-22 (H. Hexmoor, C. Castelfranchi & R. Falcone, eds. 2003), *available at* http://www.ecs.soton.ac.uk/~mml/papers/autonomy03.pdf. Later sections of the article use the terms "society" and "social system" to denote self-organizing collective systems comprised of human beings.

A "system" is a "group of interacting, interrelated or interdependent elements" that form a complex whole. AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2001), *available at* http://www.bartleby.com/61/12/C0611200.html [hereinafter AMERICAN HERITAGE DICTIONARY].

> [T]he notion of system appears . . . to require the uniting . . . of a set of elements . . . . These elements may be not only of a very different nature, between one system and another, but also of a different nature within a single system. Moreover, it is perfectly possible for these elements themselves to constitute subsystems, uniting in their turn more elementary entities . . . . The notion of system therefore appears to imply the existence of specific relations between these elements and not their simple juxtaposition; it supposes . . . the existence of an ordered or organized totality: that is, the existence of bonds of interdependence, interaction, and solidarity among the system's components. Thus, at this level the central idea is that of *order* or *organization.* Finally, the notion of system appears to imply . . . unity . . . . [U]nity . . . involves both . . . differentiation from the exterior and . . . identity, which makes it possible to determine both the elements that belong and those that do not belong . . . . This unity . . . is based . . . on . . . principles governing the relations among the . . . constitutive elements . . . . The essential idea . . . is therefore that of *structure.*

Michael van de Kerchove, The Legal System Between Order and Disorder 5-6 (1993) (notes omitted). A simple system is composed of only a few elements; complex systems are composed of many elements. *See*, *e.g.*, JOHNSON, *supra* note 24*,* at 47-48. *See also* van de Kerchove, *supra*, at 5-6.

The elements, or agents, that comprise a system can be autonomous or non-autonomous. *See infra* Part II(A)(2). A non-autonomous agent "either depends on others or is an automaton"; an autonomous agent can, but need not depend on others. *See*, *e.g.*, Luck, et.

1. Order

"Order" is the state for which all such systems strive, because without it those systems do not (and cannot) exist. Order is the subjugation of chaos; it means that a sufficient measure of control has been established over the environment within which a system operates and the individual entities who comprise it, so that the latter can successfully discharge the tasks necessary for the perpetuation of the system.[28] If a self-organizing collective system is to survive, it must, at a minimum, ensure the continuity of a populace of the entities of which it is comprised. For biological systems, this means ensuring (a) that its constituent entities have the necessities (e.g., food, water, shelter) they need to survive and to reproduce themselves; (b) that their offspring achieve adulthood and are successfully incorporated into the system; and (c) that these discrete entities and the system itself are protected from the depredations of competitors and predators.[29]

---

al., *supra* note 27. An autonomous agent has the capacity to choose between two courses of action, even if the choices involve a very low level of abstraction. *See, e.g.,* Bertil Ekdahl, *How Autonomous Is an Autonomous Agent?* (2001), *available at* http://www.cs.lth.se/home/Bertil_Ekdahl/publications/HAisanAA.pdf. *See also infra* Part II(A)(2). The capacity for autonomous behavior is typical of, though not exclusive to, systems populated by biological entities. An ant, for example, can act autonomously in carrying out a set of basic behaviors the instructions for which are genetically programmed; specific behaviors are triggered by environmental conditions, pheromonal signals and, in some species, at least, tactile communication with other ants. *See*, *e.g.*, BONNER, *supra* note 24, at 77-86 (1980). *See also* Johnson, *supra* note 24, at 30-33, 73-80; EDWARD O. WILSON, SOCIOBIOLOGY: THE NEW SYNTHESIS 397-415 (2000). The ant is not acting independently, that is, is not exercising individual judgment and deciding what its next action should be. It is acting autonomously in the sense that it can modify its behavior if circumstances so require. *See infra* Part II(A)(2).

[28] *See*, *e.g.*, AMERICAN HERITAGE DICTIONARY, (defining "order" as "[a] condition of methodical or prescribed arrangement among component parts such that proper functioning or appearance is achieved"); *cf.* MERRIAM-WEBSTER ONLINE DICTIONARY (10th ed.), *at* http://www.m-w.com [hereinafter MERRIAM-WEBSTER] (defining "chaos" as "a state of things in which chance is supreme").

[29] *See*, *e.g.*, WILSON, *supra* note 27, at 37-62. Systems populated by artificial entities must also ensure the continuation of the entities of which they are comprised. The steps they take to accomplish this may, however, differ from those that are characteristic of systems populated by biological agents. Systems populated by artificial entities will no doubt find it necessary to replace members of their population (as they fail or become hopelessly outdated), but the replacement process will presumably not include a period of maturation and socialization comparable to that required for biological entities. *See*, *e.g.*, JOHNSON, *supra* note 24, at 58-63 (describing the evolution of software able to simulate the trail navigation abilities of ants). The conditions stated are the threshold requirements for the sustainability of biological systems composed of non-intelligent entities. As explained

Order therefore has both an internal and an external component. Internal order governs the constituent entities' activities and relationships with each other and their relationships with the system as a whole. To define and maintain internal order, systems must therefore implement rules which define these activities and relationships so that, for instance, an ant knows whether it is a worker or a soldier, whether its default function is to gather food or wage war.[30] External order governs a system's relationship with its environment; "environment" includes both the physical context within which a system functions and biological agents who can threaten its survival by directly attacking its constituent entities or by competing with them for food.[31] Every system will therefore implement rules that structure its interactions with the environment; ant colonies, for example, have rules governing the conduct of war with other colonies and the process of relocating colonies and founding new colonies.[32] The rules that structure internal and external order do not operate independently; instead, they interact and evolve, allowing the system to adapt to changes in its environment.[33]

---

below, the rise of intelligence adds an additional requirement to this list.

[30] *See*, *e.g.*, WILSON, *supra* note 27, at 399 (discussing three basic castes found in ants: queen, worker and soldier); *see also* BONNER, *supra* note 24, at 82-26 (castes among ants and other social insects). Environmental triggers can cause social insects to manifest behaviors other than those that are their basic assignment. *See*, *e.g.*, JOHNSON, *supra* note 24, at 30-31 (describing how, among harvester ants, interior workers will carry their queen to the colony's "escape hatch" at the first sign of disturbance).

[31] *See*, *e.g.*, WILSON, *supra* note 27, at 245 (describing strategies Scottish ant colonies use to obtain the "warmest nest sites," i.e., gradual encroachment on a competitor's nest, occupation of sites abandoned by competitor colonies and siege warfare). While this is, so far, less common, the same dynamic can be found among non-biological agents; artificial entities comprising one system can either attack the members of another system or compete with them for necessary resources. *See generally* JOSHUA M. EPSTEIN & ROBERT L. AXTELL, GROWING ARTIFICIAL SOCIETIES: SOCIAL SCIENCE FROM THE BOTTOM UP (1996). *See also* Gordon Christopher Zaft, Social Science Applications of Discrete Event Simulation: A DEVs Artificial Society (2001) (unpublished M.S. thesis, The University of Arizona), *at* http://www.zaft.org/gordon/XeriScape/Thesis.pdf. The discussion in the text uses biological examples because the vast majority of our experience is with biologically-based systems.

[32] *See*, *e.g.*, WILSON, *supra* note 27, at 245 (discussing war among ant colonies) and 139-42 (discussing creation of new ant and termite colonies).

[33] *See, e.g.,* Michael Schillo, et al., Self-Organization in Multi-Agent Systems: From Agent Interaction to Agent Organization, *in* PROCEEDINGS OF THE THIRD INTERNATIONAL WORKSHOP ON MODELLING ARTIFICIAL SOCIETIES AND HYBRID ORGANIZATIONS 37 (2002), *at* http://www.ki.informatik.hu-berlin.de/~lindeman/Masho-rcsia-etp-proceedings.pdf:

> [T]heoretical approaches . . . call any kind of system self-organizing if it is able to determine its internal structure by itself as the environment changes. The boundaries of a self-organizing system and its structure . . . are not determined by environmental factors. Rather, these systems generate, change and adapt their internal organization within their own logic in a dynamic process to cope with environmental changes.

Rules are an absolute necessity for the emergence of self-organizing collective systems.[34] Without rules to order activities and relationships, there is no "system". There is, at best, a shifting congeries of entities, totally lacking coherence and function.[35] But while rules are a constant, the ways they manifest themselves are not. As the section below explains, intelligence very much influences the types of rules that emerge and the ways in which they are implemented.

2. Intelligence

The most direct control on the behavior of a biological system is the knowledge stored in its genes.[36]

As explained above, rules are an essential aspect of all self-organizing collective systems, whether they are populated by biological or artificial life-forms.[37] At a very basic, constitutive level, rules operate equivalently in all such systems, regardless of the characteristics of the entities that comprise them; rules establish the baseline of order without which no system can come

[34] *See, e.g.,* ALBERT K. COHEN, DEVIANCE AND CONTROL 3 (1966).

> [I]f human beings are to do business with one another, there must be rules, and people must be able to assume that, by and large, these rules will be observed. Whatever people want – food, clothing, shelter, sex, fame, contract bridge – they must get it by working with and through other people. They must take up positions in organized and complex social enterprises: families, clubs, schools, armies, political associations, ball teams. Each of these may be thought of as a way of fitting together the diverse actions of many people so that the work of the world gets done. But if the actions of many people are to be fitted together, there must be understandings about who is supposed to do what and under which circumstances . . . . [T]he first prerequisite to organized human activity is that there be *some* understandings, however arbitrary they may be. For example, if traffic is to move along the highway, it is less important whether the rule prescribes that people must drive on the right-hand side or the left-hand side of the road then that there be a rule. The alternative is chaos.

Id (emphasis in the original). *See also infra* Part II(A)(2)(c). Even the aggregation of slime mold cells into colonies, which represents one of the simplest forms of a self-organizing collective system, follows certain rules. *See, e.g.,* JOHNSON, *supra* note 24, at 12-17 (citing slime mold cells as an example of how "simple agents following simple rules" can "generate amazingly complex structures); *see also* WILSON, *supra* note 27, at 387-92.

[35] *See, e.g.,* JOHNSON, *supra* 24, at 120-21

> The intelligence of a harvester ant colony derives from the densely interconnected feedback between ants that encounter each other and change their behavior according to pre-ordained rules. Without that feedback, they'd be a random assemblage of creatures butting heads and moving on, incapable of displaying the complex behavior that we've come to expect . . . .

[36] Francis Heylighen & Donald T. Campbell, *Selection of Organization at the Social Level: Obstacles and Facilitators of Metasystem Transitions*, 45 WORLD FUTURES: THE J. OF GEN. EVOLUTION 181 (1995), *available at* http://pespmc1.vub.ac.be/Papers/SocialMST.pdf.

[37] *See infra* Part II(A)(1).

into existence and survive.[38] At a higher level of organizational extrapolation, rules function differently in various systems; and the critical factor in differentiating the functioning of rules in self-organizing collective systems is the intelligence of the entities that populate the system.[39]

"Intelligence" is difficult to define; it is an elusive concept, one that has spawned many definitions.[40] Certain elements, though, are consistent, such as the ability to make decisions, i.e., to consider two (or more) alternatives and deliberately elect to pursue one of them.[41] Definitions of intelligence also emphasize that an entity's decision to choose a particular alternative is the result of reasoning, i.e., the cognitive application of knowledge that the entity has acquired by learning from previous experience.[42] An intelligent entity,[43]

---

[38] *See infra* Part II(A)(1).

[39] *See generally supra* note 27.

[40] *See, e.g.,* THOMAS M. GEORGES, DIGITAL SOUL: INTELLIGENT MACHINES AND HUMAN VALUES 58, 58 (2003)

> [I]t is useful to recognize as intelligent certain kinds of *behavior,* regardless of the package it comes in—be it human, animal, . . . or machine. We recognize that intelligent behavior is multidimensional, that is, not measurable along a single . . . scale. We distinguish between linguistic, mathematical, musical, kinesthetic, spatial, logical, interpersonal, and emotional intelligence, to name a few.

See also John McCarthy, *What Is Artificial Intelligence?,* (2001), *at* http://www.kurzweilai.net/articles/art0088.html?printable=1 ("Intelligence is the computational part of the ability to achieve goals in the world. Varying kinds and degrees of intelligence occur in people, many animals and some machines.").

[41] *See generally supra* note 27.

> The ability to make decisions is essential to intelligent behavior. Indeed, the word *intelligent* comes from the Latin roots *inter* (between) + *legere* (to choose). We thus assume that there is only one essential characteristic of intelligence in man or machine – an ability to choose between alternatives.

W.C. Stirling & R.L. Frost, *Intelligence with Attitude*, *in* Nat'l Inst. of Standards and Tech., Proc. of the Perf. Metrics for Intelligent Sys. Workshop (2000) *available at* http://www.isd.mel.nist.gov/research_areas/research_engineering/PerMIS_Workshop/Part%20II_Section%201.pdf.

[42] *See, e.g.,* Jane M. Packard, *Social Behavior*, *in* ECOLOGY AND BEHAVIOR OF THE WOLF (L.D. Mech & L. Boitani, eds., 1998) *available, at* http://canis.tamu.edu/wfscCourses/Concepts/Packa98.html ("Intelligence is the ability to apply knowledge from previous experience to solving novel problems"); *see also Measuring Performance and Intelligence of Systems with Autonomy: Metrics for Intelligence of Constructed Systems,* Nat'l Inst. of Standards and Tech., Proc. of the Perf. Metrics for Intelligent Sys. Workshop § 1.4 (2000), at http://www.isd.mel.nist.gov/research_areas/research_engineering/PerMIS_Workshop/Part%20I%20White%20Paper.pdf; Soar Technology, Inc., *Soar: A Functional Approach to General Intelligence*, *at* http://www.eecs.umich.edu/~soar/docs/SoarFunctionalOverview.pdf (2002).

[43] While we tend to associate "intelligence" with an "individual," i.e., a discrete

therefore, is one that can act on its own – one that can make decisions and manifest autonomous behavior on some level.[44] This definition implies the existence of a residual category – i.e., a non-intelligent entity – insofar as it assumes intelligence is a zero sum commodity. This assumption is at once valid and not valid.

At one level, biological and artificial entities can be divided into "intelligent" and "non-intelligent" species. Slime mold cells and other microorganisms, for example, are not "intelligent" under the definition given above, nor are the routines that populate most software programs.[45] While they exhibit self-organizing behavior, slime mold cells and other microorganisms are not "intelligent" under this definition because their behavior is driven by instinct,[46] not by individual choice based on reasoning and learning. Similarly, most artificial entities are not "intelligent" because their actions are driven by code that programs their behavior.[47] Humans and higher primates, on the other hand, are clearly "intelligent" under this standard[48] (which is not surprising, since it is a human definition and a human concept).[49] But as we move beyond simple dichotomies and consider the gradations of behavior found in more

organism, some species exhibit a collective intelligence. *See infra* notes 58-62 and accompanying text.

[44] *See, e.g.,* Gregory J. Smith & John S. Gero, *The Autonomous, Rational Design Agent, in* WORKSHOP ON SITUATEDNESS IN DESIGN: ARTIFICIAL INTELLIGENCE IN DESIGN 19-23 (H. Fujii, ed. 2000), *available at* http://www.arch.su.edu.au/%7Ejohn/publications/2000/SmithGeroAIDWkshp.pdf ("An agent is called autonomous if its beliefs and behaviour are determined from its own experience."); *see also* Intelligent Autonomous Systems, *at* http://www.science.uva.nl/research/ias/ (last visited Nov. 30, 2003) ("The IAS group studies methodologies to create intelligent autonomous systems, which perceive their environment through sensors and use that information to generate intelligent, goal-directed behaviour."); *see also supra* note 27.

[45] *See, e.g.,* WILSON, *supra* note 27, at 382-86; *see also* BONNER, *supra* note 24, at 72-77.

[46] *See, e.g.,* WILSON, *supra* note 27, at 26-27. Professor Wilson defines instinct as an "innate behaviorial difference between . . . two species. . . that is based at least in part on a genetic difference". *Id.* at 26 ("We then speak of differences in the hereditary component of the behavior pattern, or of innate differences in behavior"). He also notes that instinct is "a behavior pattern that . . . is subject to relatively little modification in the lifetime or the organism, or varies very little throughout the population, or . . . both." *Id. See also* BONNER *supra* note 24, at 73; WILSON, *supra* note 27, at 387-93.

[47] *See, e.g.,* Jennifer Golbeck, *Unintelligent Swarming for Robust Exploratory Systems, in* Proc. of the IASTED Int'l Conf. on Automation, Control, and Info. Tech. (2002), *at* http://www.cs.umd.edu/~golbeck/downloads/Swarm02.pdf.

[48] *See, e.g.,* WILSON, *supra* note 27, at 151, 516. *See also*. BONNER, *supra* note 24, at 179.

[49] *See, e.g.,* GEORGES, *supra* note 40, at 58 ("Just as IQ tests have well-known cultural and gender biases, our present thinking about intelligence surely has *species* biases as well.").

complex species, it becomes more difficult to parse "intelligent" and "non-intelligent" entities; ants and reptiles are, for instance, capable of learning and of decision-making.[50] Does this mean they are "intelligent" in the same way humans are "intelligent?" Obviously, it does not: ants and reptiles may be able to learn to make simple choices and elect simple behaviors, but their intelligence is clearly not of the same type or of the same magnitude as that of humans and the higher primates.[51]

At this level, therefore, it is necessary to move beyond the notion of "intelligence" as a zero-sum commodity and approach it as a graduated concept – as a phenomenon that manifests itself in various ways.[52] Professor Edward O. Wilson divides organisms into three categories: the complete instinct-reflex machine (lowest), the directed learner (middle), and the generalized learner (highest).[53] The behavior of organisms in the first category is completely programmed by instinct or reflexive responses to environmental stimuli.[54] Much of the behavior of organisms in the second category is also driven by instinct-reflex; they are capable of some learning, but their learned behavior "is as stereotyped as the most neurally-programmed 'instinct.'" [55] The organisms in the third category have brains,

> large enough to carry a wide range of memories, some of which possess only a low probability of ever proving useful. Insight learning may be performed, yielding the capacity to generalize from one pattern to another

---

[50] *See, e.g.,* JOHNSON, *supra* note 24, at 81 (if ants from an older colony meet ants from a neighbor colony, "the next day they're more likely to turn and go in the other direction to avoid each other."); WILSON, *supra* note 27, at 444 (describing how lizards learned their way through mazes and how to press a bar to obtain more heat for their cages).

[51] *See, e.g.,* GEORGES, *supra* note 40, at 58-59.

We could say . . . that an entity is intelligent to the degree that it

1. stores and retrieves knowledge;
2. learns from experience and adapts to novel situations;
3. discriminates between what is important and what is irrelevant to the situation at hand;
4. recognizes patterns, similarities, and differences in complex environments;
5. creates new ideas by combining old ideas in new ways;
6. plans and manages strategies for solving complex problems;
7. sets and pursues goals;
8. recognizes its own intelligence and its place in the world.

Using these criteria, we would say that an entity is minimally intelligent if it does only (1), for example, and more intelligent the more it is able to do. Dogs, for example, appear to do (1) through (4) reasonably well. *Id. See also id.* at 57-73 (various aspects of intelligence).

[52] *See supra* notes 40 and 51 and accompanying text.

[53] *See* WILSON, *supra* note 27, at 151-52.

[54] *See id.* at 151.

[55] *See id.*

> and to juxtapose patterns in ways that are adaptively useful. Few if any complex behaviors are wholly programmed morphogenetically at the neural level. The process of socialization . . . is prolonged and complex . . . . The key social feature of the grade, which is represented by man, the chimpanzee, baboons, macaques, and . . . other . . . primates . . . , is a *perception of history*. The organism's knowledge is not limited to particular individuals and places with attractive or aversive associations. It also remembers relationships and incidents . . . and it can engineer improvements in its social status by relatively sophisticated choices of threat, conciliation, and formations of alliances . . . .[56]

These hierarchical categories are based on the capacities of individual members of a biological species; individual intelligence conforms to the definition provided earlier, i.e., it is an entity's capacity to engage in autonomous action based upon a process of decision making which, in turn, is predicated upon reasoning and learning.[57] For many species, certainly for mammals, "intelligence" is properly analyzed as an individual phenomenon because the members of these species are functionally discrete entities – "individuals" – who engage in self-directed behavior.[58] For other species,

---

[56] *See id.* at 152.

[57] *See supra* note 44 and accompanying text.

[58] *See supra* note 44 and accompanying text. At the most basic level, an "individual" is a "physically distinct organism." WILSON, *supra* note 27, at 8. This definition serves to differentiate more evolved species – such as insects, amphibians, birds, fish and humans – from simpler biological entities in which the line between "individual" and "colony" blurs. *See id.* at 383-86. It does not, however, address the functional difference between, say, an ant and a human being; each is a "physically distinct organism," but the ant's "individuality" ends there. Unlike a human being, a single ant is not capable of autonomous behavior because, as explained in note 60, *infra,* an ant's behavior is programmed by a series of simple, pre-determined rules, not by individual cognition. *See supra* note 39 and accompanying text (discussing autonomous behavior). While humans, like ants, live in a collective environment, human behavior, unlike ant behavior, is individuated, i.e., the product of idiosyncratic reasoning which takes into account both the circumstances of the empirical world and the realities of the collective environment. *See, e.g.,* Kerstin Dautenhahn, *Evolvability, Culture and the Primate Social Brain, in* PROC. OF THE EVOLVABILITY WORKSHOP AT THE SEVENTH ANN. INT'L CONF. ON THE SIMULATION AND SYNTHESIS OF LIVING SYS. (ARTIFICIAL LIFE) (2000), *at* http://homepages.feis.herts.ac.uk/~nehaniv/al7ev/.

> In primate societies, and different from members of social insect societies, an individual is not only socially situated (being part of and surrounded by a social environment) but also socially embedded which means that the agent needs to pay attention to other agents and their interactions individually. Particularly human primates are specialized in predicting, manipulating and dealing with highly complex social dynamics . . . . Humans, different from social insects live in *individualized societies* . . . .

particularly the social insects, "intelligence" is a collective, not an individual, phenomenon; discrete ants are not "intelligent,"[59] but a swarm intelligence emerges from the interactions of the ants in a colony.[60] The swarm

Id. (citations omitted and emphasis in the original). *See also* W.D. Christensen & C.A. Hooker, *An Interactivist-Constructivist Approach to Intelligence: Self-Directed Anticipative Learning,* 13 PHIL. PSYCHOL. 5 (2000), *available at* http://www.kli.ac.at/personal/christensen/SDAL_PhilPsych.pdf.

[59] *See infra* Part II(A)(3); *see, e.g.,* BRIAN GOODWIN & RICARD SOLE, SIGNS OF LIFE: HOW COMPLEXITY PERVADES BIOLOGY 148 (2000).

> [A]nt colonies constantly adjust the number of ants actively foraging for good, based on a number of variables: overall colony size . . . ; amount of food stored in the nest; amount of food available in the surrounding area; . . . the presence of other colonies in the near vicinity. No individual ant can assess any of these variables on her own . . . . There are no . . . ways to perceive the overall system – and, indeed, no cognitive apparatus that could make sense of such a view.

JOHNSON, *supra* note 24, at 74-75.

[60] *See infra* Part II(A)(3). For a description of how this collective intelligence emerges, *see, e.g.,* JOHNSON, *supra* note 24, at 78-79.

> [T]he statistical nature of an interaction demands that there be a critical mass of ants for the colony to make intelligent assessments of its global state. Ten ants roaming across the desert floor will not be able to accurately judge the overall need for foragers or nest-builders, but two thousand will do the job admirably . . . .
>
> The simplicity of the ant language – and the relative stupidity of the individual ants – is . . . a feature . . . . Having individual agents capable of directly addressing the overall state of the system can be a real liability in swarm logic, for the same reasons that you don't want one of the neurons in your brain to suddenly become sentient . . . .
>
> [A]nt colonies rely heavily on the random interactions of ants exploring a given space without any predefined orders. Their encounters with other ants are individually arbitrary, but because there are so many individuals in the system, those encounters eventually allow the individuals to gauge and alter the macrostate of the system itself . . . .
>
> The primary mechanism of swarm logic is the interaction between neighboring ants in the field: ants stumbling across each other, or each other's pheromone trails, while patrolling the area around the nest. Adding ants to the overall system will generate more interactions between neighbors and will consequently enable the colony . . . to solve problems and regulate itself more effectively.

Ant communication strategies are crude and typically quite limited. *See id.* at 75 (communication between workers in fire ant colonies relies "on a vocabulary of ten signals, nine of which are based on pheromones"). *See also* Deborah M. Gordon, *The Organization of Work in Social Insect Colonies,* COMPLEXITY (2002), *at* http://www.santafe.edu/~cmg/netdyn/.

> [A]n ant's moment-to-moment decision about which task to perform, and whether to perform it actively, depends on its interactions with other workers. Interactions between workers of some task groups apparently provide negative feedback, while others provide positive feedback. It appears that what matters to an ant is the *pattern* of interactions it experiences, rather than a particular message or signal transferred at each interaction. Ants do not tell each other what to do when they meet, but the pattern of interaction each ant experiences influences the probability it will perform a task.

intelligence probably qualifies as "intelligence" under the definition given earlier: It engages in decision making (which is predicated on reaction, not reasoning); it has at least some capacity to learn from experience; and the swarm (but not the constituent entities, i.e., the ants) engages in autonomous behavior.[61] The swarm intelligence differs, though, from the individual "intelligence" found in many of the mammals, especially the primates. This mammalian "intelligence" possesses all the characteristics found in swarm intelligence, but it adds others, including capacities for self-awareness, for invention and innovation, and for planning and strategizing.[62]

This brings us back to the proposition advanced earlier, namely, that while basic rules operate equivalently in self-organizing collective systems, rules that emerge at a higher level of organizational extrapolation operate idiosyncratically, the differentiating factor being the intelligence of the entities that populate the system.[63] To understand why this is true, it is necessary to consider three systems, each populated by agents possessing varying types of "intelligence."[64]

a. Ants

The first system to consider is an ant colony. This colony, like all self-organizing collective systems, must implement rules that establish internal and external order.[65] Establishing internal order requires (a) allocating the ants that inhabit the colony to certain essential tasks (e.g., nest building, food collection, reproduction and nurturing the offspring to maturity) and (b) ensuring that they perform these tasks properly, in a consistent, predictable manner.[66] The colony uses two types of rule-sets to establish internal order: role-allocation and task-performance.[67] Role-allocation rules tell an ant what its function is, i.e.,

---

Each ant uses a set of rules such as, 'I'm a forager and if I meet a returning patroller every so often, I remain likely to go out'.

See generally WILSON, *supra* note 27, at 413-15.

[61] *See supra* notes 41-44 and accompanying text.

[62] *See supra* note 51 and accompanying text.

[63] *See supra* notes 37-38 and accompanying text.

[64] The intelligence levels roughly correspond with the categories discussed above. *See supra* notes 53-56 and accompanying text.

[65] *See supra* Part II(A)(1).

[66] *See id.*

[67] In insect colonies, the system of allocating individuals to perform particular functions is usually referred to as involving "castes," not roles. *See, e.g.,* WILSON, *supra* note 27, at 298-99. This distinction is made because the allocation of tasks in insect societies often reflects physiological differences. *See, e.g., id.* ("In social insects, a caste is any set of individuals of a particular morphological type, or age group, or both, that performs specialized labor in the colony.") Among ants, "[t]here basic physical castes are found . . . all members of the female sex: the worker, the soldier, and the queen." WILSON, *supra* note

whether it is a soldier, a worker or a queen.[68] Task-performance rules give an ant the repertoire of behaviors it needs to carry out its assigned function, such as foraging for food.[69] Task-performance rules also allow ants to shift between functions so that, for example, a worker ant that has been foraging for food may move to nest-building.[70] Ensuring external order involves a similar process.[71] In an effort to protect itself from predators and competing ant colonies, the colony implements (a) role-allocation rules that assign members of the colony to function as soldiers and (b) task-performance rules that prescribe the behaviors soldiers employ in fending off aggressors and/or attacking encroaching colonies.[72]

The ants in the colony do not formulate the rules that govern role-allocation and task-performance, as ants are incapable of such a task.[73] To some extent, the basic rules governing both endeavors are genetically pre-coded.[74] More accurately, the capacity to engage in these behaviors is genetically pre-coded,

---

27, at 399. Males are not usually considered a caste, primarily because they live for such a short time. *See, e.g.,* JOHNSON, *supra* note 24, at 81 (males live for a single day: "Their life span is so abbreviated that natural selection didn't bother to endow them with jaws to eat.") Ant colonies "can live as long as fifteen years – the life span of the egg-laying queen ant, whose demise signals the final death of the colony itself." *Id.* at 80.

[68] *See, e.g.,* Vanessa S. Fraser et al., *Genetic Influence on Caste in the Ant Camponotus Consobrinus,* 47 BEHAV. ECOL. SOCIOBIOLOGY 188 (2000), *available at* http://www.bio.usyd.edu.au/Beelab2/BensPDFs/FraserGeneticInfluenceCaste.pdf.

[69] *See, e.g.,* WILSON, *supra* note 27, at 302 ("The behavior of the ant soldiers is often extremely specialized."); *see also id.* at 301-04. The task-performance rules operate in a fashion analogous to the rules governing moves in a board game, such as checkers. *See, e.g.,* HOLLAND, *supra* note 24, at 33-42 (discussing game theory). That is, they specify the behaviors that are appropriate for an ant assigned to a particular role, or caste; worker ants have a repertoire of behaviors that differs from soldier ants and queens have a repertoire that differs from that of either workers or soldiers. The repertoire of behaviors defines the range of behaviors in which the ant can engage. Ants shift into a new range of behaviors if they move from performing one task to performing another, but in either event the universe of behaviors in which they can engage is delimited, much the way the moves of one playing checkers are delimited. *See supra* notes 59-60.

[70] *See supra* notes 59-60; *see, e.g.,* WILSON, *supra* note 27, at 549 ("As one requirement such as brood care or nest repair intensifies, workers shift their activities to compensate until the need is met, then change back again.").

[71] *See supra* Part II(A)(1).

[72] *See, e.g.,* WILSON, *supra* note 27, at 245 (strategies include encroaching on a competitor's nest, occupying sites temporarily abandoned by other colonies and siege warfare).

[73] *See supra* notes 59-61 and accompanying text; *see also infra* Part II(A)(3).

[74] *See, e.g.,* Kenneth G. Ross & Laurent Keller, *Genetic Control of Social Organization in an Ant,* 100 PROC. NATL. ACAD. SCI. USA 14232 (1998), *available at http://www.pubmedcentral.nih.gov/articlerender.fcgi?tool=pubmed&pubmedid=9826683*.

because the behaviors themselves are triggered by forces external to the ants.[75] Among ants and other social insects, the rules that govern the allocation of functions and the performance of tasks are chemically and environmentally controlled. Environmental conditions affect role allocation and task performance (a) by determining the number of entities a colony can support and (b) by influencing nutrition within the colony.[76] Nutrition affects role-allocation in various ways, not the least of which is the incidence of cannibalism.[77] Chemical signals, though, are primarily responsible for the orchestration of behavior among social insects; ants (like termites, bees, wasps and other social insects) communicate almost exclusively through pheromonal signals.[78] Some of these signals are simple binary codes, indicating, for example, whether another ant is friend or foe, but "ants can also detect *gradients* in pheromones," which is "essential for forming food delivery lines."[79] Pheromonal signals also convey information about tasks, such as whether an ant is foraging for food (and has found a large quantity of food which needs to be collected by other ants) or disposing of dead nest-mates.[80]

The basic constitutive rules that govern role-allocation and task-performance do a marvelous job of establishing order, especially internal order, in ant colonies and other aggregations of social insects. They do this laterally since no one creature is in charge of formulating or implementing the rules or otherwise sees to the creation and continuance of order in colonies populated by ants or other social insects.[81] Order is an emergent phenomenon which emerges from the basic repertoire of rules available to members of the colony. These rules shape the behavior of all members of the collectivity.[82] The rules are for the most part fixed and pre-given; they define the limited

[75] *See, e.g.,* BONNER, *supra* note 24, at 83.

[76] *See, e.g.,* WILSON, *supra* note 27, at 303-09 (analyzing effects of environmental factors upon colony size and function allocation).

[77] *See, e.g.,* WILSON, *supra* note 27, at 85 (discussing cannibalism among social insects). Nutrition can also produce morphological specialization among ants and other social insects. *See, e.g., id.* at 303-09.

[78] *See, e.g.,* WILSON, *supra* note 27, at 413-14*; see also* JOHNSON, *supra* note 24, at 75 ("the great bulk of ant information-processing relies on the chemical compounds of pheromones . . . . Ants secrete . . . chemicals . . . as a means of communicating with other ants.").

[79] Johnson, *supra* note 24, at 76 ("Gradients in the pheromone trail are the difference between saying 'There's food around here somewhere' and 'There's food due north of here.'").

[80] *See, e.g.,* WILSON, *supra* note 27, at 55-56, 413-14; JOHNSON, *supra* note 24, at 765; *see also id.* at 32-33 (ant burial details).

[81] *See, e.g.,* JOHNSON, *supra* note 24, at 29-33, 73-79*; see also infra* Part II(A)(3).

[82] *See, e.g.,* JOHNSON, *supra* note 24, at 29-33, 73-79*; see also infra* Part II(A)(3).

universe of behaviors that are available to colony members.[83] It is true that individual ants have the apparent ability to, in effect, make "choices." It seems that foraging ants that are not following a pre-established pheromone trail "choose" the paths down which they proceed in search of food. But what looks like "choice" to a human being is not; an ant's taking a particular path is not the product of decision making as defined above.[84] The ant does not formulate alternatives and use a process of reasoning, which is based upon a learned store of knowledge and inferences from that knowledge, to select the path that rationally seems the most likely to offer the opportunity to find food. An ant cannot do this because individual ants are not "intelligent."[85] And while this approach might well prove unsuccessful if only one or two ants were searching for food, with hundreds or thousands of ants foraging, some of them are very likely to happen upon food. When this occurs, the lucky forager returns to the colony with the food it can carry. If the site contains more food than it can carry, the forager uses chemical signals to direct other ants to the food source.[86]

In a sense, an ant colony is like a game of chess with thousands of players. Each ant (each "player") has its defined set of behaviors ("moves"), which vary with the ant's role in the system (e.g., worker, queen, soldier). The collaborative activities of the players produce a self-organized collective system which is directed toward achieving certain ends. In a chess game, the ends are the players' amusement and the resolution of a competitive endeavor. In an ant colony, the ends are the survival and perpetuation of the colony and its inhabitants through a collaborative endeavor.

An ant colony and a chess game are functionally analogous in certain respects, one of which is particularly relevant to the issues addressed in this article. The rules of both systems are entirely constitutive: they define what the members of that system can and must do.[87] Chess players must move when it is their turn, utilizing a circumscribed range of alternatives in doing so; the alternatives are prescribed by the rules of the game and depend upon which

---

[83] *See, e.g.,* JOHNSON, *supra* note 24, at 77-79.

[84] *See supra* notes 41-44 and accompanying text.

[85] *See supra* notes 59-61 and accompanying text.

[86] *See, e.g.,* WILSON, *supra* note 27*,* at 55-56, 413-14; JOHNSON, *supra* note 24, at 32-33 (discussing ant burial details).

[87] *See, e.g.,* FREDERICK SCHAUER, PLAYING BY THE RULES: A PHILOSOPHICAL EXAMINATION OF RULE-BASED DECISIONMAKING IN LAW AND IN LIFE 6 (1991):

> [C]onstitutive rules create the very possibility of engaging in conduct of a certain kind. They define and thereby constitute activities that could not otherwise even exist. Rules of games are the archetypes . . . . The rule providing . . . that in order to castle a chess player must not previously have castled does not just control a process but constitutes it. Without the rules of chess you cannot castle at all.

piece (queen, pawn, rook) a player uses.[88] Ants must perform the tasks attendant upon their role (worker, queen, soldier), utilizing a circumscribed set of biologically-defined behaviors in doing so.

How is any of this relevant to the issues under consideration in this article? It is relevant because this functional analogy between chess and an ant colony illustrates what is missing in systems that are organized laterally, according to the principles that structure ant colonies (and chess). What is missing is the capacity for deviant behavior; "deviant behavior" is, essentially, an entity's deliberate failure to follow applicable rules.[89] The behavior of the ants, like

---

[88] *See, e.g., id.* at 7 (noting that constitutive rules can have "regulative" aspects, i.e., can prescribe and proscribe behavior).

[89] *See, e.g.,* COHEN, *supra* note 34, at 12 ("Deviant behavior . . . is behavior that violates normative rules."); EDWIN M. LEMERT, HUMAN DEVIANCE, SOCIAL PROBLEMS AND SOCIAL CONTROL 13 (2d ed. 1972) ("deviance is defined as violations of norms, or departures from social expectancies."); *see also supra* note 34.

The definition given above incorporates the requirement that the failure to follow rules must be "deliberate," that is, the result of "careful thought and thorough consideration." *See* MERRIAM-WEBSTER (defining "deliberate"). A failure to abide by governing rules can be deliberate or unintentional, advertent or inadvertent. If, for example, an ant were to find a morsel of food and take it to the wrong colony, the ant would not have followed the rules that prescribe a foraging ants' conduct; under those rules, foragers find food and bring it back to their own colony. *See supra* note 86 and accompanying text. The ant has failed to follow applicable rules, but the error is more properly characterized as a "deviation" from expected behavior than as deviant behavior.

Why is that the correct characterization? There are two reasons, one context-specific and one general. The context-specific reason derives from the limited capacities of ants. As was explained earlier, an individual ant is not "intelligent" and therefore cannot engage in a process of decision making. *See supra* notes 59-61 and accompanying text. The hapless forager who goes to the wrong colony is, therefore, incapable of having done so "deliberately."

The general reason is found in the tension between order and disorder. As explained above, self-organizing collective systems strive for order because without it they cannot perform the functions that are essential for the survival of the system and its constituent entities. *See infra* Part II(A)(1). In a sense, any entity's failure to follow the constitutive rules of such a system undermines the system's ability to maintain order; the ant's error proves that the rules in place in the hypothesized colony are not perfect. If the imperfection responsible for this ant's default in the performance of her duty were to spread, the colony's ability to maintain order would be threatened and it might well collapse. But little in life (real life, anyway) is perfect; it is therefore reasonable to assume that some level of inadvertent errors will occur in any system. *See, e.g.,* JAMES GLEICK, CHAOS: MAKING A NEW SCIENCE 15, 193 (1988). This ant's failure to follow the rules is an anomaly of the type to be expected in the operation of a system such as this. It is, therefore, a matter of no particular concern for the colony (though it is for the ant, since she will no doubt be killed by ants from the other colony). *See, e.g.,* WILSON, *supra* note 27, at 206-07.

"Deviant behavior," on the other hand, has a significant potential for undermining the

that of the pieces in a chess game, is pre-defined. A white rook cannot capture a white pawn; an ant cannot steal food from the colony stores and flee, attack another ant from its own colony or take a day off from work.[90] Ant rules, like chess rules, are simple and straightforward; they leave no capacity for deviance. Since there is no capacity for deviance, there is no need for an enforcement mechanism. Ants have war but not crime, soldiers but not police.

Systems populated by non-intelligent entities do not confront the risk of chaos arising from internal forces, i.e., from deviant behavior.[91] The absence of individual intelligence means that there are no "wild cards" in the deck – no potential for antisocial behavior.[92] That, in turn, means they have no need to devise special rules – "criminal rules" – to deal with deviance.[93] As explained below,[94] "criminal rules" deal with the potential for deviance in a system by defining the behaviors that are prohibited. Systems populated by intelligent agents find it necessary to define behaviors they will not tolerate because the constituent entities can innovate, i.e., indulge in behaviors other than those that are socially prescribed.[95] Systems populated by intelligent agents will therefore have two sets of rules in place that govern the behavior of their constituents: (1) a set of constitutive rules that establish the rights and obligations of the constituent entities and (2) a set of proscriptive rules that outlaw certain types of behaviors.[96] Systems populated by non-intelligent entities, however, have no need for proscriptive rules because there is no capacity for behavioral innovation and, consequently, no potential for deviance.

The sections immediately below examine two systems that are populated by entities of varying degrees of intelligence; the entities that populate both systems are sufficiently intelligent to engage in deviant behavior. The sections below, therefore, analyze how systems deal with a constituent entity's failure to follow governing rules.

b. Wolves

Individual intelligence is found in many species, but it is most highly

order or a self-organizing collective system populated by intelligent entities. This issue is discussed later. *See infra* Part II(A)(2)(c).

[90] *See, e.g.,* WILSON, *supra* note 27, at 165 (social insects do not play).

[91] For an overview of how deviant behavior threatens internal order, see *supra* note 89. *See also infra* Part II(A)(2)(c).

[92] *See, e.g.,* MERRIAM WEBSTER (defining "antisocial" as "hostile or harmful to organized society" and "being or marked by behavior deviating sharply from the social norm."); *see also supra* note 89.

[93] *See infra* Part II(A)(2)(c).

[94] *See id.*

[95] *See id.*

[96] *See id.*

evolved in mammals.[97] Notwithstanding their intelligence, many mammals are not suitable for the present analysis because they live "solitary" lives.[98] Since our focus is on ensuring order in collective systems, we must consider how order is established and maintained among mammalian species that are both "intelligent" and "social."[99]

Wolves are clearly intelligent under the definition given above; indeed, they are one of the most intelligent non-primate mammalian species.[100] Wolves are also social creatures:[101] Among mammals, "the carnivores are surpassed only by the primates in the intricacy and variety of their social behavior," and at "what might be called the summit of carnivore social evolution," wolves display a level of social organization that is otherwise found nowhere except among "a few of the Old World monkeys and apes."[102]

Wolves, like ants, must establish and maintain internal and external order if their social groupings are to survive.[103] Wolves live in packs that contain as

---

[97] *See generally* BONNER, *supra* note 24, at 38-53.

[98] *See, e.g.,* WILSON, *supra* note 27, at 499. "Solitary" means that the species' social groupings are "comprised exclusively of the mother and her unweaned young, and adult males and females associate only during the breeding season." *Id.*

[99] Although ants are described as "social insects," biology differentiates the simple sociality found in insect species from the more complex social arrangements characteristic of mammals. *See, e.g., id.* at 7 (defining "society" as "a group of individuals belonging to the same species and organized in a cooperative manner") & 8 (defining "colony" as a group "of organisms which are highly integrated, either by physical union . . . or by division into specialized . . . castes"). In sociobiology, "colony" is reserved for communities of social insects, "tightly integrated masses of sponges . . . and other 'colonial' invertebrates." *Id.* at 8.

[100] *See supra* notes 41-44 and accompanying text; *see also supra* note 55; *see, e.g.,* PETER STEINHART, THE COMPANY OF WOLVES 126-36 (1995); *see also* WILSON, *supra* note 27, at 504-13; DEFENDERS OF WILDLIFE, WOLVES: THE BASICS OF WOLF BIOLOGY AND TAXONOMY, *at* http://www.defenders.org/wildlife/wolf/wolfbio.html (last visited Nov. 30, 2003) [hereinafter Wolf Basics].

[101] STEINHART, *supra* note 100, at 12-13 ("Wolves are social creatures . . . . The life of the individual is inextricably woven into the life of the pack.").

[102] WILSON, *supra* note 27, at 499. This section examines wolves, rather than one of these primate species, because the goal is to analyze a species that is, in effect, intermediate between the social insects and man. Wolves are individually intelligent, but their behavior and social organization is sufficiently distinct from mankind's to provide a useful point of comparison. The behavior and social organization of the higher primates is in many respects functionally analogous to that of mankind, which provides little basis for comparison. *See, e.g.,* FRANS DE WAAL, CHIMPANZEE POLITICS: POWER AND SEX AMONG APES 3-41 (rev. ed. 1998).

[103] *See infra* Part II(A)(1). Like ants, a wolf pack is an extended family; *see, e.g.,* L. David Mech, *Alpha Status, Dominance, and Division Of Labor In Wolf Packs,* 77 CANADIAN J. OF ZOOLOGY 1196, 1196-1203 (1999), *available at*

many as twenty individuals.[104] As with ants, establishing internal order means the pack must ensure that its members carry out essential tasks, such as creating and maintaining a den,[105] hunting food, reproducing and nurturing offspring to maturity, in a consistent, predictable manner.[106] Individual wolves, unlike individual ants, are intelligent;[107] intelligence confers the ability for independent decision making and autonomous action upon members of a species.[108] This means that wolves cannot rely on the strategies ants use to maintain order in their colonies.[109] Unlike ants, wolves have to deal with the potential for deviant behavior, i.e., with the possibility that a pack member will deliberately steal food, attack other members of the pack or otherwise disrupt the internal order that is necessary for the survival of the pack and of its members.[110] Wolves deal with this potential, and with the processes of establishing and maintaining internal order, by implementing a dynamic hierarchical rank order among pack members.[111]

Many species use rank order to structure their social systems.[112] Known as a "dominance hierarchy," this strategy consists of a set of,

> sustained aggressive-submissive relations . . . . The simplest . . . version of a hierarchy is . . . the rule of one individual over all other members of the group, with no rank distinctions being made among the subordinates . . . . More commonly, hierarchies contain multiple ranks in a more or less linear sequence: an alpha individual dominates all others, a beta individual dominates all but the alpha, and so on down to the omega individual at the bottom, whose existence may depend simply on staying

---

http://www.npwrc.usgs.gov/resource/2000/alstat/alstat.htm.

[104] *See, e.g.,* STEINHART, *supra* note 100, at 13 ("wolves live in packs of two to twenty, the pack size depending on the size of available prey."); WILSON, *supra* note 27, at 509 ("A new pack is formed when a mated pair leaves its parental group to produce a litter on its own."); *see also* PACKARD, *supra* note 42, at ¶ 7 ("Packs usually are founded by an unrelated male and female, each having dispersed from their natal families and joining up in an area defensible from encroachment by other packs . . . . Each family grows with successive litters (typically 5-6 pups) and shrinks as offspring disperse.").

[105] *See, e.g.,* STEINHART, *supra* note 100, at 15.

[106] *See infra* Part II(A)(2)(a); JENNY RYON, SOCIAL ORGANIZATION OF WOLVES, (2000), *at* http://www.wolfca.com/SocialOrg.html (last visited Mar. 30, 2004) (Pack members work together to "maintain territories, obtain food and rear young.").

[107] *See supra* note 99 and accompanying text.

[108] *See infra* Part II(A)(2)(a).

[109] *See infra* Part II(A)(2)(a).

[110] *See infra* Part II(A)(1); *see also supra* note 89.

[111] *See, e.g.,* WILSON, *supra* note 27, at 283 ("the vast majority of mammal species forming groups with any degree of social complexity . . . display dominance" hierarchies).

[112] *See, e.g., id.*

out of the way of its superiors.[113]

Dominance hierarchies are formed during "encounters between animals by means of repeated threats and fighting."[114] After these encounters resolve the issue of rank, subordinates give way to their superiors "with a minimum of hostile exchange."[115] Once a dominance hierarchy has been established, it is often maintained,

> by 'status' signs. The identity of the leading male in a wolf pack is unmistakable from the way he holds his head, ears, and tail, and the confident, face-forward manner in which he approaches other members of his group. He controls his subordinates in the great majority of encounters without any display of overt hostility.[116]

Once established, a dominance hierarchy is far from permanent, especially among some species: "The behavioral ontogenies of species seem designed to give each loser a second chance, and in some of the more social forms the subordinate need only wait its turn to rise in the hierarchy."[117] Among some species, this is simply a matter of waiting until the dominant animal "weakens or expires from age or injury".[118] Another alternative is for defeated challenger(s) to leave the initial social grouping to form another group.[119]

Wolf packs conform almost exactly to this description of a dominance hierarchy.[120] A pack "is a well-ordered society" in which "each member is expected to learn, observe, and obey the laws . . . . The elder pack members teach the cubs about pack etiquette."[121] Pack etiquette revolves around "linear dominance orders" that form among the members of a pack.[122] Wolf packs have rank orders for each sex:

> [T]he dominant, or alpha, male lords it over all the other males, and a dominant, or alpha, female asserts her will over the other females. There may be a beta and a gamma, second- and third-ranked wolves of each sex, each imposing some will on the lesser-ranking wolves down through the

---

[113] *Id.* at 279 (citation omitted & emphasis in the original).

[114] *Id.* at 280.

[115] *Id.*

[116] *Id.*

[117] *Id.* at 290.

[118] WILSON, *supra* note 27, at 290.

[119] *See, e.g., id.* at 290-91; STEINHART, *supra* note 100, at 13-14.

[120] RAISED BY WOLVES, INC., ESSENTIAL WOLVES, *at* http://www.raisedbywolves.org/EssentialWolvesWord.pdf (last visited Nov. 30, 2003).

[121] *Id. (*A wolf pack consists of "an alpha, or dominant pair, their pups, and several other subordinate or young animals. The alpha female and male are the pack leaders, tracking and hunting prey, choosing den sites, and establishing the pack's territory."); *See also* WOLF BASICS; STEINHART, *supra* note 100, at 15.

[122] WILSON, *supra* note 27, at 509.

> Greek alphabet to omega . . . .
>
> The dominance rank order of a pack changes as wolves age or get injured and younger wolves mature and gain strength, confidence, and understanding . . . . Old dominants may be chased out of the pack or beaten and brought down to submissive roles. Younger challengers may arise, assert themselves, be beaten and sink back into submission.[123]

A wolf's rank "begins to be established early in life, when puppies play-fight."[124] Once established, rank is "reinforced . . . by repeated exchanges of hostile and submissive displays."[125] Wolves have a complex language of gesture and posture for dominance behavior.[126] For example, dominant wolves may need only to stare at a subordinate to freeze it in its tracks.[127]

The alpha male is the dominant member of a wolf pack; he holds it together as a society.[128] He tends to be the center of attention, and is treated with great deference by the others.[129] When a pack travels, any of the higher-ranked pack members can take the lead, but the alpha male takes command when the pack

---

[123] STEINHART, *supra* note 100, at 13; s*ee also id.* at 113 ("A hierarchy of strong to weak is constantly evolving and changing in the pack."). When a dominant wolf is dethroned, he/she may leave the pack and form a new pack. *See, e.g., id.* at 14 (describing how an alpha female who was displaced as lead female left her original pack, found a new mate and founded a new pack; the new pack included wolves who had left the original pack to join her).

[124] WILSON, *supra* note 27, at 509*; see, e.g.,* WOLF BASICS*;* STEINHART, *supra* note 100, at 113 ("Wolves compete for status from an early age. Fox found wolf pups routinely working out dominance hierarchies at eight weeks; Mech saw four-week-old pups fighting for status.") (citing MICHAEL W. FOX, THE BEHAVIOR OF WOLVES, DOGS AND RELATED CANIDS (1971) and L. DAVID MECH, THE WOLF: THE ECOLOGY AND BEHAVIOR OF AN ENDANGERED SPECIES (1970)).

[125] WILSON, *supra* note 27, at 509; *see, e.g.,* STEINHART, *supra* note 100, at 113 ("A hierarchy of strong to weak is constantly evolving and changing in the pack."); *see also* THE ANGLIAN WOLF SOCIETY, AN OVERVIEW OF WOLF AGGRESSION, *at* http://www.anglianwolf.com/D_FrontPage/D_AR_Article/D_Waggr/Waggr.htm (last visited Nov. 30, 2003).

[126] *See, e.g.,* STEINHART, *supra* note 100, at 113.

[127] STEINHART, *supra* note 100, at 113-14 ("If a stare is not enough, a dominant may lunge at a subordinate, growling with bared teeth, erect ears and tail, and bristling hackles. Usually, bites . . . are inhibited and do not draw blood. A dominant wolf may discipline a subordinate wolf merely by placing its mouth around the subordinate's muzzle.").

[128] *See, e.g.,* WILSON, *supra* note 27, at 312 (alpha male exercises leadership in a manner that is "more nearly consonant" with leadership among human beings than the leadership found among other species); STEINHART, *supra* note 100, at 103 (noting that it is not known whether the alpha male accomplishes this by "being aggressively intolerant of disorder or by fostering a sense of companionability").

[129] *See, e.g.,* WILSON, *supra* note 27, at 509; STEINHART, *supra* note 100, at 121.

hunts or battles enemies.[130]

When they hunt, pack members display "elaborate cooperative behavior."[131] They coordinate their actions, which can extend to splitting pack members up so they can encircle or otherwise entrap their prey.[132] Pack members play different roles in hunting, depending upon their strengths and aptitudes.[133] Packs also employ a basic division of labor in caring for their offspring: Initially, the mother stays in the den and cares for the cubs when they are small. "[O]ther wolves bring both her and the cubs food when they return from a hunt. As they mature other members of the pack take turns baby-sitting so that the mother can join the pack in a hunt."[134]

Like ants, wolf packs must maintain external order. This requires that they do two things: (a) preserve the integrity of their territory against predation by other packs; and (b) fend off attacks from other packs. Here, too, wolf packs display an essential characteristic of dominance hierarchies: a "violent united front against strangers."[135]

Given their size and specialized predatory habits, wolves must maintain "low population densities and occupy relatively immense home ranges."[136] Each pack occupies a distinct territory, which it defends from other wolves.[137]

> Territories change size and shape from year to year. Resident wolves scent-mark heavily at the boundaries of their territories, and trespassing wolves mark assiduously when they stray inside another pack's domain. It is as if a wolf thus leaves a string of boasts and threats . . . to taunt and intimidate other packs and keep them out of its larder. Wolves . . . have been known to kill neighboring wolves that strayed into their

---

[130] *See* WILSON, *supra* note 27, at 312; *See also* STEINHART, *supra* note 100, at 121.

[131] BONNER, *supra* note 24, at 89.

[132] *See, e.g.,* STEINHART, *supra* note 100, at 112-13 (some suggest that adult wolves' tendency to engage in frequent play is a way of "rehearsing" the coordination needed for the hunt); *see also id.* at 127 (describing how wolves split up to encircle a deer); WILSON, *supra* note 27, at 505 (describing how wolves split up; one hiding and the others driving the prey toward the hidden wolf).

[133] *See, e.g.,* STEINHART, *supra* note 100, at 24 ("When wolves hunt, they make use of disparate special abilities. Some wolves are good at finding prey, some at reading the strengths and weaknesses of prey, some at chasing prey, some at killing prey.").

[134] BONNER, *supra* note 24, at 89*; see also* STEINHART, *supra* note 100, at 15, 121.

[135] WILSON, *supra* note 27, at 286.

[136] *Id.* at 505*; see, e.g.*,STEINHART, *supra* note 100, at 16 (pack territories can range from 50 to 800 square miles or even more, depending on the nature of the terrain). Wolves "move ceaselessly over their domains in search of prey." WILSON, *supra* note 27, at 505.

[137] *See, e.g.,* STEINHART, *supra* note 100, at 16 ("We think wolves keep territories either to protect den sites or to conserve hunting opportunities, and that the abundance of pretty generally defines the size of a territory.").

territories.[138]

In addition to defending their territory, wolves engage in "a primitive form of warfare."[139] One expert has described how they leave their territory to raid "neighboring territories, to all appearances bent on murdering their neighbors . . . . If . . . one pack senses a strong advantage, it will attack the other."[140]

As a self-organizing collective system, a wolf pack is an interesting intermediate analytical step between an ant colony and human society (which is the last system to be considered).[141] Like ants, a wolf pack relies on laterally-structured behavior, at least for basic interactions. No one, for instance, not even the alpha male, articulates rules that "tell" wolf pups to play-fight and thereby begin the process of achieving pack rank;[142] and no rule "tells" adult wolves to play and thereby hone their skills for hunting.[143] Wolves do not need formal, articulated rules to structure basic behaviors such as these because a wolf is essentially a small extended family the members of which collectively carry out the activities needed to ensure the survival of the pack and its constituent members.[144] Except for the care of cubs, there is no division of labor in a wolf pack. The adults join together to hunt and defend themselves from competing packs and enemies.[145]

Unlike ants, wolves cannot rely exclusively on laterally-structured behavior because they are intelligent creatures who use their intelligence to survive.[146] A wolf's life is not like a chess game;[147] while some general rules of conduct exist,[148] individual wolves survive because they successfully establish and

---

[138] *Id.* at 16.

[139] *Id.* at 115.

[140] *Id.* at 115-16*; see also* WILSON, *supra* note 27*,* at 505.

[141] *See infra* Part II(A)(2)(c).

[142] *See supra* note 114 and accompanying text.

[143] *See supra* note 132.

[144] *See supra* notes 131-34 and accompanying text*; see also supra* notes 103-04*; see, e.g.,* PACKARD, *supra* note 42, at 45*:*

> At all ages, relatively hard-wired responses to specific stimuli bring individuals into situations where each is likely to learn the contingencies of interaction with the specific environmental conditions into which it is born. Examples include caching, food-begging, social interaction, foraging, risk-avoidance, activity patterns, leadership and orientation relative to homesites.

[145] *See supra* notes 131-34 and accompanying text*; see also supra* notes 135-38 and accompanying text.

[146] *See, e.g.,* STEINHART, *supra* note 100, at 99 (a lone wolf "may starve without the shared hunting experience and concentrated killing power of the pack, or be . . . killed by other wolves . . . . [T]hey are immensely more vulnerable to hunters.").

[147] *See infra* Part II(A)(2)(a).

[148] *See, e.g.,* STEINHART, *supra* note 100, at 102 ("Any wolf in possession of food is

maintain their rank in a wolf pack and because they work cooperatively with other members of the pack.[149] Much of the behavior within a pack is unorchestrated, but the overall activities of the pack and its essential cohesion reflect an underlying order that derives from the dominance hierarchy described above. As noted earlier, the dominance hierarchy holds a pack together;[150] in so doing, it controls the limited capacity for deviant behavior that exists in a wolf pack. As explained earlier, "deviant behavior" is an entity's deliberate failure to follow rules that govern behavior in a social system.[151] For various reasons, this capacity is not nearly as evolved among wolves as it is in human beings,[152] but it is an aspect of wolf sociality.

In an ant colony, each ant's function and behaviors are prescribed by external factors; an ant has no ability to elect not to perform her assigned function by engaging in the prescribed behaviors.[153] This is to some extent true of wolves; they must hunt to survive and their chances of hunting successfully, and surviving, are much greater if they belong to a pack.[154] Unlike ants, however, wolves are not inevitably tied to their original pack; they can leave to strike out on their own or join another pack.[155] Wolves can also shift position within their original pack.[156] As noted above, wolf packs are hierarchical,[157] and higher rank brings certain advantages; only alpha wolves breed, alphas feed first, and alphas bully and dominate subordinates.[158] These

likely to have a zone of one to two feet around it that no other wolf will enter.").

[149] *See, e.g., id.* at 127-36. Ants in a colony collectively find and acquire food by sending hundreds or thousands of foragers out into their territory; when a forager finds a food source, she brings back what she can carry and lays down a trail that will signal other foragers to do the same. Wolves, on the other hand, collectively search for, eventually find and then kill their food, a task which can be both challenging and dangerous. *See, e.g., id.* at 22-23, 54-77. Wolves employ intelligence in deciding where to hunt, when to hunt, what to hunt and how to hunt. *See id.*

[150] *See supra* note 128.

[151] *See infra* Part II(A)(1)*; see also supra* note 89.

[152] *See infra* Part II(A)(2)(c).

[153] *See infra* Part II(A)(2)(a).

[154] *See supra* note 146.

[155] *See, e.g.,* STEINHART, *supra* note 100, at 12, 93-101.

[156] *See supra* note 123 and accompanying text.

[157] *See supra* note 123 and accompanying text. The presence of queens, workers and soldiers may suggest that ant colonies and the hives of other social insects are hierarchically organized, but that is not the case. As the previous section explained, ant colonies are organized laterally; there are castes in the sense that ants have a fixed, to some extent biologically-determined division of labor, but the castes are not ranked. *See infra Part* II(A)(2)(a).

[158] *See, e.g.,* STEINHART, *supra* note 100, at 102*; see also* PACKARD, *supra* note 42 (noting that alpha wolves "'police' access to clumped food", such as an "ungulate carcass").

and other advantages create incentives for subordinate wolves to try to move up in a pack hierarchy; their efforts to do so create a potential for disorder within a pack.[159] But wolf hierarchies also establish other ranks and ordered priorities within a pack and thereby reduce the potential for disorder that is an inevitable aspect of a system populated by highly intelligent, highly aggressive predators.[160] In one sense, therefore, wolf hierarchy creates the potential for disorder, while in another sense, it produces order and stability.[161]

How do wolf hierarchies control deviance and promote order? As noted earlier, the ranks establish priorities that serve to channel behavior in predictable ways, thereby minimizing casual, individual conflict between wolves.[162] The ranks ensure, for instance, that a gamma or even lower-ranked wolf will not take food from a beta wolf, at least not unless and until the lower-ranked wolf is ready to mount a full-blown challenge to the beta's authority.[163] The ranks create a fluid system of rules that predictably order the interactions – and some of the essential functions – of a wolf pack.[164]

But what about a subordinate challenging a higher-ranked wolf's authority? Dominance hierarchies are based on personal characteristics; an alpha male's rank is based on his ability to subordinate other wolves through physical aggression and/or psychological influence.[165] Since an alpha male's position at the top of the hierarchy is based on his ability to impose his will upon the other members of the pack, it is transient, subject to divestment.[166] Challenges occur almost constantly, at all levels of the hierarchy in a pack.[167] If a challenge succeeds, the challenger becomes the new ranking wolf and the defeated wolf

---

[159] *See, e.g.,* STEINHART, *supra* note 100, at 99-100, 111-12.

> Wolves are social beings, enjoying warm, companionable . . . lives within the pack. But wolves are also individuals, . . . competing, sometimes violently, for social standing . . . . It is in a wolf's interest to accommodate and coordinate with other wolves, yet also to contend with the same wolves . . . . Humans and wolves both evolved as group hunters . . . . [T]hey have surprisingly similar social lives. Both have dominance hierarchies; both care deeply for their young and their families and can display . . . exacting coordination in complex tasks; both take pleasure in companionship . . . and play. Yet both can be aggressive and violent.

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] *See, e.g.,* PACKARD, *supra* note 42 (describing how, in one pack "two adult daughters approached their father [who was feeding on a deer carcass] in a low crouch, he pinned each to the ground with an inhibited muzzle-bite . . . . The grown daughters stayed away from the carcass until their father was finished.").

[164] *Id.*

[165] *See supra* note 128.

[166] *Id.*

[167] As noted earlier, there are also alpha females, beta males and females, and still other ranks. *See supra* note 125 and accompanying text.

becomes a subordinate or leaves the pack;[168] if a challenge fails, the challenger sinks back into subordination or leaves the pack.[169] Is this dynamic another type of deviant behavior threatening order within a pack?

One could argue that challenges to a higher-ranked wolf's authority represent deviant behavior insofar as they constitute a failure to abide by the rules that constitute the pack *at a given time*.[170] That is, if Wolf Y is the alpha male of Pack Dakota, one of the rules of the pack is that other wolves defer to Wolf Y; by failing to defer to Wolf Y, Wolf Z violates the rules of the pack as they exist at the time he challenges Wolf Y's authority. In that sense, Wolf Z's challenge represents deviant behavior.[171] That characterization of Wolf Z's behavior is inaccurate, however, because it ignores the fact that challenges to the authority of higher-ranked wolves is an intrinsic component of wolf social life.[172] No rule of pack or species behavior prohibits such challenges; indeed, as noted above, Wolf Y's claim to dominance rests upon his ability to withstand such challenges.[173] Challenges by lower-ranked wolves are therefore the legitimate process that is used to determine leadership;[174] as such, they cannot be considered deviant behavior.

Notwithstanding that, wolf packs do conform to the proposition advanced above, namely, that systems populated by intelligent agents find it necessary to define certain behaviors as prohibited because the constituent entities can engage in behaviors other than those prescribed by the system.[175] Unlike human societies, wolf packs accomplish this by using relational instead of structural rules. That is, the definition of behavior as prohibited derives from the status relationship which exists between the specific wolves who are involved in an encounter. It is, therefore, prohibited behavior for a lower-ranked wolf to feed contemporaneously with an alpha wolf because such conduct violates the essential constitutive rules that sustain order in the social system.[176] In modern human societies, on the other hand, the definition of

---

[168] *See supra* note 125 and accompanying text.

[169] *See supra* note 125 and accompanying text.

[170] *See* RYON, *supra* note 106, *at* http://www.wolfca.com/SocialOrg.html.

[171] *See id.*, *at* http://www.wolfca.com/SocialOrg.html.

[172] *See id.*, *at* http://www.wolfca.com/SocialOrg.html.

[173] *See id.*, *at* http://www.wolfca.com/SocialOrg.html.

[174] *See, e.g.,* RYON, *supra* note 106 (wolf social organization is "like politics in that there is always a contender for the dominant position no matter how long the incumbent has been in power. To quote a political adage 'the day you are elected is one day closer to leaving office.'").

[175] *See supra* note 95 and accompanying text.

[176] *See, e.g.,* STEINHART, *supra* note 100, at 102. Conversely, it is not prohibited (deviant) behavior for beta wolves to feed contemporaneously because this conduct comports with the behaviors prescribed by the essential constitutive rules that create and govern order within a wolf pack. *See Id.*

behavior as prohibited derives from formal, institutionalized rules which apply without regard to the identities and/or relative status positions of the individuals who are involved in an encounter.[177] It is, therefore, prohibited behavior for an American citizen to attack any other American citizen regardless of their social, economic or other position in society.[178] Unlike the relational rules that govern wolf behavior, this prohibition is structural and, therefore, categorical in nature.[179]

Wolf packs also conform to the secondary proposition advanced above, i.e., that systems populated by intelligent agents will have one set of rules that prescribes rights and obligations and another that proscribes certain types of behavior.[180] Here, too, wolf packs use relational rules instead of structural rules.[181] The rules that prescribe rights and obligations are embedded in the web of relationships that exist among the wolves in a pack.[182] In wolf society, the two types of rules essentially operate as mirror images of each other.[183] The rights and privileges an alpha male enjoys are defined by his status as alpha male; his status as alpha male also defines the respective behaviors that are proscribed for specific members of the pack.[184] Fewer behaviors will, for example, be proscribed for the alpha female than for a beta female, for a beta male than for a gamma male, and so on.[185] Unlike the categorical rights and obligations that are structurally conferred upon members of a modern human society,[186] the rights and privileges a member of a wolf pack enjoys are dynamic, only changing if and when the wolf's status changes.[187]

---

[177] *See infra* Part II(A)(2)(c).

[178] *Id.*

[179] *Id.*

[180] *See supra* note 96 and accompanying text.

[181] *See id.*

[182] *See id.*

[183] *See supra* note 176 and accompanying text.

[184] *See id.*

[185] *See supra* note 125 and accompanying text.

[186] *See infra* Part II(A)(2)(c).

[187] The status and consequent rights and privileges enjoyed by particular wolves is a dynamic aspect of wolf social life. The general structure of wolf social life, on the other hand, is far less dynamic than the structure of social life in human societies. *See infra* Part II(A)(2)(c).

c. Humans

A being, independent of any other, he has no rule to pursue, but such as he prescribes to himself . . . .[188]

Humans, like wolves and ants, are social creatures.[189] Humans, like wolves but unlike ants, are intelligent creatures under the definition given above.[190] Humans are so far the most intelligent species to inhabit the Earth; human intelligence not only exceeds that of all other species, it is far more complex.[191] Since humans are social, they live in self-organizing collective systems;[192] and since humans are far more intelligent than any other earthly creature, the social systems they create are far more complex than those found among any other terrestrial species.[193] The social systems humans create are also much more flexible than those found among other species.[194]

Why are human social systems much more complex and much more flexible than those of other species? One reason is the complexity of human beings, who vary greatly in behavior, intelligence and achievement.

> Even in the simplest societies individuals differ greatly . . . . Human societies are organized by high intelligence, and each member is faced by a mixture of social challenges that taxes all of his ingenuity. This baseline variation is amplified at the group level by other qualities exceptionally pronounced in human societies: the long, close period of socialization; the loose connectedness of the communication networks; the multiplicity of bonds; the capacity, especially within literate cultures, to communicate over long distances and periods of history; and from all these traits, the capacity to dissemble, to manipulate and to exploit.[195]

Another reason is the relative rigidity of the processes that maintain order in social systems populated by other species, including social insects.

---

[188] 1 WILLIAM BLACKSTONE, COMMENTARIES *39.

[189] *See supra* note 99 and accompanying text*; see also infra* Parts II(A)(2)(a) and II(A)(2)(b).

[190] *See supra* notes 41-44 and accompanying text*; see also infra* Parts II(A)(2)(a) and II(A)(2)(b).

[191] *See, e.g.,* WILSON, *supra* note 27, at 555*; see also supra* note 56 and accompanying text; *see, e.g.,* Wilson, *supra* note 27, at 567-68 (for the premise that intelligence and sociality interacted in the process of human evolution).

[192] *See infra* Part II(A)(1).

[193] For a discussion of the complexity of human societies, *see supra* notes 202-207 and accompanying text.

[194] *See, e.g.,* WILSON, *supra* note 27, at 548 ("The parameters of social organization, including group size, properties of hierarchies, and rates of gene exchange, vary far more among human populations than among those of any other . . . species.").

[195] *See id.* at 548-49.

> In honeybees and in ants of the genera *Formica* and *Pogonomyrmex* . . . [s]ome . . . specialization . . . occurs. Certain individuals remain with the brood as nurses far longer than the average, while others concentrate on nest building or foraging. Yet . . . [w]hen one colony . . . is compared with another of the same species, the statistical patterns of activity are about the same . . . . [S]ome of this consistency is due to negative feedback. As one requirement such as brood care . . . intensifies, workers shift their activities to compensate until the need is met, then change back again. Experiments have shown that disruption of the feedback loops, and thence deviation by the colony from the statistical norms, can be disastrous.[196]

Human societies do not operate within such a narrow range of behavioral possibilities. Indeed, as one scholar noted, "anthropological literature abounds with examples of [human] societies that contain obvious inefficiencies and even pathological flaws – yet endure."[197]

It is the "lack of competition from other species" that frees human societies from the constraints that channel other animal social systems into rigid patterns:

> [M]an . . . has been so successful in dominating his environment that almost any kind of culture can succeed for a while, so long as it has a modest degree of internal consistency and does not shut off reproduction altogether. No species of ant or termite enjoys this freedom. The slightest inefficiency in constructing nests, in establishing odor trails, or in conducting nuptial flights could result in the quick extinction of the species by predation and competition from other social insects. To a scarcely lesser extent the same is true for social carnivores and primates.[198]

As a sociologist noted, humans are unique in the animal kingdom in that they have "no species-specific environment."[199] A wolf, for instance, "has a largely fixed relationship with its environment, which it shares with all other members of its respective species."[200] This relationship, which is common to all non-human species, is "biologically fixed", so that "all non-human animals, as species and as individuals, live in closed worlds whose structures are predetermined by the biological equipment of the . . . species." [201]

Humans, on the other hand, create their environment; unlike the biologically determined environments in which non-human animals live, human

---

[196] *See id.* at 549.

[197] *Id.* (citing the "slave society of Jamaica" and the Ik of Uganda).

[198] *Id.* at 550*; see also infra Parts* II(A)(2)(a) and II(A)(2)(b).

[199] BERGER & LUCKMANN, *supra* note 10, at 47.

[200] *Id.; see, e.g., infra* Part II(A)(2)(b).

[201] BERGER & LUCKMANN, *supra* note 10, at 47.

environments are "a social enterprise" – the collective product of collaborative human activity.[202] The creation of such environments is a matter of necessity, since humans lack the "biological means to provide stability for human conduct. Human existence, if it were thrown back on its organismic resources . . . would be existence in . . . chaos."[203] The question is how humans successfully create and maintain social order. As explained earlier, every social system, whether populated by biological or artificial entities, must establish and maintain order – both internal and external – if it is to survive.[204] The answer is that social order is,

> a human product, or, more precisely, an ongoing human production . . . . Social order is not biologically given . . . . Social order . . . is also not given man's natural environment, though particular features . . . may be factors in determining certain features of a social order . . . . Social order exists *only* as a product of human activity . . . . Both in its genesis (social order is the result of past human activity) and its existence in any instant of time (social order exists . . . insofar as human activity continues to produce it) it is a human product.[205]

Human social order is, therefore, an artifice, a construct; since order is an artifice, it can assume various forms in different social systems, but it is a necessary constant in every such system.[206] The question is: How is this artifice produced? Since humans – unlike ants, wolves and other non-human species – are not constrained by biologically-driven behavioral parameters, it is at least conceptually possible that the tactics humans use to produce social order across their social systems are idiosyncratic; that is, it is conceivable that while social order is a constant, the devices humans use to achieve it are not. It may seem, however, that this conceptual possibility is inconsistent with the postulates advanced earlier, namely, that systems populated by intelligent agents (a) will find it necessary to define behaviors they cannot tolerate and (b) will therefore rely upon two types of rules – constitutive rules and proscriptive rules – to establish and maintain order within the system.[207]

---

[202] *Id.* at 51*; see also id* ("[N]one of these formations may be understood as products of man's biological constitution, which . . . provides only the outer limits for human productive activity."); *see, e.g., id.* at 47-50 (limited role of biology in human social evolution). *See generally*, WILSON, *supra* note 27*,* at 567-74.

[203] BERGER & LUCKMANN, *supra* note 10, at 49.

[204] *See infra* Part II(A)(1).

[205] BERGER & LUCKMANN, *supra* note 10, at 52 (emphasis in the original)*, see, e.g.,* David E. Van Zandt, *Commonsense Reasoning, Social Change, and the Law,* 81 Nw. U. L. Rev. 894, 898 (1997) ("[S]ocial order is produced by identifiable or discoverable processes that hold society together.").

[206] *See supra* Part II(A)(1).

[207] *See supra* Part II(A)(2)(c).

In point of fact, human systems – like the wolf packs discussed in the previous section and other systems populated by intelligent agents – do construct social order in accordance with these postulates.[208] But because human beings are very intelligent and do not operate within a limited range of biologically-driven behavioral possibilities, the ways in which they accomplish this can and do vary somewhat from system to system. There is, in essence, a macro-consistency in the way social order is constructed across human societies, but there has historically been a level of idiosyncrasy in the discrete manifestations of social order in particular societies.

To understand why this is true, it is necessary to consider how humans construct social order. Unlike other self-organizing collective systems, systems that are populated by intelligent entities (such as humans and wolves) *do* confront the risk of chaos arising from deviant behavior, which is an entity's deliberate failure to follow governing rules.[209] As noted earlier, all systems – social, biological, physical and artificial – operate according to a set of rules.[210] In many systems, these rules are pre-given: The rules that govern physics, for instance, are fixed and predetermined; the laws of thermodynamics are subject neither to dispute nor modification.[211] The same can be said of the rules that govern many biological systems; a particular colony of ants does not hold a referendum to decide how it will establish order.[212] The rules that maintain order among the ants and other social insects are for the most part biologically determined;[213] since ants are not intelligent, they do not have the capacity to alter these rules or to contumaciously refuse to comply with them.[214]

Intelligent entities can do either or both. The specific ability to do this varies with the degree of intelligence possessed by the individual members of the species and the extent to which they are subject to biological constraints that limit their capacity to realize the potential their intelligence gives them.[215]

---

[208] *See supra* Part II(A)(2)(b).

[209] *See supra* notes 89-96 and accompanying text.

[210] *See supra* notes 24-25 and accompanying text.

[211] *See, e.g.,* ARCHIVES OF SCIENCE, SYMMETRY, BROKEN-SYMMETRY AND THE FIRST AND SECOND LAWS OF THERMODYNAMICS (2001), *at* http://www.entropylaw.com/entropyenergy.html [herinafter ARCHIVES OF SCIENCE] (laws of thermodynamics "sit above the ordinary laws of nature as . . . laws upon which the other laws depend."); *Id.* (citing R. Swenson & M. Turvey, *Thermodynamic Reasons for Perception-Action Cycles*, 3 ECOLOGICAL PSYCHOLOGY 317 (1991), *available at* http://www.ecologicalpsychology.com/SwenTurv.pdf).

[212] ARCHIVES OF SCIENCE, *supra* note 211; *see, e.g., infra* Part II(A)(2)(a).

[213] *See, e.g.,* BONNER, *supra* note 24, at 79*; see also infra* Part II(A)(2)(a).

[214] *See infra* Part II(A)(2)(a).

[215] *See supra* notes 195-97 and accompanying text*; see also infra* Parts II(A)(2)(a) and II(A)(2)(b).

Because humans are highly intelligent and essentially free from biological constraints, the ability to create, alter and ignore rules is most pronounced in mankind.[216] Consequently, the most elaborate rule systems have grown up among by humans.

In human social systems, as in all self-organizing collective systems, rules are used to establish and maintain order both internally and externally.[217] Internal order is the highest priority, and the first task undertaken, because without it a system cannot exist and cannot, therefore, resist external threats. Consequently, the first type of rules to emerge in human society are the constitutive rules noted earlier.[218] These rules establish order by specifying and limiting the choices individual constituents can make. In human societies, the complexity of these constitutive rules evolved as human social groupings increased in size and complexity.

Initially, human systems were organized around the nuclear family; until about 10,000 years ago humans were hunter-gatherers who lived in "multi-family . . . bands of a few tens of people."[219] The constitutive rules that established order in these systems were simple. The purpose of these rules was ensuring that each social system – each band – met the conditions needed for it to survive and continue. This requires ensuring that the members of the system survive and reproduce, that their offspring mature and are incorporated into the system, and that the members of the system are protected from predators and human competitors.[220] The constitutive rules that governed the bands, which were the first form of human social organization, channeled the activities of their members toward the achievement of these ends by establishing a basic command structure and a general division of labor.[221] The command structure was analogous to that found in a wolf pack;[222] it consisted, minimally, of a

---

[216] *See supra* notes 195-97 and accompanying text*; see also infra* Parts II(A)(2)(a) and II(A)(2)(b).

[217] *See supra* notes 29-31 and accompanying text.

[218] *See supra* note 95 and accompanying text.

[219] JOHN STEWARD, EVOLUTION'S ARROW: THE DIRECTION OF EVOLUTION AND THE FUTURE OF HUMANITY 116 (2000), *available at* http://www4.tpg.com.au/users/jes999/Part%204.pdf; *see also* Wilson, *supra* note 27*,* at 553-54, 569.

[220] *See supra* notes 29-31 and accompanying text.

[221] The social order described above is characteristic of characteristic of a "complex" hunter-gatherer band. *See, e.g.,* Paul Rubin, *Hierarchy*, 11 HUMAN NATURE 259 (2000) (noting the distinction between "simple" hunter-gatherers and "complex" hunter-gatherers; the former are "mobile, egalitarian, live in small settlements and the only 'occupational specialization' is by age," while the latter are organized by a dominance hierarchy and possess a division of labor).

[222] There are other similarities between human social organization at this stage of is evolution and the behavior of wolves. Like wolf packs, human bands were territorial; and

male who had gained authority over the others by birthright or physical prowess.[223] The dominant male directed the basic activities of the band: summoning the other men for hunting or defense, leading them in these and other essential activities, directing the movements of the band as it migrated from place to place, and orchestrating its relations with other, non-hostile bands.[224] The division of labor was gender-based; men hunted while women remained in the band's camp to raise children and gather food.[225] While conflict was certainly not absent from these bands, this minimal set of rules sufficed to maintain the level of internal necessary order for survival. These rules channeled the efforts of the members of the band in productive directions; this ensured performance of the tasks needed to sustain the band and limited the behavioral options open to the band members.[226]

Once agriculture was invented, "populations increased enormously in density, and the primitive hunter-gatherer bands gave way . . . to the relentless growth of tribes, chiefdoms, and states."[227] As human social systems grew in size, they also grew in complexity. This complexity extended to the constitutive rules that set the baseline for social order in a system.[228] The constitutive rules still specified the contours and staffing of system authority (i.e., government) and the division of labor, both of which became more complex; they also expanded into other areas. Constitutive rules came, for example, to govern such matters as: (a) the categories, identities and number of

---

like wolves, humans played. *See, e.g.,* WILSON, *supra* note 27, at 567-68.

[223] *See infra* Part II(A)(2)(b). For a theoretical model of why dominance evolves even in small human social groupings, *see, e.g.,* James L. Boone, *Competition, Conflict, and the Development of Social Hierarchies, in* EVOLUTIONARY ECOLOGY AND HUMAN BEHAVIOR 301-37 (Eric Alden Smith, *et al.,* eds. 1992)*; see also* Polly Weissner, *Leveling the Hunter Constraints on the Status Quest in Foraging Societies*, *in* Food AND THE STATUS QUEST: AN INTERDISCIPLINARY PERSPECTIVE 171-88 (Wulf Schiefenhovel & Polly Weissner, eds. 1995). Physical prowess would have been the original mode of gaining authority, just as it is with wolves. As human social life evolved in complexity, the notion of inherited authority appeared, supplementing, if not replacing, physical prowess. *See, e.g.,* ALBERT SOMIT & STEVEN A. PETERSON, DARWINISM, DOMINANCE, & DEMOCRACY: THE BIOLOGICAL BASES OF AUTHORITARIANISM 53 & 62 n. 2 (1997) (noting the inheritance of dominance in chimpanzees and other non-human species).

[224] In addition to these routine matters, the dominant male would no doubt deal with challenges to his authority, resolve conflicts between members of the band and, perhaps, make decisions about mating between members of his band and members of other bands.

[225] *See, e.g.,* WILSON, *supra* note 27, at 553-54, 566, 569.

[226] *See infra* Part II(A)(2)(b).

[227] WILSON, *supra* note 27, at 569.

[228] *See, e.g.,* DAVID RONFELDT, TRIBES, INSTITUTIONS, MARKETS, NETWORKS: A FRAMEWORK ABOUT SOCIAL EVOLUTION 5-17 (RAND 1996), *available at* http://www.rand.org/publications/P/P7967/P7967.pdf*; see also* SCHAUER, *supra* note 87, at 168 (discussing "permissions" and power-conferring rules).

individuals one can marry; (b) the ages and conditions under which one can marry; (c) the conditions and constraints, if any, placed upon reproduction; (d) the endeavors one can/must engage in to "earn a living" (i.e., to obtain the resources needed to survive and reproduce); (e) the duties and practices involved in religious observances; (f) the terms and conditions upon which one can validly enter into contractual agreements with others; (g) one's right to recompense from another who inadvertently causes injury or loss; (h) the obligations one owes to one's family; and (i) the obligations one owes to the social system itself (which can range from paying taxes to serving in the military).[229]

In more evolved social systems, constitutive rules come in two forms: norms, the informal consensus-based standards that define what is, and is not, "correct" behavior and laws, the formally adopted standards governing behavior, obligations and expectations.[230] Both work to sustain social order,

---

[229] *See generally* HENRY MAINE, ANCIENT LAW, Chapter 5 (1861); CLAUDE HERMANN WALTER JOHNS, BABYLONIAN LAW – THE CODE OF HAMMURABI*, in* Encyclopedia Britannica (1910-11). *See, e.g.,* The Code of Hammurabi, The Avalon Project at Yale Law School, *at* http://www.yale.edu/lawweb/avalon/medieval/hamframe.htm (last visisted Mar. 30, 2003); Laws of the Kings, http://www.yale.edu/lawweb/avalon/medieval/laws_of_thekings.htm (last visisted Mar. 30, 2003); The Statute of Laborers (1351), http://www.yale.edu/lawweb/avalon/medieval/statlab.htm (last visisted Mar. 30, 2003)*;see also* Tacitus, Germania, http://www.fordham.edu/halsall/basis/tacitus-germanygord.html (last modified Sept. 1998).

The extent to which constitutive rules define and circumscribe the behavioral options of its respective members varies with the nature of the social system; feudal societies, for example, were characterized by an intricate system of constitutive rules. *See, e.g.,* NORMAN F. CANTOR, THE CIVILIZATION OF THE MIDDLE AGES 195-204, 465-73 (1994).

[230] *See, e.g.,* ROBERT K. MERTON & ROBERT A. NISBET, CONTEMPORARY SOCIAL PROBLEMS: AN INTRODUCTION TO THE SOCIOLOGY OF DEVIANT BEHAVIOR AND SOCIAL DISORGANIZATION 21-22 (1961).

> All societies have rules that specify appropriate and inappropriate ways of behaving. These . . . 'norms' . . . are sets of directions for behavior, and members of a society are expected to follow them. When a child is born, he . . . comes under the influence of the . . . 'society,' in which he lives . . . . [W]hat he is fed, when he is fed, and how he is fed all are determined by norms existing in advance of his arrival. And as he grows older . . . he is increasingly expected to conform to norms himself . . . .
>
> [N]orms . . . are not all of equal importance. The most important ones have been called *mores,* and they constitute the basic rules that are . . . holding a society together. When the mores are violated, members of the society respond with great moral indignation; punishment is likely to be quite severe . . . . [A]cts, such as cannibalism, rape, and murder, are violations of mores. Less important norms are called *folkways,* and punishments for violation of them are likely to be quite mild . . . . Rules about table manners, styles of dress, and etiquette are folkways . . . . [T]he *criminal law* is a body of rules stipulating that anyone violating certain folkways and mores will be considered a criminal and will be *officially* punished (emphasis in the original).

Id.; see also Richard A. Posner & Eric B. Rasmussen, *Creating and Enforcing Norms with*

but they do so in different ways: norms operate internally; to the extent the members of a social system accept and internalize its norms, they will seek to conform their behavior to the standards the norms embody.[231] Laws can operate both internally and externally; the members of a social system will conform their behavior to its laws because they accept the legitimacy of the standards they embody and/or because they seek to avoid the consequences of not doing so.[232] Constitutive laws and norms create and maintain social order by providing direction (indicating the choices members of a social system should make and the behaviors they should engage in) and channeling behavior in socially constructive directions.[233] Their effectiveness is due in large part to

Special Reference to Sanctions, 19 INT'L REV. L. & ECON. 369, 369-72 (1999).

[231] *See, e.g.,* MERTON & NISBET, *supra* note 230, at 21-22*; see also* Cristiano Castelfranchi, *Engineering Social Order*, First International Workshop on Engineering Societies in the Agents' World (2000), *available at* http://lia.deis.unibo.it/confs/ESAW00/pdf/ESAW04.pdf.

Norms have historically been effective because there was little in the way of behavioral innovation; the rise and proliferation of technology, however, can undermine the effectiveness of norms as an agent of social control. *See, e.g.,* CNN.com, *Cam Phones Spread New Brands of Mischief,* (July 10, 2003), *available at* http://www.cnn.com/2003/TECH/ptech/07/10/naughty.camphones.ap/index.html ("'The problem with a new technology is that society has yet to come up with a common understanding about appropriate behavior,' said Mizuko Ito, an expert on mobile phone culture.").

[232] *See, e.g.,* MAX. WEBER, ECONOMY AND SOCIETY 34 (G. Roth & C. Wittich ed. 1978) ("An order will be called . . . law if it is externally guaranteed by the probability that . . . coercion will be applied by a staff of people . . . to bring about compliance or avenge violation.")*; see also* EDWIN M. SCHUR, LAW AND SOCIETY: A SOCIOLOGICAL VIEW 76 (1968); MAX WEBER ON LAW IN ECONOMY AND SOCIETY 5 (Max Rheinstein, ed., trans. by E. Shils & M. Rheinstein 1954). The "consequences" cited above are not the relatively Draconian consequences attendant upon failing to conform to the dictates of the criminal law, which is discussed later in the text. The "consequences" attendant upon failing to conform to the dictates of civil, constitutive law are less onerous in nature and, indeed, may take the form of a default; if, for example, one purports to enter into marriage without having obtained the necessary license and otherwise complying with the requirements of the constitutive law, the marriage will null and void. *See, e.g.,* ALA. CODE § 30-1-9 (1998) ("No marriage shall be solemnized without a license.")*; see also* Parks v. Martinson, 694 So.2d 1386, 1390 (Ala. Civ. App. 1997).

[233] *See, e.g.,* WILSON, *supra* note 27, at 562:

> The extreme plasticity of human social behavior is both a great strength and a real danger. If each family worked out rules of behavior on its own, the result would be an intolerably amount of tradition drift and growing chaos. To counteract selfish behavior and the 'dissolving power' of high intelligence, each society must codify itself.

Id. (quoting HENRI BERGSON, THE TWO SOURCES OF MORALITY AND RELIGION (1935)); *see also* H.L.A. Hart, *Law as the Union of Primary and Secondary Rules, in* THE NATURE OF LAW 144, 145 (M. P. Golding ed. 1966) ("Legal rules defining the ways in which valid

the socialization process all members of a human social system undergo; it is in the course of this process that the members of a social system internalize its constitutive rules and learn to follow them.[234]

The laws embodying constitutive rules are the "civil law" of an evolved human social system; they are "rule[s] of civil conduct, prescribed by the supreme power in a state, 'commanding what is right.'"[235] Constitutive rules are sufficient to maintain order in social systems populated by entities that are not "intelligent."[236] As explained earlier, intelligence introduces a "wild card" – the possibility of choice.[237] Choice means that the entities who populate a social system can decide (a) what the rules are and (b) whether or not they, as individuals, will follow a particular rule or set of rules. Their intelligence determines the extent of their ability to make these choices; the greater their intelligence, the greater their ability to make these choices.[238] Humans, who are equipped with what Henri Bergson called the "dissolving power" of intelligence,[239] can make these decisions. The existence of that ability creates a direct and intolerable threat to social order: if each member of a social grouping can decide for him or herself whether to follow the constitutive rules in effect in that system, the rules are of no import; the system essentially exists in a state of anarchy because each member can freely elect to abide by its constitutive "civil" rules or ignore them.[240] This erodes the system's ability to maintain order in two ways:[241] (1) essential functions are not performed because individual behavior is not structured and channeled in socially

---

contracts or wills or marriages are made do not require persons to act in certain ways whether they wish to or not. Such laws do not impose duties or obligations. Instead, they provide individuals with *facilities* for realizing their wishes.") (emphasis in the original).

[234] *See, e.g.,* BERGER & LUCKMANN, *supra* note 10, at 129-47.

[235] 3 WILLIAM BLACKSTONE, COMMENTARIES 1.

[236] Systems populated by ants and other social insects, for example, have only constitutive rules. *See infra* Parts II(A)(2)(a) and II(A)(2)(b). For the definition of "intelligence" used in this article, *see supra* notes 42-44 and accompanying text.

[237] *See supra* note 233; *see also supra* notes 42-44 and accompanying text.

[238] *See infra* Parts II(A)(2)(a) and II(A)(2)(b).

[239] *See supra* note 233*; see also supra* notes 42-44 and accompanying text.

[240] *See supra* note 34 and accompanying text*; see, e.g.,* COHEN, *supra* note 34, at 11 ("Deviance, if not contained, is always a threat to organization."). *See generally* THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2000) (defining anarchy as "[a]bsence of any common cohesive principle, such as a common standard or purpose"), *available at* http://www.bartleby.com/61/20/A0282000.html.

[241] For a slightly different perspective, *see, e.g.,* COHEN, *supra* note 34, at 4 (stating that deviance destroys social organization in three ways: (1) by disrupting coordinated processes; (2) by destroying people's willingness to play their parts in the system; and (3) by destroying one's faith that other members of the system will play their parts in the system).

constructive ways; and (2) socially destructive behavior proliferates because one person's inclination to prey upon other can prompt decisions not to abide by the "civil" rules.[242] Each of these alternatives is the product of deviant behavior; that is, each represents behavior which is predicated upon a deliberate decision not to conform conduct to the dictates of the constitutive rules in effect in the social system.[243]

We have not addressed the possibility of deviant behavior because we have been concentrating on the tactics systems use to *create* order; that is, we have been concentrating on how social order emerges from the interaction of constituent entities whose behavior is ordered by a set of relatively simple rules.[244] As explained earlier, deviant behavior, which serves to destroy order, is not an issue in systems that are populated by less intelligent entities whose behavior is biologically constrained.[245] The primary threats to social order in these systems are external, posed by competing systems composed of members

---

[242] "Preying upon" another can take any of a variety of forms, including sexual attack, theft, fraud, physical assault, and murder. It is, perhaps, helpful to illustrate the behaviors, and results, that fall into each category: If a parent chose not to provide for his children, a function essential for the survival of the system would not be performed. *See supra* note 29 and accompanying text. If a man chooses to murder his neighbor's children, this would constitute socially destructive behavior.

[243] *See supra* note 89 and accompanying text.

> Jeremy Chase admits to shaking down his enemies. His Web site advertises extortion, hits and prostitution for a hefty fee.
>
> Chase is a mob leader – but only in the virtual world. He is one of hundreds of players who found the path of lawlessness and deviance too irresistible when 'The Sims Online' challenged them to 'Be Somebody . . . else.'
>
> The popular . . . game . . . is turning into a petri dish of anti-social behavior. And that's raising questions about whether limits on conduct should be set in such emerging virtual worlds . . . .

CNN, *Sex, Mob Hits: Sims Tests Virtual Morals,* (July 5, 2003), *at* http://www.cnn.com/2003/TECH/fun.games/07/05/misbehaving.online.ap/index.html*; see also id.* ("'We're going to be forced to create a whole new area of social convention – and probably law – that reflects that kind of behavior,' said psychologist David Greenfield.").

[244] *See infra* Parts II(A)(2)(a) and II(A)(2)(b).

[245] The same is true of systems populated by intelligent artificial entities as long as their behavior is subject to constraints which operate in a fashion analogous to those biology imposes on most species. *See, e.g.,* EPSTEIN & AXTELL, *supra* note 31, at 23-26. If a social system were populated by artificial entities (a) whose intelligence was at least comparable to that of humans and (b) who were not subject to constraints analogous to those that channel the behavior of non-human biological species, then that system could confront the possibility of deviant behavior. To be truly "deviant," though, behavior has to originate in the intellect and autonomy; deviant behavior, in other words, has to be contumacious. *See supra* note 89 and accompanying text. *See also* THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2000) (defining contumacious as "[o]bstinately disobedient or rebellious"), *available at* http://www.onelook.com/?w=contumacious&ls=a.

of the same species or by predators.[246]

Systems populated by humans (and entities with equivalent capacities)[247] must confront the problem of deviant behavior; constitutive rules are not enough to maintain order in these systems.[248] To prevent the erosion of social order, systems populated by humans (and equivalent entities) must therefore come up with a solution, a way to defeat and discourage deviant behavior. The solution human social systems have used for several millennia is to create a new set of rules – criminal rules – that essentially require members of the system to follow the "civil" rules, i.e., the constitutive rules that constitute the system.[249]

Human systems essentially employ a tripartite system to maintain internal order. The first and most basic device is the internal controls implemented by the unwritten rules – the norms every member of the social system learns in their socialization process. Individual internalization of these norms is the primary technique used to establish order at a very basic level. The second device is the constitutive rules, which supplement the norms by defining appropriate behavior at a higher level of complexity. For example, while norms dictate that individuals should support their children, a system may well find it necessary to establish constitutive rules which formalize this obligation and attach consequences to one's failure to discharge it. The third device is the criminal rules which are used for those who respond neither to the informal

---

[246] *See infra* Parts II(A)(2)(a) and II(A)(2)(b).

[247] *See supra* note 245.

[248] *See supra* notes 235-43 and accompanying text.

[249] *See* PAUL H. ROBINSON, STRUCTURE AND FUNCTION IN CRIMINAL LAW 125 (1997) ("[Criminal law] defines and announces the conduct that is prohibited . . . . Such 'rules of conduct' . . . provide *ex ante* direction to the members of the community as to the conduct that must be avoided . . . upon pain of criminal sanction."); *see also* OLIVER WENDELL HOLMES, THE COMMON LAW 42 (Mark DeWolfe Howe ed., 1963) (stating that the "purpose of the criminal law is . . . to induce external conformity to rule."); EDWIN M. SCHUR, LAW AND SOCIETY: A SOCIOLOGICAL VIEW 72 (1968) (noting that "mechanisms of social control are required in all societies" to deal with the "conflict and deviance" that "constitute integral aspects of social life"); MODEL PENAL CODE § 1.02(1)(a) (1962) (stating that the purpose of criminal law is to "forbid and prevent conduct that unjustifiably . . . inflicts or threatens substantial harm to individual or public interests."); *see, e.g.,* The Code of Hammurabi, The Avalon Project at Yale Law School, *available at* http://www.yale.edu/lawweb/avalon/medieval/hamframe.htm (last visisted Mar. 30, 2003); The Salic Law, The Avalon Project at Yale Law School, *at* http://www.yale.edu/lawweb/avalon/medieval/salic.htm (last visisted Mar. 30, 2003). *See generally* Hart, *supra* note 233.

The "civil" rules in a system can be, and often are, defined to include consequences that follow upon a failure to follow a particular rule. These consequences can consist of civil litigation brought either by a private party or by the system itself. They can also take the form of fines or other regulatory sanctions imposed by the system.

dictates of the norms nor to the institutionalized commands of the constitutive rules.

Criminal rules will therefore be linked to the "civil" constitutive rules that define the basic structure of expectations and obligations which constitute a social system. Social systems, for instance, consistently, if not inevitably, adopt constitutive rules that define parent-child relationships and obligations. These rules address such matters as whether (and under what circumstances) adults are allowed to reproduce,[250] the circumstances under which a child will be deemed to be legitimate (which often triggers other constitutively-defined obligations),[251] to whom the custody of a child belongs,[252] who is obligated to provide care and support for children and for how long that obligation lasts.[253] Correlative criminal rules impose criminal liability and penalties on those who do not abide by these "civil" constitutive rules.[254] The same dynamic exists in

[250] Constitutive rules can also govern whether or not a lawfully-born child will be allowed to live. *See, e.g.,* CYNTHIA B. PATTERSON, THE FAMILY IN GREEK HISTORY 74 (1998) (describing how Spartan fathers took their children to a council of elders, who decided whether it should live). Such rules can also govern the number of children those who are allowed to reproduce can lawfully have. *See, e.g.,* Kate Xiao Zhou, *The Family Revolution in Contemporary China*, *in* THE FAMILY IN GLOBAL TRANSITION 201-04 (Gordon L. Anderson ed. 1997) ("one child rule").

[251] *See, e.g.,* 750 ILL. COMP. STAT. 5/303 (1993)*; see also* JOHN L. ESPOSITO, WOMEN IN MUSLIM FAMILY LAW 28 (1982) (discussing the rules determining legitimacy in classical Islamic law).

[252] *See, e.g.,* ARK. CODE Ann.§ 9-10-113 (2002) (custody of illegitimate child); CONN. GEN. STAT. ANN. § 46b-56b (2004) (presumption of parental custody)*; see also* J.S. La Fontaine, *The Family in Early Modern England, in* THE FAMILY IN GLOBAL TRANSITION 102-105 (Gordon L. Anderson ed. 1997) (discussing how in early modern England, families often sent their children to live with others, e.g. wet-nurses, employers or relatives).

[253] *See, e.g.,* MONT. CODE ANN. § 40-6-211 (2001) ("The parent or parents of a child shall give the child support and education suitable to the child's circumstances."); IND. CODE § 31-14-11-19 (1999) (duty to support child is terminated by emancipation)*; see also* JANE F. GARDNER, FAMILY AND FAMILIA IN ROMAN LAW AND LIFE 6-113 (1998). Constitutive rules governing emancipation also establish affirmative rules of conduct; that is, one a child has been emancipated, the parent is obliged to recognize that emancipation and behavior in accordance with the child's new status. *See id.*

[254] *See, e.g.,* CAL. PENAL CODE § 270 (1999) ("If a parent of a minor child willfully omits . . . to furnish necessary clothing, food, shelter or medical attendance, or other remedial care for his or her child, he or she is guilty of a misdemeanor punishable by a fine not exceeding two thousand dollars ($2,000), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.")*; see also* WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 6.2(a)(1) (2003) ("[A] parent may be guilty of criminal homicide for failure to call a doctor for his sick child [and] a mother for failure to prevent the fatal beating of her baby by her lover.").

other areas: Constitutive rules define property and concept of ownership;[255] criminal rules impose liability and penalties on those who violate these "civil" rules by stealing or destroying another's property.[256] There is, though, another type of criminal rule. The rules in this additional category are not specifically linked to constitutive rules; these are the rules that impose criminal liability and sanctions for conduct that violates another individual's legitimate expectations of life, liberty and safety.[257] Most social systems do not explicitly articulate the legitimacy of such expectations vis-à-vis other members of that system, perhaps because they are such deeply-embedded assumptions that it does not seem necessary.[258]

Since the capacity for deviant behavior is a constant across human populations, every social system will have criminal rules. These rules will be designed to maintain the integrity of several vital interests: the safety of persons; the security of property; the stability of the government; and the sanctity of particular moral principles.[259] No system can survive if its

[255] *See, e.g.,* CAL. CIV. CODE § 654 (1982) ("The ownership of a thing is the right of one or more persons to possess and use it to the exclusion of others. In this Code, the thing of which there may be ownership is called property."); MONT. CODE ANN. § 70-1-101 (2001) ("The ownership of a thing is the right of one or more persons to possess and use it to the exclusion of others. In this code, the thing of which there may be ownership is called property.").

[256] *See, e.g.,* LAFAVE, *supra* note 254, §§ 19.8 (theft) & 21.3 (arson).

[257] These rules address what are often called "crimes against persons." *See, e.g.,* MODEL PENAL CODE § 210.1(1) (1962) ("A person is guilty of criminal homicide if he . . . causes the death of another human being.") *See also LAFAVE,supra* note 254, § 213.1 (rape) & § 212.1 (kidnapping); William L. Barnes, Jr., *Revenge on Utilitarianism: Renouncing a Comprehensive Economic Theory of Crime and Punishment,* 74 IND. L.J. 627, 649 (1999).

[258] *See supra* note 230. The U.S. Constitution and many state constitutions do contain provisions that refer to general expectations, such as "enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. art. I § 1 (1849)*; see also* U.S. CONST. amends. v & xiv § 1; COL. CONST. art. II § 3; IND. CONST. art. I § 1; IOWA CONST. art. I § 1; KY. CONST. § 1; N.D. CONST. art. I § 1; VA. CONST. art. I § 1. But these provisions are not the constitutive correlates of criminal rules that impose liability for what are often called "crimes against persons." They are due process guarantees that constrain government, not individual action. *See, e.g.,* In Interest of Reginald D., 533 N.W.2d 181, 184-85 (Wis. 1993) (finding that the provision of Wisconsin Constitution guaranteeing "life, liberty and the pursuit of happiness is the state equivalent of the due process clause of the Fourteenth Amendment.")*; see also* Jack Stark, *A Practical Guide to Drafting State Constitutional Provisions,* 73 TEMP. L. REV. 1061, 1067 (2000); John Devlin, *Constructing an Alternative to "State Action" as a Limit on State Constitutional Rights Guarantees: A Survey, Critique and Proposal,* 21 RUTGERS L.J. 819, 850-52 (1990).

[259] *See, e.g.,* PORTUGAL CÓDIGO PENAL (2003), *available at* http://www.cea.ucp.pt/lei/penal/penalind.htm; CRIMINAL CODE OF THE RUSSIAN SOVIET

constituents are free to harm each other at will, to appropriate each other's property, to undermine the political order and/or to flout the moral principles the citizenry hold dear.[260] Every society will therefore formulate penal prohibitions defining (i) crimes against persons (e.g., murder, assault, rape); (ii) crimes against property (e.g., theft, arson, fraud); (iii) crimes against the state (e.g., treason, rioting, obstruction of justice); and (iv) crimes against morality (e.g., obscene materials, defiling a place of worship).[261] As to the content of these rules, the greatest degree of consistency will occur in the first two categories because they intrinsically involve citizens preying upon each other, something no social system can tolerate if it is to survive. There will be a fair degree of consistency on a core of rules in the third category – e.g., treason, riot, and obstructing justice – because every social system must ensure the stability of its political order.[262] Beyond this core, there will be more deviation in the rules that fall into this category because nations vary in terms of the extent to which they feel it necessary to discourage political dissidence.[263] Finally, there will be a great deal of inconsistency as to rules in the fourth category because they are the product of a society's values and religious principles and, as such, tend to be much more idiosyncratic in nature.[264]

FEDERATED SOCIALIST REPUBLIC (1934), *available at* http://www.tiac.net/users/hcunn/rus/uk-rsfsr.html.

[260] *See generally* Michael E.Tigar, *Crime Talk, Rights Talk, and Double-Talk: Thoughts on Reading the Encyclopedia of Crime and Justice,* 65 TEX. L. REV. 101, 108 (1986) ("When the powerful prey upon the weak . . . the criminal law has a legitimate concern.").

[261] *See* H.L.A. Hart, *Law as the Union of Primary and Secondary Rules, in* THE NATURE OF LAW 144, 145 (M. P. Golding ed. 1966) (noting that society must enact "in some form restrictions on the free use of violence, theft, and deception to which human beings are tempted but which they must, in general, repress if they are to coexist in close proximity to each other."); *see, e.g.,* CRIMINAL CODE OF THE REPUBLIC OF BELARUS (1996), *available at* http://www.belarus.net/softinfo/lowcatal.htm; GERMAN PENAL CODE; THE INDIAN PEN. CODE; *see also* MODEL PENAL CODE (1962).

[262] *See, e.g.,* FIJI ISLANDS PENAL CODE, §§ 50 (treason), 87 (unlawful assembly) & 130 (destroying evidence) (1978), *available at* http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; REVISED PENAL CODE OF THE PHILIPPINES, Articles 114 (treason), 153 (tumults and other disturbances of public order) & 180-81 (false testimony) (1930), *available at* http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm.

[263] *See, e.g.,* CRIMINAL CODE OF THE RUSSIAN SOVIET FEDERATED SOCIALIST REPUBLIC (1934), § 58-12, *available at* http://www.tiac.net/users/hcunn/rus/uk-rsfsr.html ("Failure to denounce a counterrevolutionary crime, reliably known to be in preparation or carried out, shall be punishable by . . . deprivation of liberty for a term not less than six months.").

[264] *Compare* ZAMFARA STATE OF NIGERIA, SHARI'AH PENAL CODE LAW §§ 126 & 127 (Jan. 2000) (fornication and adultery offenses), *available at* http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html, *with* CONN. GEN.

All of these rules are designed to establish and maintain internal order. They are, therefore, formulated by the members of a particular human social system and are applied to those who constitute that social system throughout time.[265] Human systems, like systems populated by other species, must also maintain external order.[266] The rules that establish and maintain internal order in human systems play an essential role in efforts to maintain external order insofar as they allow the system to focus its resources on external threats; if a social system is undergoing inner turmoil, it is likely to experience difficulty in fending off external threats.[267] The rules that establish and maintain internal order have not, historically, been otherwise implicated in the system's efforts to resist external threats because they simply did not apply to the nature and source of external threats. External threats to a system historically came from another system – another group of human beings. The other system could be another band, another tribe, another principality or another state, but it was always comprised of a separate populace with a distinct identity and its own agenda.[268] Consequently, the rules one system devised to maintain internal order, including criminal rules, were quite ineffectual against external threats posed by a second system because (a) the members of the "other" system were in no way bound to abide by these rules and (b) the conduct involved in the external threat was not conduct addressed by these rules.[269] Section III

STAT. § 53a-81 (date) (adultery offense repealed) *and* D.C. CODE ANN. § 22-1001 (fornication offense repealed). *See also* FIJI ISLANDS PENAL CODE, §§ 145 (insult to religion) & 232 (witchcraft and sorcery), *available at* http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html (last visited Mar. 30, 2004); REVISED PENAL CODE OF THE PHILIPPINES, Article 200 (1930) (grave scandal), available at http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm; UNITED ARAB EMIRATES PENAL CODE Article 358 (1988) (offense of committing "publicly an infamous act constituting a violation of the rules of decency").

[265] *See generally* Hart, *supra* note 261, at 216 (noting that the term "state" is a "way of referring to two facts: first, that a population inhabiting a territory lives under that form of ordered government provided by a legal system with its characteristic structure of legislature, courts, and primary rules; and, secondly, that the government enjoys a vaguely defined degree of independence.").

[266] *See supra* notes 30-33 and accompanying text.

[267] *See, e.g.,* D.F. FLEMING, THE COLD WAR AND ITS ORIGINS, 1917-1960 3-27 (1961) (discussing the negative impact of Russian Revolution on Russia's participation in World War I).

[268] *See, e.g.,* PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY 75-205 (2002).

[269] *See, e.g.,* Mark A. Summers, *The International Court Of Justice's Decision In Congo V. Belgium: How Has It Affected The Development Of A Principle Of Universal Jurisdiction That Would Obligate All States To Prosecute War Criminals?,* 21 B.U. INT'L L.J. 63, 69-70 (2003) (noting that "[t]erritory . . . is the bedrock of criminal law jurisdiction", with some

explains how cybercrime alters assumptions about the relationship between internal order and external threats.

As to internal order, the existence of a set of criminal rules – a criminal law – is only one part of what is involved in maintaining internal order. Implicit in the notion of a criminal law is the premise that some members of a social system will obdurately violate the rules that govern behavior within the system; indeed, this is why criminal rules are needed. But criminal rules do not merely prohibit certain behaviors; they also prescribe the consequences of engaging in such behavior.[270] Prescribing consequences, though, is not enough; there must be some mechanism, some process, in place which ensures that these consequences are imposed upon those who violate applicable criminal rules.[271] The section immediately below and § II(B), *infra*, examine this process.

3. Control

Fatta la legge, trovato l'inganno.[272]

Our analysis of social systems populated by ants, wolves and humans shows that there are two very different ways of approaching the problem of maintaining order in a social system. One is the lateral, distributed approach found among ants and other social insects. In an ant colony, there is no "authority" – social order emerges from and is sustained by the interactions of the constituent members of the colony, none of which are individually "intelligent:"

> [A]nt colonies . . . form long-range structures without relying on the centralized, hierarchical control used in human organizations . . . . A dramatic example is the army ant raids. Army ant colonies comprise hundreds of thousands of individuals . . . . [T]he swarm behaves as a

exceptions)*;* Chris Jochnick & Roger Normand, *The Legitimation of Violence: A Critical History of the Laws of War,* 35 HARV. INT'L L. J. 49 (1994). (defining "war crimes," but these atypical rules transcend the structure of individual systems); Jeremy Colwill, *From Nuremberg to Bosnia and Beyond: War Crimes Trials in the Modern Era,* 22 SOCIAL JUSTICE 111 (1995).

[270] *See*, *e.g.,* Hall, *supra* note 31, at 296-97.

[271] *See*, *e.g.,* GEORGE P. FLETCHER, BASIC CONCEPTS OF CRIMINAL LAW 7 (1998) ("Whether one is ever held liable for a particular offense depends on the rules of procedure. These rules determine how the state enforces the criminal law by . . . convicting and punishing those responsible.").

[272] The Italian proverb quoted above translates as "the law has been made, the loophole has been found" or, more literally, "made the law, found the loophole." *See, e.g.,* Proverbi e detti italiani, *at* http://www.italissimo.de/Proverbi.htm (last visited Dec. 17, 2003). Neil Mitchison, of the European Commission's Joint Research Centre in Ispra, Italy, was kind enough to call the proverb to the author's attention and to provide the translations.

> single entity, searching and expanding . . . as though guided by some kind of intelligence. The colony, however, is blind and responds only to local concentrations of pheromones laid down by its individual members. There is no central control or individually complex behavior. This emerges from the interactions between ants.[273]

Lateral constitutive rules suffice to establish and maintain order in systems such as this because there is no potential for deviant behavior.[274] Lacking that potential, the system has no need for a set of criminal rules and for a mechanism to enforce those rules.

Systems populated by intelligent entities must confront the potential for deviant behavior, i.e., the possibility that individual members will violate system rules. Because the entities who comprise these systems are intelligent, they are also volitional and can elect not to conform their behavior to system dictates. Such systems cannot, therefore, rely only on internal controls to establish order; they must also institute measures that exert a level of external control upon the behavior of the members of a system. These measures become the "authority" that enforces the rules of a system.[275] In a wolf pack, authority is relational: Subordinate wolves' relationship to the alpha male and to each other determines the behavioral rules each must follow; if a wolf violates one of these rules, the alpha male or whichever wolf is the target of the violation will respond in an effort to bring the offender in line.[276] If the offender submits to the authority of the wolf who reacts to his/her misbehavior, order is restored; if the offender overcomes the reacting wolf, a new order is restored.[277] This is a classic example of a dominance hierarchy.[278]

"Pure" dominance hierarchies, which are based on relational rules, are typically the means by which intelligent species maintain order in small social

---

[273] GOODWIN & SOLAE, *supra* note 59, at 149-50; *see also supra* Part II(A)(2)(a).

[274] *See supra* Part II(A)(2).

[275] *See, e.g.,* J.S. EROS, KARL MANNHEIM & W.A.C. STEWART, SYSTEMATIC SOCIOLOGY: AN INTRODUCTION TO THE STUDY OF SOCIETY 126 (1957).

> [C]ontrol is based upon the existence of authority. There are people of authority, there are statements of authority. There is no social order without authority . . . . Most societies are built up on an elaborate system of controls among which physical force is only a last resort.

[276] *See supra* Part II(A)(2)(b).

[277] *See supra* Part II(A)(2)(b).

[278] "Dominance is . . . the outcome of a competitive encounter where the prize for the contest winner is prerogative to pursue desired incentives without interference from the loser." PATRICIA R. BARCHAS & SALLY P. MENDOZA, EMERGENT HIERARCHICAL RELATIONSHIPS IN RHESUS MACAQUES: AN APPLICATION OF CHASE'S MODEL IN SOCIAL HIERARCHIES: ESSAYS TOWARD A SOCIOPHYSIOLOGICAL PERSPECTIVE 81 (Patricia R. Barchas, ed. 1984).

systems, such as a wolf pack or a band of hunter-gatherers.[279] As social systems grow in size, relational rules cease to become an effective means of maintaining order within a system; the size of the constituent population means that the web of relationships becomes too complex to function efficiently.[280] To understand why this is so, imagine a wolf pack composed of a thousand wolves: There is one alpha male and one alpha female, but there are many, many beta males and beta females, many, many gamma males and gamma females, and so on. Relying on relational rules – with their attendant patterns of challenge, response and resolution (which can alter the structure of the relational rules) – would leave the system in chaos.[281]

Wolves do not live in packs of thousands or hundreds of thousands or millions, so they can continue to rely on relational rules. Humans, however, evolved ever-larger social systems and, as the size of these social systems increased, found it necessary to develop a different approach to maintaining order. Humans gradually replaced relational rules with structural rules; unlike relational rules, structural rules are institutionalized and apply categorically.[282] Structural rules have been formally adopted according to some accepted process and apply categorically across a set or subset of the population of a social system.[283] They are, therefore, not legitimately subject to testing by individual members of that population; the members of the population are bound to accept and abide by the structural rules which apply to them.[284] This eliminates the potential for chaos that results from the challenges that are an integral part of the relational rules which comprise a dominance hierarchy.[285] In a system populated by volitional entities, it does not eliminate the possibility that some members of the system will refuse to abide by these rules. This

---

[279] *See supra* Part II(A)(2).

[280] *See, e.g.,* Hart, *supra* note 233.

[281] BARBARA W. TUCHMAN, A DISTANT MIRROR: THE CALAMITOUS 14TH CENTURY 482 (1978) (Wenceslas IV of Bohemia "lacked the character to dominate" his subjects; "the incessant warring of groups and classes, of towns versus princes, lesser nobles against the greater . . . created a network of dissension that defied sovereignty – and destroyed the sovereign.").

[282] *See, e.g.,* MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION 324-86 (A.M. Henderson & Talcott Parsons trans. 1947)*; see supra* notes 1, 177-78 and accompanying text.

[283] *See supra* notes 1, 177-78 and accompanying text*; see, e.g.,* M. MARVIN BERGER & MARTIN ALAN GREENBERG, AUXILIARY POLICE, THE CITIZEN'S APPROACH TO PUBLIC SAFETY 14 ("[A]s ancient villages became ancient kingdoms additional norms were imposed upon the community and these norms were set down in written form.").

[284] *See supra notes* 1, 177-78 and accompanying text; WEBER, *supra* note 282, at 324-386. The process was gradual, and relational rules persisted, in some form, for centuries. *See* CANTOR, *supra* note 229, at 195-204, 465-473.

[285] *See supra* notes 1, 177-78 and accompanying text; WEBER, *supra* note 282, at 324-86.

requires the incorporation of a control mechanism, of some system for enforcing the structural rules. As Part II(B) explains, human social systems developed different approaches to enforcing their structural rules, particularly their criminal rules, over the course of human history; as that section also explains, the current approach, like a dominance hierarchy, concentrates the power and authority to respond to violations of criminal rules in a small subset of the population of the social system.

4. Territory

As noted earlier, the rules human social systems devise to maintain system order are, for the most part, territorially-based.[286] That is, each social system is situated in a physical space to which it lays claim by the tenets of the law, by the force of weapons and/or by whatever other standard applies. This is a trait human social systems share with wolf packs, ant colonies and, indeed, all real-world social systems, that is, all of the social systems that have heretofore been established by biological species. This is, as Part III explains, a trait that can make the enforcement of system rules problematic when the conduct at issue occurs in or is mediated through cyberspace.

B. Model

> *[S]overeignty . . . is rooted to . . . territory and is contingent on the ability of the state to protect its citizens, maintain order and uphold the law within confined geographical boundaries . . . .*[287]

The traditional model of law enforcement, which is the model still in use today, evolved to deal with real-world crime; [288] the essential components of the model were, for all intents and purposes, in place by the nineteenth century. The discussion below examines this model: Section II(B)(1) identifies four assumptions that shaped the model, while § II(B)(2) sketches its evolution.

1. Real-world crime

Because it is firmly situated in a corporeal, physical environment, real-world

---

[286] *See* LAFAVE, *supra* note 254, at § 4.1*; see, e.g.,* MODEL PENAL CODE § 1.03 (1985) (territorial applicability of provisions).

[287] *Cybercrime: The Challenge to Leviathan,* London School of Economics: The Hayek Society, *at* http://www.lse.ac.uk/clubs/hayek/Essays/cybercrime.htm (last visited Dec. 17, 2003).

[288] Real-world crime is crime perpetrated in and via the real, physical world, that is, without the use of technology. "Technology" refers to *any* technology, not simply computer technology. The model of real-world crime articulated above is based upon the repertoire of "harms" a perpetrator could inflict before, say, the nineteenth century, which saw great advances in firearms and other technology.

crime has several defining characteristics; these characteristics became assumptions that shaped the extant model of law enforcement. The sections below examine the four characteristics that are the most significant for this discussion.

a. Proximity

Perhaps the most fundamental characteristic of real-world crime is that the perpetrator and the victim are physically proximate to each other at the time the offense is committed or attempted.[289] It is, for instance, not possible to rape or realistically attempt to rape someone if the rapist and the victim are fifty miles apart; by the same token, in a non-technological world it is physically impossible to pick someone's pocket, take their property by force or defraud them out of their property if the thief and victim are in different countries (or even different counties).

b. Scale

A second characteristic of real-world crime is that it tends to be one-to-one crime; that is, it consists of an event involving one perpetrator and one victim. This event – the "crime" – commences when the victimization of the target is begun and ends when it has been concluded; during this event the perpetrator focuses all of his/her attention on the consummation of that "crime."[290] When

[289] One can avoid the need for physical proximity by engaging someone to carry out the offense on their behalf, as when someone hires another to kill their unfaithful spouse or ungenerous wealthy relative. This does not undermine the validity of the point being made above because, in a non-technological world, the actual perpetrator will have to occupy some degree of physical proximity to the victim at the time the crime is committed. *See also infra* note 292.

[290] The characterization of real-world crime presented above assumes substantive crimes such as murder, rape, theft, arson, burglary and the like. The one-to-one character of these substantive offenses may not hold for inchoate crimes and clearly does not apply to compound crimes such as felony-murder, CCE or RICO offenses. As to inchoate crimes, one can be part of a conspiracy to commit bank robbery while robbing the bank; it is also possible simultaneously to conspire and attempt or conspire and solicit the commission of a crime. *See* Ira P. Robbins, *Double Inchoate Crimes,* 26 HARV. J. ON LEGIS., 54-58, 89-91 (1989). The one-to-one nature of real-world substantive crime is abrogated by compound offenses such as felony-murder and RICO, the rationale of which is that one course of conduct constitutes the simultaneous commission of various offenses. *See, e.g.,* Susan W. Brenner, *RICO, CCE, and Other Complex Crimes: The Transformation of American Criminal Law?,* 2 WM. & MARY BILL RTS. J. 239, 255-57(1993) [hereinafter *RICO*].

Finally, the characterization presented above does not encompass the rare occasions when a single course of conduct results in the coincident commission of two different substantive crimes. A father, for example, who rapes his daughter simultaneously commits the crimes of rape and incest. *See, e.g.,* State v. Rosenbalm, No. E2002-00324-CCA-R3-CD, 2002 WL 31746708 (Tenn. Crim. App. 2002).

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:[291] 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.[292] Real-world crime is therefore serial crime.

The one-to-one nature of real-world crime is more a default than an absolute; exceptions occur, especially with regard 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 "organized crime" is a tendency that has accelerated over the last few centuries.[293] But while many-to-one deviations from the one-to-one model have occurred for centuries, one-to-many deviations were rare prior to the use of technology. For example, 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; the forger falsifies a document, uses it to victimize his target and then moves on, to another document and another victim. The same is true of fraud; the perpetrator necessarily focuses his or her efforts on a single target, succeeds, and, having done so, moves on to another target.[294]

---

[291] For the additional role physical constraints play in structuring the nature of real-world crime, *see infra* Part II(B)(1)(c).

[292] This has never been true of murderers who employ poison; they can cause the more or less simultaneous deaths of many victims by, say, poisoning the food served at a banquet. And those who use poison also deviate from the model being articulated above in another way: They do not have to be in physical proximity with their victim(s) at the time the homicide occurs, though they do require physical proximity either to the victim or to some substance the victim will consume in order to cause the victim's death. In a non-technological world, "remote" poisoning is not a viable possibility. It is, however, quite possible in a technological world. The killer might, for example, hack into a hospital's computer system and alter the medication prescribed for patients, either by changing the medication entirely or by increasing the prescribed dose. Such an alteration could cause the death of some patients, depending on the nature of the alteration and the likelihood that the medical staff became aware of it and decline to administer the modified prescriptions.

[293] *See, e.g.,* Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships,* 4 N.C. J. L. & TECH. 1 (2002), *available at* http://www.jolt.unc.edu/ (last visited Dec. 17, 2003) [hereinafter *Organized Cybercrime?*].

[294] There were, no doubt, one-to-many deviations in the pre-nineteenth century world. A forger might, for example, falsify a document and use it to victimize a company, perhaps a bank; if one construes the bank as constituting "many" victims, then this would be an instance of simultaneous one-to-many victimization. Or a robber might intercept a

c. Physical constraints

A third characteristic of real-world crime is that its commission is subject to the physical constraints that govern all activities in the "real," physical world.[295] Since 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.[296] Every "crime," even routine offenses such as prostitution and street-level drug dealing, requires some level of preparation, planning and considered implementation if it is to succeed. For real-world crime, these activities must be conducted in physical, actual space.

So, one who decides to rob a bank must visit that bank corporeally to familiarize herself with its physical layout (entrances, teller windows, vault location), security (visible alarm systems, guards, surveillance cameras) and general routine (when employees arrive and leave, when the bank is likely to have the fewest customers, currency pickup and delivery).[297] This process exposes the robber to public scrutiny, which can lead to her being apprehended after she commits the crime.[298] The same is true of the robbery itself; while physically inside the bank, the robber can leave evidence or become the subject of observations that can lead to her being apprehended.[299] It is equally true of the perpetrator's flight once the robbery has been committed; again, the perpetrator is exposed to public view and runs the risk of being noticed and identified.[300] In addition to the risks of exposure that arise from planning and committing the "crime," the robber will presumably need to secure a weapon and some type of disguise;[301] and she may need to launder the funds she takes

stagecoach and use a weapon to take property from several travelers at essentially the same time; this could be brought within the one-to-one premise if the occupants of the stagecoach are construed as "one," but it is more logical to construe this as an instance of simultaneous one-to-many victimization.

[295] *See generally* Hans Geser, *Toward a (Meta)-Sociology of the Digital Sphere*, § 3, Sociology in Switzerland (Dec. 2002), *at* http://socio.ch/intcom/t_hgeser13.htm#3.

[296] The operation of physical constraints accounts for the one-to-one nature of real-world crime. *See supra* Part II(B)(1)(b).

[297] *See, e.g.,* John W. Kennish, Developing a Comprehensive Bank Robbery Prevention Program (2000), *at* http://www.kennish.com/robberythreat/*;see also Nebraska Robbery Suspects Denied Bail*, Muzi News (Sept. 27, 2002), *available at* http://news.1chinastar.com/ll/english/1227483.shtml (bank robbers planned the robbery for two weeks, "casing" the bank several times during that period).

[298] *See, e.g.,* United States v. Morrison, 254 F.3d 679, 680-82 (7th Cir. 2001).

[299] *See, e.g., id.* at 681*; see also* People v. Ihrig, No. H021885, 2002 WL 31501922, at *1-*2 (Cal. App. 6 Dist. 2002); Smith v. State, 571 S.E.2d 817, 819 (Ga. App. 2002).

[300] *See, e.g., Morrison*, 254 F.3d at 680*; see also* People v. Barnes, No. A090415, 2002 WL 1999737, at *1 (Cal. App. 2002).

[301] *See, e.g.,* Davis v. Commonwealth, No. 1149-01-3, 2002 WL 31163645, at *2 (Va. App. 2002); *Barnes*, 2002 WL 1999737, at *1.

from the bank.[302] Like the processes involved in the robbery itself, each of these steps takes time and effort and incrementally augments 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.[303]

d. Patterns

A fourth characteristic of real-world crime is that over time it becomes possible to identify the general contours and incidence of the "crimes" committed within a social system.[304] Real-world victimization tends to fall into demographic and geographic patterns for two reasons. One is that, is explained below, only a small segment of a functioning society's total populace will be persistently engaged in criminal activity.[305] Those who fall into this category are apt to be from economically-deprived backgrounds and reside in areas that share certain geographic and demographic characteristics.[306] They will be inclined to focus their efforts on those with whom they share a degree of physical proximity are their most convenient victims.[307] This means that much of the "crime" in a social system will be

[302] *See, e.g.,* State v. Mullins, 517 N.E.2d 945, 948-49 (Ohio App. 1986).

[303] *See, e.g.,* People v. Aleman, 809 So.2d 1056, 1065-66 (La. Ct. App. 2002).

[304] *See, e.g.,* U.S. DEP'T OF JUSTICE – BUREAU OF JUSTICE STATISTICS, CRIME VICTIMIZATION 2001: CHANGES 2001-01 WITH TRENDS 1993-2001, at 6-7, 9-10, 15 (2002), *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/cv01.pdf; U.S. DEP'T OF JUSTICE – BUREAU OF JUSTICE STATISTICS, HOMICIDE TRENDS IN THE UNITED STATES (2001), *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/htius.pdf.

[305] *See, e.g.,* Leslie W. Kennedy, Erika Poulsen & John Hodgson, *Problem Solving Using Crime Mapping: Concentration and Context,* Crime Mapping Research Center, 2001 Conference Papers, *available at* http://www.ojp.usdoj.gov/nij/maps/Conferences/01conf/Kennedy.doc ("[A]bout 60 percent of crime occurs in 10 percent of the places, 10 percent of offenders account for about 50 percent of offenses, and 10 percent of victimized people are involved in about 40 percent of the crimes.") (citation omitted)*; see also* FEDERAL BUREAU OF INVESTIGATION, UNIFORM CRIME REPORTS, CRIME IN THE UNITED STATES (2001), at § II, 64 and § IV, 292, *available at* http://www.fbi.gov/ucr/01cius.htm. A "functioning society" is one in which the rule of law prevails and the assumption that "crime" represents extraordinary behavior consequently holds. *See supra* Part II(A).

[306] *See generally* Pablo Fajnzylber, Daniel Lederman & Norman Loayza, *Crime and Victimization: An Economic Perspective*, 1.1 ECONOMIA 219 (2000), *available at* http://muse.jhu.edu/journals/economia/v001/1.1fajnzylber.pdf.

[307] *See, e.g., id.* at 266-73 (discussing patterns of criminal behavior within Latin American cities)*; see also* Ken Pease & Gloria Laycock, *Revictimization: Reducing the Heat on Hot Victims,* U.S. Department of Justice – National Institute of Justice, Research in Action 3 (Nov. 1996), *at* http://www.ncjrs.org/pdffiles/revictim.pdf (suggesting that access, in terms of geography and low risk of getting caught, create "hot spots" – locations where people are repeatedly victimized).

concentrated in specific areas, such on the "West Side of Notown" or "South of 31st Street in Megalopolis."[308]

The other reason why "crime" falls into certain patterns because each society has a repertoire of "crimes" – legal rules that proscribe a set of behaviors ranging from more to less serious in terms of the respective "harms" each inflicts.[309] 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;[310] a theft causes the "harm" inflicted by the "crime" of theft;[311] a forgery yields the "harm" subsumed by the "crime" of forgery, and so on.[312] In a functioning society, the more egregious "crimes" will occur much less often and may occur less predictably than the minor "crimes."[313] Murder, for instance, is an extraordinary event in any society that

[308] *See, e.g.,* Kennedy, Poulsen & Hodgson, *supra* note 305*;* Gary LaFree, et al., *The Changing Nature of Crime in America*, U.S. DEPARTMENT OF JUSTICE – NATIONAL INSTITUTE OF JUSTICE, 1 CRIMINAL JUSTICE 2000, at 1, 21-24, *available at* http://www.ncjrs.org/criminal_justice2000/vol_1/02a.pdf; Luc Anselin, et al., *Spatial Analyses of Crime*, U.S. DEPARTMENT OF JUSTICE – NATIONAL INSTITUTE OF JUSTICE, 4 CRIMINAL JUSTICE 2000, at 213, 221-22 (2000), *available at* http://www.ncjrs.org/criminal_justice2000/vol_4/04e.pdf; Paul Brantingham & Patricia Brantingham, *A Theoretical Model of Crime Hot Spot Generation*, 8 STUDIES ON CRIME AND CRIME PREVENTION 7, 7-10 (1999), *available at* http://www.bra.se/dynamaster/studies/pdf_archive/9903121462.pdf.

[309] *See* Goodman & Brenner, *supra* note 17*,* at 55-65*; see also supra* Part II(A)(3). For the proposition that a "crime" inflicts "harm" upon the victim. *See, e.g., Virtual Crime, supra* note 2.

[310] *See, e.g.,* MODEL PENAL CODE § 213.1(1) (2002).

[311] *See, e.g.,* MODEL PENAL CODE § 223.2 (1980).

[312] *See, e.g.,* MODEL PENAL CODE § 224.1 (1980).

[313] *See, e.g.,* FEDERAL BUREAU OF INVESTIGATION, UNIFORM CRIME REPORTS, *supra* note 305, at § II, 64. The unpredictability of some of the more serious crimes, such as rape and murder, lies in the motivations for their commission; crimes of passion, which is what often drives murder, are often committed spontaneously, in a burst of emotion or, in the case of serial killers, as the result of irrational psychological impulse. *See, e.g.,* STEPHEN J. GIANNANGELO, THE PSYCHOPATHOLOGY OF SERIAL MURDER: A THEORY OF VIOLENCE 7-43 (1996). While some types of murder – such as familial homicide – might have been predicted by those who knew the family members, it is difficult, if not impossible, to generalize as to the frequency with which this type of crime will occur. *See generally* Lawrence W. Sherman, *Preventing Homicide Through Trial and Error, in* 17 AUSTRALIAN INSTITUTE OF CRIMINOLOGY, HOMICIDE: PATTERNS, PREVENTION AND CONTROL 21, 25-26 (Heather Strang & Sally-Anne Gerull eds., 1992), *available at* http://www.aic.gov.au/publications/proceedings/17/sherman.pdf. On the other hand, it is possible to predict that certain types of offenses – such as various levels of drug-dealing, assaults, robberies, trafficking in stolen goods and prostitution—will occur in "hot spots," i.e., urban geographies in which crime is highly concentrated. *See, e.g.,* U.S. DEPARTMENT OF JUSTICE – NATIONAL INSTITUTE OF JUSTICE, POLICING DRUG HOT SPOTS, NIJ RESEARCH

is successfully maintaining social order and resisting chaos.[314] Theft in its various forms[315] is a far less extraordinary event;[316] and, depending on the cultural mores of the society, drunkenness and/or prostitution may be quite common.[317] Also, various "crimes" fall into localized patterns reflecting geography and particular types of victimization.[318]

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 section below explains how each characteristic contributed to the model.

2. Traditional Model of Law Enforcement

As social control strategies[319] evolved, the empirical characteristics of real-world crime – physical proximity of victim-victimizer; one-to-one scale; physical constraints; and offender-offense "crime" patterns[320] – became embedded assumptions that shaped the traditional model and its approach to "crime." The model encompasses both a general strategy for dealing with "crime" and an organizational model for implementing this strategy. The sections below explain how these assumptions shaped the model and how the model evolved through time.

a. Assumptions

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

PREVIEW (Jan. 1996), *available at* http://www.ncjrs.org/pdffiles/hotspot.pdf.

[314] *See, e.g.,* FEDERAL BUREAU OF INVESTIGATION, UNIFORM CRIME REPORTS, *supra* note 305, at § II, 64.

[315] *See* MODEL PENAL CODE § 223.1 (1980).

[316] *See, e.g.,* FEDERAL BUREAU OF INVESTIGATION, UNIFORM CRIME REPORTS, *supra* note 305, at § II 64.

[317] *See generally* BUREAU OF JUSTICE STATISTICS, SOURCEBOOK OF CRIMINAL JUSTICE STATISTICS - 2000, at Tables 4.1 & 4.6 (2002), *available at* http://www.albany.edu/sourcebook/1995.

[318] *See, e.g.,* Kansas City Police Department – Property Crimes Division, *Security Alert*, *at* http://www.kcpd.org/propertycrimes.html ("[W]e have identified a pattern involving check forgeries. These offenses usually occur in areas where there is a strip mall or several businesses very close together.") (last visited Nov. 8, 2003).

[319] *See supra* Part II(A)(3).

[320] *See supra* Part II(B)(1).

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 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, since the local citizenry paid particular attention to those who "did not belong" in their portion of the physical world.[321] Law enforcement dealt effectively with this type of crime because its parochial character meant that investigations were limited in scope.[322] The model therefore assumes that the investigation of a "crime" can focus upon a specific geographical area surrounding the site where the "crime" occurred.[323]

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 extraordinary events in a social system; the model assumes, in other words, that "crime" is a deviation from the law-abiding conduct that constitutes the prevailing pattern of behavior in a system. This assumption derives not from the physical characteristics of real-world crime but from the nature of criminal law, the function of which is to maintain an acceptable level of social order within a social system.[324] It does this by defining what behaviors are unacceptable and by specifying the consequences of engaging in such behavior.[325] The presumptive result is that "crime" becomes a subset, generally a small subset, of the total behaviors in a system population; law enforcement personnel can, therefore, focus their efforts on a limited segment of the conduct within a given society.

---

[321] Indeed, the presence of a stranger might offer a ready, simple solution to criminal investigation. Since the stranger had no local ties, prosecuting and punishing him was unlikely to cause unrest in the local community; and punishing an outsider avoided any controversy or ill-will that might attend the apprehension and prosecution of a local citizen. *See, e.g.,* WALTER VAN TILBURG CLARK, THE OX-BOW INCIDENT (2001).

[322] The premise that victim and victimizer were necessarily physically proximate during the commission of an offense also contributed another element to the traditional model: the concept of criminal jurisdiction. *See supra* note 269 and accompanying text.

[323] *See, e.g.,* STEVEN A. EGGER, *Linkage Blindness: A Systemic Myopia*, *in* 8 SERIAL MURDER: AN ELUSIVE PHENOMENON 163, 164 (1990).

> In a stranger-to-stranger murder lacking in physical evidence or witnesses, criminal investigators are left to deal with a very large set of suspects, with only a small probability of this set including the offender . . . . [M]ost serial murderers are caught by chance or coincidence . . . . Law enforcement agencies today are simply not adept at identifying or apprehending the murderer who kills strangers and moves from jurisdiction to jurisdiction and crosses state lines.

[324] *See supra* Part II(A)(2)-(3).

[325] *See supra* Part II(A)(2)-(3).

This assumption that "crime" is committed by a small subset of the populace is the first element – the "offender element" – that structures the model's conceptualization of the scale of "crime." The second element – the "offense element" – is the assumption that one-to-one victimization is the default case. As explained earlier, "crimes" involve the infliction of a specific type of "harm" upon the victim.[326] If one-to-one victimization is the norm, each completed "crime" inflicts *one* "harm" upon *one* victim; additive "harms" must be inflicted sequentially.[327] So, while a serial killer can cause many deaths, many "harms," he necessarily does so sequentially.[328]

The conceptualization of scale derived from these assumptions posits that the incidence of victimization in a system will be relatively small both (a) in relationship to the size of the population and (b) in terms of the absolute level of "harm" inflicted. The first proposition derives from the assumption that only a subset of the system populace will engage in criminal activity. The derivation of the second proposition is more complex. The level of "harm" inflicted by the incidence of victimization in a system is a function of three variables: (1) the number of individuals engaged in committing "crimes;" (2) the number of discrete "crimes" these individuals commit during a given time period; and (3) the types of "harm" caused by the "crimes" these individuals commit. The operation of these variables is illustrated by a hypothetical. Assume that a social system consists of 10,000,000 people, of whom 500,000 engage in criminal activity on a more or less regular basis.[329] 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.[330] Defining the remaining two variables is more problematic because they tend to interact. That is, it is difficult to set a 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

---

[326] *See supra* Part II(B)(1)(d).

[327] *See supra* Part II(B)(1)(b).

[328] *See supra* Part II(B)(1)(b).

[329] *See generally* BUREAU OF JUSTICE STATISTICS, *supra* note 304, at 346-49, Table 4.5 (total arrests per state in 2000 averaged roughly 4%-6% of the state population).

[330] Some "crimes" will be committed by individuals who have no history of criminal activity; this is often true of domestic violence offenses, for example. These non-career offenders are not included in the analysis above for two reasons: One is that there is no accurate way to predict the number of situational offenders who will emerge in a population during a given time period. The other is that persistent offenders are primarily responsible for the rate of victimization in a society. *See, e.g.,* Criminal Justice System Online, *Narrowing the Justice Gap* 13, *at* http://www.cjsonline.org/njg/documents/njg-framework.pdf (last visited Nov. 8, 2003).

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.[331] As the seriousness of a "crime" increases, the frequency with which it is committed tends to decrease; most murderers, for example, kill only once.[332] Crime statistics therefore indicate, and the traditional model assumes, that most of the "crimes" committed by a system'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.[333]

Finally, the traditional model's conceptualization of scale incorporates the fourth characteristic of real-world crime: the assumption that offenses and offenders fall into identifiable patterns.[334] What this adds is the notion of localization. As explained above, 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.[335] This final premise contributes the notion that an identifiable percentage of these real-world "crimes" will occur in geographically and demographically demarcated

[331] Most offenders will perpetrate "crimes" only sporadically; the sporadic nature of crime is a product of the motives for committing real-world "crime" and the logistics involved in doing so. People commit real-world "crimes" for various reasons, including a desire for economic gain (e.g., theft, fraud), passion (e.g., spousal homicide, harassment) or compulsion (e.g., serial murder). Since the consummation of a "crime" tends to extinguish one's motivation, at least for a while, the commission of real-world offenses is sporadic, even as to "career" offenders. The intermittent nature of real-world criminality is also a function of the logistical issues offenders must address if they are to commit their "crimes" successfully and avoid prosecution. *See supra* Part II(B)(1)(c).

[332] This is not true of serial killers, but even they tend to offend sporadically. *See, e.g.,* EGGER, *supra* note 323, at 164.

[333] The Federal Bureau of Investigation's Uniform Crime Reports establish that the overwhelming majority of indexed crimes committed in the United States for the period 1982-2001 were non-violent offenses. *See* FEDERAL BUREAU OF INVESTIGATION, UNIFORM CRIME REPORTS, *supra* note 305, § II, 64.

[334] *See supra* notes 329-30 and accompanying text. This premise is similar to the others that influence the conceptualization, but it differs in an important respect. This final premise is concerned not with the amount of "crime" but with how it is distributed, geographically and demographically, in a system. The amount of "crime" can affect the development of patterns, especially at the extremes: If a system were so crime-riddled as to have become dysfunctional, it is doubtful that its "crime" would fall into identifiable patterns; the same would be true of a system in which the incidence of "crime" was essentially infinitesimal. But for most functional societies, the incidence of real-world "crime" falls into what might be termed the "normal range," for the reasons given earlier. *See supra* Part II(B)(1)(d).

[335] *See supra* notes 331-33 and accompanying text.

areas.[336]

The traditional model therefore 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 law enforcement. The model assumes that "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 contribute the premise that "crimes" necessarily leave information, evidence, in the real-world locale where they are committed; extrapolating from this premise yields the conclusion that law enforcement personnel reacting to the report of a "crime" can locate this evidence and use it to apprehend the perpetrator. The model further postulates that perpetrators remain in or near the area where their "crime" was committed, which facilitates their being apprehended. The first two assumptions, therefore, inferentially establish law enforcement's ability to deal with specific "crimes." The last two establish its ability to deal with "crime" as a systemic phenomenon; the premise here is that since real-world "crime" occurs on a limited scale and assumes certain patterns, law enforcement can mobilize its modest resources so as to deal with it effectively.[337]

b. Strategy and Structure

The model assumes real-world crime because it 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 has been in use since pre-history and the dynamic employed in its implementation is the same as it was centuries ago, when law enforcement consisted of a constable or night watchman: A "crime" is committed and called to the attention of law enforcement personnel, who investigate; if their investigation is successful, they identify and apprehend the perpetrator, who is charged with the "crime," prosecuted, and presumably convicted and punished.[338]

---

[336] *See supra* notes 304-17 and accompanying text.

[337] *See, e.g.,* Surrey Police, United Kingdom, *Increased Emphasis on Intelligence by Surrey Police*, (Dec. 14, 2001), *at* http://www.surrey.police.uk/news_item.asp?artid=1088 (police department allocating resources to "more effectively target the active criminals in Surrey. There are a comparatively small number of these who are responsible for a surprisingly large proportion of crime. By dealing effectively with those individuals we will reduce crime . . . .").

[338] *See, e.g.,* J. MICHAEL OLIVERO, CYRIL D. ROBINSON & RICHARD SCAGLION, POLICE IN CONTRADICTION : THE EVOLUTION OF THE POLICE FUNCTION IN SOCIETY 14-23 (1994).

This reactive approach to deviant behavior is a very basic strategy, functionally analogous to the social control tactics common in dominance hierarchies.[339] A violation of the rules in effect in a social system occurs, which produces a reaction by the member of that system charged with maintaining order. In a wolf pack, this is typically the alpha male, who enforces the relational rules that maintain order in the pack;[340] in evolved human social systems, it is typically a member of the system who has been assigned to enforce the structural rules that maintain order in the system. The source of authority for the rules differs in the two systems, but the operating rationale is the same: A violation of the rules requires a reaction by someone in authority; the purpose of the reaction is to achieve a response. Ideally, the response takes the form of continuing submission to authority; the offender ceases to offend at that moment and does not re-offend in the future. This is control-by-deterrence (though it can also be control-by-incapacitation if the reaction results in the offender's incarceration or demise).[341] That is, the threat of sanction brings the offender into line and has the consequent effect of impressing the other members of the system with the consequences of offending, thereby helping to ensure that they will not offend in the future.[342] As human societies develop more complex cultures, the reaction can also be seen as having a symbolic effect, i.e., "doing justice" or "exacting retribution" according to some philosophical or religious principles.[343]

This reactive approach emerged millennia ago as a pragmatic solution to what was then atypical behavior. "Crime" is an unusual event in small social systems because the informal social control exerted by shared norms and values is sufficient to deter most would-be offenders.[344] When a "crime" does occur, it is relatively easy to address given the nature of the system in which it is committed: Identifying the perpetrator, who may literally be caught red-handed, is generally not difficult given the small size of the populace; the operation of the physical constraints discussed above is magnified, so it may be impossible for an offender to avoid observation and detection in the process of

[339] *See supra* Part II(A)(2)(b).

[340] *See supra* Part II(A)(2)(b).

[341] *See, e.g.,* LAFAVE, *supra* note 254, at § 1.5(a)(1)-(2), (4).

[342] *See, e.g., id.* § 1.5(a)(4).

[343] *See, e.g.,* The Avalon Project at Yale Law School, *Code of Hammurabi*, (L.W. King, trans.), *available at* http://www.yale.edu/lawweb/avalon/medieval/hamframe.htm (last visited Dec. 20, 2003) ("the lord of Heaven and earth . . . called . . . me, Hammurabi, the exalted prince, who feared God, to bring about the rule of righteousness in the land, to destroy the wicked and the evil-doers."); *see also* LAFAVE, *supra* note 254, § 1.5(a)(6).

[344] *See, e.g.,* THE ROLE OF POLICE IN AMERICAN SOCIETY: A DOCUMENTARY HISTORY, at xxv (Cynthia Morris & Bryan Vila eds., 1999) ("Serious crimes were rare in the earliest American colonies, and there was little need for formal law enforcement."); *see also* OLIVERO ET AL., *supra* note 338, at 15-16.

committing the "crime" or in the process of fleeing from it.[345] And the unlikelihood of "stranger danger" makes it relatively easy to deduce who might have had the motive and opportunity for the offense.[346] The reactive approach to deviant behavior emerged from this context and persisted as social systems evolved in size and complexity.

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 the identification, apprehension, prosecution and eventual punishment of the offender will satisfactorily resolve things, returning "harm" for "harm" and deterring future "crimes."[347] 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.[348] Yet another reason is that it is still a workable means of dealing with real-world "crime." The reactive approach may not be the most effective means, but real-world "crime" retains the characteristics described earlier; the persistence of those characteristics means this approach continues to be a viable strategy for addressing traditional "crime."[349]

But strategy alone is not enough. There must also be an allocation of human and other resources plus an organizational structure designed to implement the strategy, i.e., to identify and apprehend those who commit "crimes." The level of organizational development in the society determines who will actually be responsible for reacting to a completed "crime." Among some hunter-gatherers, for example, "communal, collective security efforts generally suffice;"[350] in others, this function is assigned to a subset of the populace, typically males who enjoy higher status within the grouping.[351] Historically, as human social systems became larger and more complex they tended to institutionalize this function: Egypt had established an "early system of citizen police" by 1500 B.C.; the ancient Greeks used "an effective system of 'kin

---

[345] *See supra* Part II(B)(1)(c).

[346] *See supra* Part II(B)(1)(c).

[347] *See, e.g.,* Richard A. Leo, *Some Thoughts about Police and Crime, in* THE CRIME CONUNDRUM, ESSAYS ON CRIMINAL JUSTICE 121-22 (George Fisher & Lawrence M. Friedman eds., 1997) ("[T]he American public . . . and political leaders all assume that police . . . deter crime.").

[348] *See* John E. Eck, *Rethinking Detective Management: Why Investigative Reforms Are Seldom Permanent or Effective*, *in* 8 POLICE AND POLICING: CONTEMPORARY ISSUES 178-79 (Dennis Jay Kenney & Robert P. McNamara eds., 2nd ed. 1999) (proactive efforts are "very expensive"); *see also* SUSAN M. HARTNETT & WESLEY G. SKOGAN, COMMUNITY POLICING: CHICAGO STYLE 13 (1997).

[349] *See infra* notes 447-48 and accompanying text.

[350] OLIVERO ET AL., *supra* note338, at 65*; see, e.g., id.* at 59-64.

[351] *See id.* at 65-71.

policing'" and the ancient Romans used both civilian patrols and military forces to "maintain law and order."[352] The disintegration of the Roman Empire plunged Europe into chaos; social systems that had relied on Roman institutions were forced to resort to older measures to maintain order.

> The closest equivalent to the modern police officer that emerged at the time of Alfred the Great . . . was the 'Saxon tythingman.' Every male person over the age of twelve was required to participate in . . . the tything system. A tything was a group of ten families, headed by a 'tythingman' responsible for the acts of the persons . . . in his group. It was each tythingman's duty to raise the 'hue and cry' when a crime was committed, to collect his neighbors and to pursue a criminal who fled . . . . If such a group failed to apprehend a lawbreaker, the tything could be required to pay a fine.[353]

The Normans kept this system in place but expanded the role of the "shire reeve" (later, sheriff). Under the Norman system, the shire reeve could "raise a 'hue and cry,' but instead of merely requiring the members of a tything to . . . apprehend an accused, he was able to summon the *posse comitatus* which consisted of the tythingmen . . . of several hundred tythings."[354] The shire reeve was responsible for maintaining order in the shire over which he presided; by the end of the thirteenth century, the shire reeve had an assistant, the constable, who eventually assumed responsibility for maintaining law and order.[355] In 1285, the Statute of Winchester established a system of,

> patrols in each of the large towns of England. Men between the ages of fifteen and sixty were required to perform watch service on a rotating basis between sunset and sunrise. They were responsible for protecting property against fire, guarding the town gates and apprehending anyone who committed a crime. The "hue and cry" could be commenced by any watchman and the entire community of able-bodied males was required to join in the pursuit of any wrongdoer. A failure to participate in the watch

---

[352] *See id.* at 15. The Greek system seems to have involved private retribution. The Roman Emperor Augustus organized citizens "into a semimilitary force known as the 'Vigiles'"; while their "responsibilities included fire protection and street patrol[,]" their "main purpose was apparently to protect the ruling class from the threat of rebellion."

[353] *Id.* at 19 (quoting T. A. CRITCHLEY, A HISTORY OF POLICE IN ENGLAND AND WALES 1-3 (2d ed.1972) & PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 3 (1967)) (notes omitted); *see also* MORRIS & VILA, *supra* note 344, at 3 ("In England, the active involvement of civilians in law enforcement began in about the tenth century. Each citizen was made responsible for aiding neighbors who were victimized by outlaws.").

[354] OLIVERO ET AL., *supra* note 338, at 19; *see also* L.F. SALZMAN, ENGLISH LIFE IN THE MIDDLE AGES 215-20 (1926).

[355] *See* OLIVERO ET AL., *supra* note 338, at 20.

or to aid in the pursuit of fugitives would result in punishment.[356]

The statute also "required every man between the ages of fifteen and sixty to maintain specified weaponry, which varied according to his wealth."[357]

Policing in England, and later in the American colonies,[358] "continued to follow this style, known as the 'watch and ward' system of law enforcement, for nearly five hundred years."[359] But "as time passed the voluntary observance of the 'watch and ward' system" weakened, and it became common practice "to pay others to do the required service.[360] The substitutes were generally "too old to be of any value" and the consequent rise in crime rates caused wealthy merchants to hire "private watchmen to guard themselves and their businesses . . . ."[361] The Industrial Revolution brought "a vast migration to urban areas and the need for a regular system of policing became greater than ever before."[362] For a time, London experimented with "a number of fragmented civic associations," which tended to disintegrate into bounty hunters.[363] The "first regular professional police force" in London was created in 1800; when the privately-funded force was a success, Parliament authorized a publicly funded police force.[364] But since it was small, the primary burden of law enforcement remained with elderly or indifferent night watchmen.[365]

This changed in 1829 when Sir Robert Peel successfully maneuvered the

> Metropolitan Police Act through Parliament. The act called for the creation of a tax-supported police force for the London metropolitan area . . . . [T]he Metropolitan Police created by this legislation provided the model for modern policing . . . . First, the officers were independent from the courts . . . . Second, the force was uniformed, and quasi-military in organization. Patrols were assigned to constables, who were supervised by sergeants, who in turn reported to inspectors, who were

---

[356] *Id.; see also* DOUGLAS G. BROWNE, THE RISE OF SCOTLAND YARD: A HISTORY OF THE METROPOLITAN POLICE 11-18 (Greenwood 1973) (1956).

[357] David A. Sklansky, *The Private Police,* 46 UCLA L. REV. 1165, 1197 (1999).

[358] *See, e.g.,* MORRIS & VILA, *supra* note 344, at 2-3 (American colonists established "variants of the law enforcement and protection procedures that long had been in place in their European homelands, such as the night watch, constabulary, and sheriff.").

[359] OLIVERO ET AL., *supra* note 338, at 20*; see also* BROWNE, *supra* note 356, at 11-24.

[360] OLIVERO ET AL., *supra* note 338, at 21*; see also* MORRIS & VILA, *supra* note 344, at 4 (similar problems with the American colonial version of the night watch-constable system).

[361] OLIVERO ET AL., *supra* note 338, at 21*; see also* CLIVE EMSLEY, GENDARMES AND THE STATE IN NINETEENTH-CENTURY EUROPE 149-50 (1999) (nineteenth century Italy used the sbirri, "armed thugs who performed some policing functions.").

[362] OLIVERO ET AL., *supra* note 338, at 21.

[363] *Id.*

[364] *Id.*

[365] *Id.* at 22.

> under the command of superintendents, who reported to the commissioner. Third, policing was a full-time occupation, and officers were not allowed to demand or to accept supplemental private payments for their work.[366]

In 1856, Parliament required that similar police forces be established in the cities and towns outside London, and "the English police system has remained practically unchanged since that time."[367]

As American cities rapidly expanded in the nineteenth century, they experienced the same problems London had dealt with until it established the Metropolitan Police.[368] In the early part of the nineteenth century, some called for the creation of a public police force, but these early advocates of professional policing "were unable to overcome the long-standing American aversion to anything resembling a standing army – an aversion dating back to the abuses of Cromwell's constabulary in seventeenth-century England and reinforced by the Redcoats' behavior prior to the Revolution."[369] By the mid-1800s,

> unrestrained growth, frequent mob violence . . . and the influx of foreign immigrants into urban areas fueled social disorder and contributed to rising fear among the country's growing middle class . . . . When fears of social disintegration finally became stronger than distrust of a quasi-standing army, America's larger and more disorderly cities began searching for a successful model . . . . [T]hey seized upon the 'modern' police model established by the Metropolitan Police Act of 1829, which created the first police force in the world . . . .[370]

In 1845, New York "became the first American city to establish a fully consolidated police force, with 800 paid full-time officers."[371] Other cities followed suit, and in "less than fifteen years, New York-style, full-time consolidated police departments . . . had become standard in all large American cities."[372] A similar process occurred in other countries, and eventually public police forces modeled on Peel's Metropolitan Police became the general global standard for maintaining internal order.[373]

---

[366] Sklansky, *supra* note 357, at 1202-03; *see also* BROWNE, *supra* note 356, at 73-112.

[367] OLIVERO ET AL., *supra* note 338, at 22.

[368] *See, e.g.,* MORRIS & VILA, *supra* note 344, at 25. For the origins of the term "police," *see, e.g.,* TREVOR JONES & TIM NEWBURN, PRIVATE SECURITY AND PUBLIC POLICING 2-3 (1998).

[369] MORRIS & VILA, *supra* note 344, at 25.

[370] *Id.*

[371] *Id.* at 26.

[372] *Id.*

[373] *See, e.g.,* CLIVE EMSLEY & BARBARA WEINBERGER, POLICING WESTERN EUROPE: POLITICS, PROFESSIONALISM AND PUBLIC ORDER 1-14, 18-24, 55-68 (1991); EMSLEY, *supra*

The net effect of all this was to eliminate citizen involvement in the process of maintaining internal order and assign that task exclusively to professionals employed by the state.[374] In exchange for receiving free police services,[375] citizens effectively surrendered responsibility for their own security. We return to this issue in Part IV, *infra.*

III. CYBERCRIME AND THE CURRENT MODEL

There is currently no effective way to police cyberspace.[376]

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

A. Proximity

Unlike real-world "crime," cybercrime does not require any degree of physical proximity between victim and victimizer at the moment the "crime" is committed.[377] Cybercrime is unbounded crime, borderless crime.[378] It can be

---

note 361, at 155-250.

[374] *See, e.g.,* JONES & NEWBURN, *supra* note 368, at 7:

> From the mid-nineteenth century . . . a professional state police force not only existed but was accorded a degree of legitimacy that would have been unimaginable a century earlier . . . . '[I]n contrast to the eighteenth century paradigm in which individuals. . . were centrally involved in policing, the implication . . . was to . . . exclude . . . the people from such involvement by redefining policing as the work of a state bureaucracy.'

Id. (quoting Philip Rawlings, *The Idea of Policing: A History,* Policing and Society 129, 143 (1995)*; see also supra* note 6.

[375] *See, e.g.,* THE HANDBOOK OF CRIME & PUNISHMENT 439 (Michael Tonry ed.,1998):

> The initial public expectation for modern police was an extraordinary idea . . .: that police services should be performed free of charge. Prior to the creation of the New York City Police Department in 1845, policing was primarily a fee-for-service business. If your neighbor burglarized your house and you wanted him prosecuted, you would have to pay a fee to the constable to arrest him. . . .

[376] RICHARD O. HUNDLEY & ROBERT H. ANDERSON, *Emerging Challenge: Security and Safety in Cyberspace, in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 231, 239 (John Arquilla and David Ronfeldt eds., 1997), available *at* http://www.rand.org/publications/MR/MR880/MR880.ch10.pdf.

[377] *See supra* Part II(B)(1)(a).

[378] *See* Goodman & Brenner, *supra* note 17, at 7-8*; see, e.g., Counterfeit Ring Hacks Nebraska Bank's Computer,* USA TODAY (July 23, 2003), *at* http://www.usatoday.com/tech/news/computersecurity/2003-07-23-ne-hack_x.htm (Malaysian hackers attacked Kearney bank).

committed against a victim who is in another city, another state, another country.[379] All a perpetrator needs is access to a computer that is linked to the Internet; with this, he can inflict "harm" upon a victim directly, by attacking her computer, or indirectly by obtaining information that lets him assume her identity and use it commit fraud on a grand scale. As a report issued several years ago explained,

> In the physical world . . . human travel is spatially based. By contrast, because one can access a computer remotely without knowing where, in physical space, that computer is located . . . cybercriminals are no longer hampered by the existence of national . . . boundaries . . . .
>
> [A] cyberstalker in Brooklyn . . . may send a threatening e-mail to a person in Manhattan. If the stalker routes his communication through Argentina, France, and Norway . . . the New York Police Department may have to get assistance from the Office of International Affairs at the Department of Justice . . . which . . . may have to get assistance from law enforcement in . . . Buenos Aires, Paris, and Oslo just to learn that the suspect is in New York . . . . [T]he perpetrator needs no passport and passes through no checkpoints as he commits his crime, while law enforcement agencies are burdened with cumbersome mechanisms . . . that often derail or slow investigations . . . . And any delay in an investigation is critical, as a criminal's trail often ends as soon as he or she disconnects from the Internet.[380]

B. Scale

Cybercrime differs from real-world "crime" in another important regard: It is not one-to-one "crime" because it is not corporeal crime; consequently, a one-to-one scale of offense commission is not a viable default assumption for cybercrime.[381] Much of cybercrime is already "automated crime," and the use of automation will only increase. "Automated crime" is using technology to multiply the number of "crimes" someone can commit in a given period of

---

[379] "Computer-related crimes . . . can . . . be perpetrated from anywhere and against any computer user in the world." Creating a Safer Information Society By Improving the Security of Information Infrastructures and Combating Computer-Related Crime: Communication from the European Commission to the Council and the European Parliament 1.1, COM (2001) 890 final, at 9 (Brussels, Jan. 26, 2001), *available at* http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html.

[380] PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET, § II(D)(2) (Mar. 2000), *at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#CHALLENGES.

[381] *See supra* Part II(B)(1)(b).

time;[382] automation gives perpetrators the ability to commit many cybercrimes very quickly.[383] Indeed, with automation, a perpetrator can start the process of victimization and then turn his attention to other matters, letting automated systems complete it.[384]

This capacity to automate crime alters traditional assumptions about the scale of crime and thereby creates problems for law enforcement.[385] Under the traditional model of law enforcement, officers react to a report of a "crime" by initiating an investigation; the investigation is intended to culminate in the identification and apprehension of the perpetrator, who will then be prosecuted and presumably sanctioned.[386] This ensures that the criminal law is enforced

---

[382] *See* Donn Parker, *Automated Crime,* WindowSecurity.com Web Site (Oct. 16, 2002), *at* http://secinf.net/misc/Automated_Crime_.html/. For an example of how automation can increase the scale of criminal activity, *see, e.g.,* Kelli Arena, *U.S. Targets Porn Site's Customers,* CNN.com Web Site (Aug. 8, 2001), *at* http://www.cnn.com/2001/LAW/08/08/ashcroft.childporn/ (Texas website offering child pornography had 250,000 subscribers around the world and took in $1.4 million in a one-month period).

[383] *See, e.g., About Cybercrime*, IPWatchdog.com Web Site, *at* http://www.ipwatchdog.com/cybercrimes.html (last visited Dec. 20, 2003) ("through the use of inexpensive and widely available computer and telecommunications systems individuals are able to commit wrongs with unprecedented speed and on scale never before seen."); *see also* Christopher M.E. Painter, *Tracing in Internet Fraud Cases: PairGain and NEI Webworld,* U.S. Department of Justice – U.S. Attorneys' Bulletin, *at* http://www.cybercrime.gov/usamay2001_3.htm (last visited Dec. 20, 2003) (online stock fraud scheme involved thousands of victims).

[384] *See, e.g.,* Parker, *supra* note 382.

> [A]n automated crime is a complete, fully automated, ready-to-use crime – from the selection of a victim to the perpetration of the misdeed and the covering of the perpetrator's tracks and identity – that is packaged in a single computer program . . . . When the program is executed, it automatically commits the crime and removes any damning evidence (including itself) before the victim can blink an icon . . . . The perpetrators can then execute the crime to attack any number of victims' computers without the creator's – or even the perpetrators' or victims' – further involvement.
>
> [B]ecause the crime can be designed for bi-directional, perfect anonymity, the perpetrator need not know who the victim was, what crime occurred, what method was used or even the results of the crime. The victim, likewise, would not know the perpetrator, what method was used, and where his or her losses went. And the entire crime could take place in only a few milliseconds. . . .

Id.; see also Automated Tools & Mail Bombs, *at* http://www.silkroad.com/papers/html/bomb/node17.html (last visited Dec. 20, 2003)*; see, e.g., Stealth Program Hijacks PC's to Send Porn Ads* USA Today Web Site (July 11, 2003), http://www.usatoday.com/tech/news/computersecurity/2003-07-11-hijacked-porn-spammers_x.htm (Trojan program hijacked nearly 2,000 PC's with high-speed connections and used them to send ads for porn sites).

[385] *See supra* Part II(B)(1)(b).

[386] *See supra* Parts II(A)(2)(c) and II(B)(2).

and order is maintained.[387] The problem with this scenario is that it assumes real-world "crime" and, in so doing, assumes "crimes" will be committed on a manageable scale.[388]

Cybercrime violates these assumptions in two ways: (a) it is committed on a scale far surpassing that of real-world "crime;"[389] and (b) 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.[390] These factors combine to create an overload; law enforcement's ability to react to cybercrime erodes because the resources that were adequate to deal with the real-world "crime" are inadequate to deal with real-world "crime" plus cybercrime.[391]

---

[387] *See supra* Parts II(A)(2)(c) and II(B)(2).

[388] *See supra* Part II(B)(1)(b).

[389] *See, e.g., supra* notes 382-84 and accompanying text*; see also* PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, *supra* note 380. ("The potential to reach vast audiences easily means that the scale of unlawful conduct involving the use of the Internet is often much wider than the same conduct in the offline world. To borrow a military analogy, use of the Internet can be a 'force multiplier.'").

[390] *See, e.g.,* Bob Tedeschi, *Crime Wave Washes Over Cyberspace,* INTERNATIONAL HERALD TRIBUNE, January 28, 2003, *available at* 2003 WL 56172695 ("Criminal activity on the Internet is growing . . . exponentially, both in frequency and complexity."); *Inquiry into Cybercrime Takes Paedophilia Focus,* SMH.com.au Web Site (Mar. 31, 2003), http://www.smh.com.au/articles/2003/03/31/1048962691620.html ("The exponential growth rate of cybercrime has prompted a parliamentary inquiry into child pornography, fraud and national security threats associated with the internet."). In sorting out priorities between the two, law enforcement agencies may feel that real-world "crimes" should take priority because they are, so far, more likely to result in the infliction of death or bodily injury; to this point, most cybercrime results in property loss or damage. *See, e.g.,* U.S. Department of Justice – National Institute of Justice, *Electronic Crime Needs Assessment for State and Local Law Enforcement*, 11 (2001), http://www.ncjrs.org/pdffiles1/nij/186276.pdf (participants reported that cybercrime cases are assigned "a low to medium priority within their agency").

[391] The inadequacy of these resources is a function both (a) of the incremental offenses added by cybercrime and (b) of the fact that cybercrime cases are particularly difficult to investigate. *See, e.g.,* U.S. Department of Justice – National Institute of Justice, *Electronic Crime Needs Assessment for State and Local Law Enforcement*, *supra* note 390, at 16, 23-25. Cybercrime cases are extraordinarily difficult to investigate, first of all, because of their inherent technological complexity; investigations must be conducted by officers who have specialized expertise and access to sophisticated investigatory tools. *See id.; see also infra* Part III(C). Cybercrime cases can also be difficult to investigate (a) because they cross traditional jurisdictional boundaries and (b) because they can pose difficult legal questions as to the unlawfulness of the conduct involved. As to the first issue, *see supra* Part III(A). *See also* Susan W. Brenner & Joseph Schwerha IV, *Transnational Evidence-Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. LAW 347, 375-77 (2002). As to the second issue, *see, e.g.,* U.S. Department of Justice – National

C. Physical Constraints

Cybercrime differs from real-world "crime" in a third respect: The constraints that govern action in the real, physical world do not restrict the perpetrators of cybercrime.[392] Cybercrimes can be committed instantaneously and therefore require a rapid response; law enforcement, however, is accustomed to dealing with real-world "crimes," the investigation of which proceeds at a more deliberate pace.[393] 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.[394] The transborder nature of cybercrime further enhances the difficulties officers face when they attempt to react to a cybercrime because traditional assumptions about a perpetrator's being observed preparing for, committing and/or fleeing from an offense no longer hold.[395]

Cyberspace also lets perpetrators conceal or disguise their identities in a way that is not possible in the real world.[396] 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 or perfect pseudonymity;[397]

Institute of Justice, *Electronic Crime Needs Assessment for State and Local Law Enforcement*, *supra,* at 13; Brenner & Schwerha IV, *supra* at 377.

[392] *See supra* Part II(B)(1)(c).

[393] *See supra* Part III(B); *see, e.g.,* Reuters, *FBI Overwhelmed By Cybercrime* (Mar. 20, 2002), *at* http://zdnet.com.com/2100-1105-864453.html ("'Technology permits cyber crimes to occur at the speed of light and law enforcement must become more sophisticated in uncovering them,' FBI assistant director Ronald Eldon told a conference on fighting organized crime in Hong Kong . . . . 'Government must respond not at government time but at Internet time,' said Eldon.").

[394] *See supra* Part II(B)(2)(c).

[395] *See supra* Part III(A).

[396] It is useful to distinguish between anonymity and pseudonymity: Both involve shielding one's true identity, but the approach used to do so varies. Pseudonymity is using a false name, i.e., an alias, to *disguise* one's identify, while anonymity consists of *concealing* one's identity. *See, e.g.,* Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology and the Constitution,* 7 U. FLA. J. TECH. L. & POL'Y 123, 137 n.43 (2002), *available at* http://grove.ufl.edu/~techlaw/ [hereinafter *Privacy Privilege]; see also* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace,* 11 U. CHI. LEGAL F. 139, 149-52 (1996).

[397] *See supra* note 396 and accompanying text*; see, e.g.,* Anonymizer Total Net Shield, at http://www.anonymizer.com/tns/index.shtml (last visited Dec. 21, 2003) (anonymous email, newsgroups, web surfing, chat and instant messages); Freedom WebSecure, at http://www.freedom.net (last visited Dec. 21, 2003) (anonymous web browsing)*; see also*

consequently, officers may have no way of identifying the person who victimized someone in their jurisdiction.[398] As one report noted, "[t]he ability for criminals to remain anonymous on the Internet presents a huge challenge for police and policy makers."[399]

Even if police can identify a perpetrator, gathering evidence of the cybercrime 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;[400] 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;[401] or the evidence may have been destroyed,

---

Testimony of Deputy Attorney General Eric Holder Before the Subcommittee on Crime of the House Judiciary Committee and the Subcommittee on Criminal Justice Oversight of the Senate Judiciary Committee (Feb. 29, 2000), http://www.cdt.org/security/000229justice.shtml.

> [A] criminal using tools . . . easily available over the Internet can operate in almost perfect anonymity. By weaving his or her communications through a series of anonymous remailers; by creating a few forged e-mail headers with powerful, point-and-click tools readily downloadable from many hacker web sites; or by using a 'free-trial' account or two, a hacker . . . or web based fraud artist can often effectively hide the trail of his or her communications.

[398] For example, in 2000 someone who used the name "Maxus" and claimed to be a Russian hacker stole 300,000 credit card numbers from the online retailer CD Universe. *See, e.g.,* CNN.com, *Rebuffed Internet Extortionist Posts Stolen Credit Card Data* (Jan. 10, 2000), *at* http://www.cnn.com/2000/TECH/computing/01/10/credit.card.crack.2/index.html. Maxus told the company of the theft and demanded that CD Universe pay him $100,000 for the return of the numbers and when CD Universe refused to pay, he posted the numbers on web sites and managed to distribute 25,000 of them before the sites were shut down. *Id.* Maxus was never identified, never caught, and never prosecuted. *Id; see also* Greg Sandoval, *Why Hackers Escape: Organized, Well-Financed Criminals Stay a Step Ahead of the Law,* CNETNews.com (May 14, 2002), *at* http://news.com.com/2009-1017-912708.html.

> The nightmare for Ecount . . . began last year when a hacker broke in to the company's system and stole personal information belonging to its customers. Nine months later, the criminal is still at large. The thief has brazenly taunted executives with repeated e-mails while staying ahead of investigators, deftly wiping away his electronic fingerprints and covering his tracks at every turn.

Id.

[399] Barbara Etter, *Critical Issues in High-Tech Crime*, presentation to the Commonwealth Investigations Conference at the Australasian Centre for Policing Research 13 (Sept. 10, 2002), http://www.acpr.gov .au/pdf/Presentations/CIinHi-tech.pdf.

[400] *See, e.g.,* Goodman & Brenner, *supra* note 17, at 3-5. We may see the emergence of "cybercrime havens," analogies of the bank secrecy havens that appeared in the 1980's. A cybercrime haven country would refuse to prosecute or to extradite, either on the basis of financial gain or ideological considerations. *See id.* at 73-76.

[401] *See, e.g.,* Brenner & Schwerha IV, *supra* note 391, at 377.

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.[402]

D. Patterns

Perhaps because cybercrime is still such a new phenomenon, we cannot identify patterns comparable to those that exist for real-world crime.[403] We cannot, at least so far, empirically derive conclusions as to how various types of cybercrime will manifest themselves geographically and demographically.[404] Consequently, we cannot develop the type of crime maps law enforcement uses to allocate its resources in dealing with real-world crime.[405]

One factor which contributes to 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.[406] 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."[407] Another is that while law enforcement agencies do record reported cybercrimes, they tend not to break them out into a separate category; online fraud, for example, is recorded as "fraud."[408] Yet another reason for the lack

---

Evidence-gathering and presentation can be impeded by yet another factor: expense. Assume, for example, that a county prosecutor in Pennsylvania has identified the perpetrator who hacked into a local bank from India, has charged her with violating Pennsylvania's anti-hacking statute and is preparing the case for trial. Further assume that to present the case the prosecutor will need to present a witness who lives and works in India to authenticate records provided by the Internet Service Provider which the perpetrator used in committing the offense. Finally, assume that it will cost the Pennsylvania county $15,000 to bring the witness in for the trial. Many counties may not be able to bear this expense; even if they have the money available, they will have to consider whether the funds should instead be used to prosecute more "localized" crime, e.g., crimes having a greater and more immediate nexus to that county. *See, e.g., id.*

[402] *See, e.g., Explanatory Report on the Convention on Cybercrime by the Comm. of Ministers*, Council of Eur., 109th Sess., ETS no. 185 (2001) ¶¶ 28-31, ¶¶ 149-57, *available at* http://conventions.coe.int/treaty/ EN/cadreprincipal.htm.

[403] *See supra* Part II(B)(1)(d).

[404] *See supra* Part II(B)(1)(d).

[405] *See supra* Part II(B)(1)(d).

[406] *See, e.g.,* Etter, *supra* note 399, at 9 ("[C]urrently, no comprehensive statistics on hi-tech crime are maintained by Australasian police.").

[407] *See, e.g., id.* ("High-tech crime is variable in its manifestations, so it is difficult to discuss in terms of aggregate incidence and impact."); *see also Virtual Crime, supra* note 2.

[408] *See, e.g.,* FEDERAL BUREAU OF INVESTIGATION, UNIFORM CRIME REPORTS - 2002, *at* http://www.fbi.gov/ucr/cius_02/ 02prelimannual.pdf. *But see* Carol J. DeFrances, *Prosecutors in State Courts 2001*, BUREAU OF CRIM. JUST. STAT. BULL. 5 (May 2002), *at*

of accurate cybercrime data 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 20 countries, one crime or thousands of crimes?[409] 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.[410]

But maybe the lack of accurate statistics is not the real reason why we cannot identify patterns: Pperhaps the notion of "cybercrime patterns" is an oxymoron. After all, the 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 who are, therefore, apt to reside and function in identifiable, economically-disadvantaged neighborhoods.[411] These neighborhoods generate offense and offender patterns because perpetrators tend to target victims of opportunity, i.e., vulnerable individuals who are within some convenient zone of physical proximity.[412]

---

http://www.ojp.usdoj.gov/bjs/pub/pdf/psc01.pdf (reporting number and type of cybercrime prosecutors by state prosecutors). Cybercrime statistics are complied in a few specialized areas. *See, e.g.,* Internet Fraud Complaint Center, *IFCC Annual Internet Fraud Report 2002*, *at* http://www1.ifccfbi.gov/strategy/statistics.asp.

[409] *See, e.g.,* Goodman & Brenner, *supra* note 17*,* at 3-5.

[410] *See, e.g., id. at 27-28*. The lack of official statistics means that the only data we have comes from privately-conducted surveys. *See, e.g., CSI/FBI Computer Crime and Security Survey* conducted by the Computer Security Institute and the San Francisco FBI Office's Computer Intrusion Squad, at http://www.gocsi.com/press/20030528.html (last visited Dec. 22, 2003) (finding that UK businesses seldom reported attacks to law enforcement because they were worried about damage to their reputation resulting from publicity about an attack); *2002 Australian Computer Crime and Security Survey*, *at* http://www.auscert.org (last visited Dec. 22, 2003) (survey conducted by Deloitte Touche Tohmatsu and AusCERT and based on responses from "a wide cross section" of Australian organizations, found that 67% of those responding had suffered attacks within the last year and 35% had experienced six or more attacks. The respondents sustained almost A$6,000,000 in damage. Most attacks (89%) came from the Internet and only a small percentage of the victims (31%) reported the attacks to law enforcement. The survey reported that pessimism as to "the apprehension of attackers" was "the primary inhibitor to greater reporting."); *see also* Survey by the Confederation of British Industry (CBI) (Aug. 2001), at http://www.cbi.org.uk (reporting that two-thirds of the 148 respondents reported having suffered "a serious cybercrime attack" within the last year).

[411] *See supra* Part II(B)(1)(d).

[412] A victim of opportunity is basically someone who is in the wrong place at the wrong time. *See, e.g.,* Jackie Rosenberg, *Victims,* CourtTV.com, *at* http://www.courttv.com/onair/shows/profiler/column_rothenberg.html (last visited Dec. 22, 2003).

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.[413] 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.[414] 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.[415] 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.[416]

"Crime"-category patterns are derived from compilations of data on reported offenses.[417] How does law enforcement use the patterns that appear in the commission of offenses? They can be used to develop profiles of offenders;[418] they can also be used to determine the best means of allocating limited police resources among various units.[419] "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.[420] Location patterns are derived both from data

---

[413] *See supra* Part II(B)(1)(d).

[414] *See supra* Part II(B)(1)(d).

[415] *See supra* Part II(B)(1)(d).

[416] *See supra* Part II(B)(1)(d).

[417] *See, e.g.,* FEDERAL BUREAU OF INVESTIGATION, UNIFORM CRIME REPORTS - 2002, *supra* note 408.

[418] *See, e.g.,* JOHN DOUGLAS & MARK OLSHAKER, MINDHUNTER: INSIDE THE FBI'S ELITE SERIAL CRIME UNIT (1997).

[419] *See, e.g.,* MARILYN B. PETERSON, APPLICATIONS IN CRIME ANALYSIS: A SOURCEBOOK 2 (1998).

[420] *See, e.g.,* Symposium, *Advanced Crime Mapping Topics*, National Law Enforcement & Corrections Technology Center 94-134(held June 25-27, 2001 published 2002), *available at* http://www.nlectc.org/cmap/cmap_adv_topics_symposium.pdf.

compilations of reported offenses and from crime-mapping techniques.[421]

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 they are already emerging. The current inadequacy of statistical data concerning the incidence of cybercrime makes it difficult to extrapolate with any precision as to 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.[422] Another is online fraud, which may exceed hacking in the frequency with which it is committed.[423] The third category encompasses child pornography and using the Internet to solicit children for sexual activity.[424] 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" 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.[425]

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: Since humans 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."[426] If crime is finite, then we should see the same types of "crime" being committed in and via cyberspace – online "crime" will manifest itself in essentially the same ways as real-world "crime." This assumes that we have seen mankind's entire repertoire of antisocial activity, an assumption which

---

[421] *See, e.g., id*.

[422] *See, e.g., Virtual Crime, supra* note *2; CERT Coordination Center 2002 Annual Report*, *at* http://www.cert.org/annual_rpts/cert_rpt_02.html.

[423] *See, e.g.,* Internet Fraud Complaint Center, *IFCC Annual Internet Fraud Report 2002*, *supra* note 408, at 3.

[424] *See, e.g., Enhancing Child Protection Laws After the April 16, 2002 Supreme Court Decision, Ashcroft v. Free Speech Coalition: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary*, 107th Cong. (May 1, 2002) (statement of Michael J. Heimbach, Fed. Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress02/heimbach050102.htm (incidence of online child pornography and its use by child molesters).

[425] *See supra* Part II(B)(1)(d).

[426] *See, e.g.,* Peter B. Wood et al., *Motivations for Violent Crime Among Incarcerated Adults: A Consideration of Reinforcement Processes,* 1994 J. OF THE OKLA. CRIM. JUST. RES. CONSORTIUM, *at* http://www.doc.state.ok.us/DOCS/OCJRC/OCJRC94/940650g.htm.

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.[427] We may well see traditional motivations generating antisocial activity that takes new and different forms in cyberspace,[428] which of course 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" trends 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 these individuals recapitulated what they had observed of real-world criminality in their illicit activities online; they are, in other words, committing "crimes" and have not yet begun to imagine "cybercrime." Cyberspace, after all, not only erases the importance of geography - it also lets us do things we cannot do in real-space. So we may see the emergence of new and as yet unimagined 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 assisted by technology the commission of one "crime" or 5,000 "crimes"?[429] 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 and 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 possibility of mapping the location of cybercrimes? Is there any purpose in doing so? One difficulty that arises is determining what is meant by the "location" of the "crime." As explained earlier, the traditional

---

[427] *See supra* Part II(B)(1)(c).

[428] *See, e.g., Virtual Crime, supra* note 2, at para. 73 (noting that one new type of "crime" has already emerged – the denial of service attack).

[429] *See, e.g.,* Goodman & Brenner, *supra* note 17, at 3-5.

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 when the "crime" is committed.[430] Geography consequently assumes a great deal of importance in dealing with real-world "crime;" focusing an investigation on the physical location of a "crime" offers police their best opportunity for identifying and apprehending the offender(s).[431] 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. If a woman in the Ukraine uses the Internet to defraud a man in Texas, where did the "crime" occur? If one assumes the victim is the locus of a "crime," then it occurred in Texas; but little evidence of the "crime" will be found in Texas and the perpetrator will certainly not be found there. Does this mean "crime"-location patterns will be irrelevant in dealing with cybercrime? It is impossible to answer that question with any certainty.

E. Sum

While the apparent difficulty of identifying patterns in cybercrime does not itself sound the death knell for the traditional model of law enforcement, it, in conjunction with the other difficulties discussed above, clearly establishes that the traditional model is not a suitable means of dealing with online criminal activity. We must come up with a better approach. Doing so could involve 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 Section takes up these issues.

[430] *See supra* Part II(B)(1)(a).

[431] *See supra* Part II(B)(1)(a).

IV. TOWARD A NEW MODEL: DISTRIBUTED SECURITY[432]

[T]here are impediments in the current legal system to fostering . . . computer security.[433]

This section takes up the question posed at the beginning of the Article: why do we need a criminal law for cyberspace? The first part of the discussion explains why the traditional model of law enforcement will become an ever-less-effective means of dealing with cybercrime; this section also explains how modifications in our criminal law can improve our ability to deal with cybercrime.[434] The remainder of this section posits some specific changes to criminal law doctrines and analyzes the extent to which each could enhance our efforts to address cybercrime.[435]

A. From Hierarchy to Network

[N]onstate actors . . . are able to organize into networks . . . more readily than can traditional, hierarchical, state actors . . . . [W]hoever masters the network form stands to gain the advantage.[436]

Our need for a criminal law of cyberspace derives from three premises, the first of which was derived above: It is already apparent that the traditional model of law enforcement, with its reactive approach and hierarchical, military-style organization, cannot deal effectively with cybercrime.[437] The

---

[432] In computer science, "distributed security" denotes a decentralized approach to securing computer networks. *See, e.g.,* Tech FAQ, Techieindex, *What is distributed security?*, *at* http://www.techie.techieindex.com/techie/tech_faq/SecurityFAQ.jsp (last visited Dec. 22, 2003) ("distributed security . . . puts intrusion prevention on every node on the network. By placing intrusion prevention on every node you are not only protecting each of the computers connected to the network, you are protecting the network itself from attack."). This Article uses the term to denote a decentralized system of ensuring internal order within a social system. *See infra* Parts IV(A), IV(B) & V.

[433] *Cyber Security – How Can We Protect American Computer Networks from Attack? Hearing Before the House Committee on Science*, 107th Cong., 107-41(2001) (statement of Dr. William A. Wulf, President, National Academy of Engineering) [hereinafter *Cyber Security Hearing*].

[434] *See infra* Part IV(A).

[435] *See infra* Part IV(B).

[436] David Ronfeldt & John Arquilla, *Networks, Netwars and the Fight for the Future,* 6 FIRST MONDAY 10, (Oct. 2001), *at* http://firstmonday.org/issues/issue6_10/ronfeldt/index.html.

[437] *See supra* Parts II.B, III. The development of this model is the culmination of a process that began centuries ago with the transformation of criminal law enforcement into a state monopoly. As criminal law enforcement became a state monopoly, it evolved a hierarchical organizational structure, at least as to the processes involving the apprehension

second premise derives from the proliferation of technology: Technology – in the form of computers, personal digital assistants, cellular phones, mobile entertainment devices, pagers, Global Positioning System gear and other appliances – pervades much of our daily life, at least in more developed countries.[438] This tendency will only become more pronounced as wireless communication technologies, sentient chips, wearable computers, smart rooms, digital cities and other techno-components of life transform our environment in the twenty-first century.[439] As one student of this phenomenon explains,

> major population centers of the planet will be saturated with trillions of microchips, some of them tiny computers, many of them capable of communicating with each other . . . . [P]eople . . . will have a device with them most of the time that will enable them to link objects, places, and people to online content and processes . . . .[440]

The proliferation of these devices, all linked in various and varying ways, will create and sustain a fluid, continuously operating global network.

This takes us to the third premise: The proliferation of these technologies will have a profound effect upon the organization of human social systems and activities. As noted above, the world will become a single interdependent, interlinked network.[441] For the last several millennia, the organization of human social systems and activities – government, commerce, education, religion, military – has been hierarchical: a top-down approach to the structuring of social relationships and the allocation of authority.[442] This default hierarchical organizational model evolved to deal with the organization of activity in the real world: since human activity is subject to the physical constraints of empirical reality, it requires the use of techniques such as a chain of command to orchestrate and focus the efforts of groups of humans on achieving particular tasks, e.g., mining coal, smelting steel, sailing ships,

---

of perpetrators. *See id.* Civil law, on the other hand, tends to have a more lateral structure; the state acts primarily as a facilitator, a referee, between private parties.

[438] *See, e.g.,* HOWARD RHEINGOLD, SMART MOBS: THE NEXT SOCIAL REVOLUTION xi-xxii (2003).

[439] *See, e.g., id.* at 84-85 (sentient chips); *see also id.* at 133-56 (wireless networks), 106-12 (wearable computers), 102-09 (smart dust & smart rooms), 98-100 (digital cities).

[440] *Id.* at xii-xiii*; see also supra* note 439.

[441] *See, e.g.,* Ronfeldt & Arquilla, *supra* note 436, *at* http://firstmonday.org/issues/issue6_10/ronfeldt/index.html.

[442] *See, e.g.,* Brian Nichiporuk & Carl H. Builder, *Societal Implications*, *in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 297 (John Arquilla & David Ronfeldt eds., 1997) ("Hierarchical organizations . . . are the basis upon which most authority, power, and command and control have been exercised for millennia.")*; see also* LEWIS MUMFORD, THE MYTH OF THE MACHINE: TECHNICS AND HUMAN DEVELOPMENT 189-202 (1967).

building pyramids, waging wars and keeping order within a social system.[443]

The proliferation of technology and consequent rise of cyberspace abolish the need to rely on the hierarchical organizational model to channel human activity. Communication technologies free us from the physical constraints of the empirical world: we can now communicate instantaneously with anyone anywhere, with multiple "anyones" in many "anywheres."[444] This produces a new type of social organization – the network.[445] The rise of the network is not without precedent. Indeed, the development of new technology has historically resulted in the appearance of new forms of social organization.[446]

---

[443] *See, e.g.,* RHEINGOLD, *supra* note 438, at 200 ("By organizing workforces and military forces hierarchically and breaking their tasks into component parts, entire populations could organize into social machines to build pyramids and conquer empires."); NATALI KASSAVIN & URI MERRY, COPING WITH UNCERTAINTY: INSIGHTS FROM THE NEW SCIENCES OF CHAOS, SELF-ORGANIZATION AND COMPLEXITY 21 (1995) ("People create the nation-state to ensure order in . . . society."); *see also* MUMFORD, *supra* note 442, at 189-202.

[444] *See, e.g., Organized Cybercrime, supra* note 293.

> [H]ierarchical organizational models are products of the real world . . . . Cyberspace . . . is not a fixed, predetermined reality operating according to principles and dynamics that cannot be controlled or altered by man. The cyberworld is a constructed world, a fabrication . . . . In the real world, it takes a great orchestration of human effort to send a hard copy file halfway around the world. In cyberspace, one can send an electronic version of the same file halfway around the world with only a few keystrokes.
>
> This essential absence of physical constraints is one factor that differentiates the cyberworld from the real world. Another differentiating factor is the way we experience the two realities. Physical reality has a fixed empirical structure; this structure itself is not hierarchical, but we necessarily experience it through the filter of socially-organized hierarchical structures. If we want to send a hard copy of a file to someone halfway around the world, speak to that person on the telephone, or travel to visit, we must rely upon and participate in hierarchical structures to do so . . . . The lack of physical constraints in cyberspace . . . means that our experiences there do not have to be mediated through hierarchical structures. Indeed, the very nature of cyberspace is inconsistent with hierarchy. Cyberspace is a network or, more properly, a network of networks. Networks are lateral, diffuse, fluid, and evolving. Hierarchies are vertical, concentrated, and tend to be rigid and fixed.

See also Ronfeldt & Arquilla, *supra* note 436, *at* http://firstmonday.org/issues/issue6_10/ronfeldt/index.html.

[445] *See, e.g.,* Ronfeldt & Arquilla, *supra* note 436, *at* http://firstmonday.org/issues/issue6_10/ronfeldt/index.html.

[446] *See, e.g.,* David Ronfeldt, *Tribes, Institutions, Markets, Networks: A Framework About Social Evolution* 5-17 RAND (1996), *at* http://www.rand.org/publications/P/P7967/P7967.pdf; Ronfeldt & Arquilla, *supra* note 436, *at* http://firstmonday.org/issues/issue6_10/ronfeldt/index.html; *see also* RHEINGOLD, *supra* note 438, at 200 ("The cultural innovations that reorganize social interaction in light of new technologies are 'social algorithms governing the uses of technology.'") (citing ROBERT

Networks are displacing hierarchies in every sector of society because a hierarchical organization is not an effective means of organizing technologically-mediated activities.[447] Nonetheless, hierarchical organization will persist in areas of human endeavor that are based in the real world, because hierarchies are an effective means of organizing activities in this venue.[448]

Networks, unlike hierarchies, are lateral, fluid systems.[449] Networks, unlike hierarchies, decentralize power and authority, thereby empowering individuals.[450] Networks have the capacity to, and very likely will, usher in a new era of cooperation among peoples and among social systems.[451] Unfortunately, they can also be exploited for destructive purposes.

> Most people might hope for the emergence of a new form of organization to be led by 'good guys' . . . . But history does not support this contention.
>
> The cutting edge in the early rise of a new form may be found equally among malcontents . . . and clever opportunists eager to take advantage of new ways to maneuver, exploit, and dominate. Many centuries ago . . . the rise of hierarchical forms of organization . . . was . . . attended . . . by the appearance of ferocious chieftains bent on military conquest and of violent secret societies . . . . [T]he early spread of the market form, only a few centuries ago, was accompanied by a spawn of usurers, pirates, smugglers, and monopolists, all seeking to elude state controls over their earnings and enterprises.
>
> Why should this pattern not be repeated in an age of networks? There appears to be a subtle, dialectical interplay between the bright and dark sides in the rise of a new form of organization. The bright-side actors may be so deeply embedded in and constrained by a society's established forms of organization that many have difficulty becoming the early . . . adopters of a new form. In contrast, nimble bad guys may have a freer, easier time acting as the cutting edge. . . .[452]

WRIGHT, NONZERO: THE LOGIC OF HUMAN DESTINY 22-23 (2000)).

[447] *See, e.g.,* Nichiporuk & Builder, *supra* note 442, at 298-99*; see also supra* note 444.

[448] *See* Nichiporuk & Builder, *supra* note 442, at 301 (noting that "functions that . . . require reactive behavior will tend to be executed by groups that are relatively hierarchical in nature, while those that . . . allow for proactive behavior will be relatively more networked."); *RICO*, *supra* note 290, at 39.

[449] *RICO supra* note 290, at 39.

[450] *See, e.g.,* Nichiporuk & Builder, *supra* note 442 at 299 (noting that networks shift power to individuals).

[451] *See, e.g.,* RHEINGOLD, *supra* note 438*,* at 208-15 ("cooperation amplification").

[452] David Ronfeldt & John Arquilla, *What Next for Networks and Netwars?*, *in*

As Part III explained, this is precisely what is occurring with regards to cybercrime. Law enforcement, which for the most part is still "embedded in and constrained by . . . established forms of organization," is lagging behind the "bad guys," who have learned how to exploit the distributed, non-territorially-based, realities of cyberspace.[453] The question is, how do we bring law enforcement up to speed? Put differently, how can law enforcement adapt to the new realities of cybercrime?[454]

The core problem is law enforcement's reactive approach to "crime." As Part III demonstrated, the traditional reactive mode is not effective for cybercrime because cybercrime is elusive. Offenders are elusive because there is no necessary nexus between the situs of a "crime" and the perpetrator's physical location, either at the time the "crime" is committed or afterward.[455] They are also elusive because they can shield their identities and avoid leaving traditional types of physical evidence.[456] "Crimes" are elusive because they do not fall into recognizable offenses and/or offender patterns[457] and because they can be committed on such a scale that law enforcement officers simply cannot react to all of them.[458]

One solution to this problem would be to somehow improve law enforcement's ability to react to completed cybercrimes. This could involve any of several approaches. One possibility would be to significantly increase the number of officers who are available to react to cybercrime. As noted earlier, one of the reasons cybercrime is so problematic for law enforcement is that it constitutes an incremental addition to the quantum of "crime" to which

---

NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME AND MILITANCY 311, 313 (John Arquilla & David Ronfeldt eds., 2001), *available at* http://www.rand.org/publications/MR/MR1382; *see also* Kevin Manson, Office of Int'l Criminal Justice, *Robots, Wanderers, Spiders and Avatars: The Virtual Investigator and Community Policing behind the Thin Digital Blue Line* (1997), *available at* http://www.dougmoran.com/tatzlwyrm/CACHE/Digital_Officer_Safety/Attachments/Robots_Wanderers_Spiders_and_Avatars.PDF ("Given the extraordinary pace of new technology development and deployment on the Internet, it will become necessary to reevaluate the paradigms that have defined the resources and procedures for the delivery of policing . . . .").

[453] *See* David Ronfeldt & John Arquilla, *supra* note 436.

[454] As noted earlier, the traditional, hierarchical, reactive model of law enforcement will no doubt continue to be an effective means of addressing real-world crime. *See supra* note 349 and accompanying text. After all, even in the mid-twentieth century world of *Minority Report,* law enforcement's way of preventing "crime" was to react to the prospect of consummated crime. *See* Minority Report: The Story, http://www.minorityreport.com (last visited Nov. 24, 2003*); see also* PHILIP K. DICK, THE MINORITY REPORT (2002).

[455] *See supra* Part III(A).

[456] *See supra* Part III(C).

[457] *See supra* Part III(D).

[458] *See supra* Part III(B).

law enforcement must react.[459] Since cybercrime undermines the effectiveness of the reactive strategy by increasing the number of "crimes" to which officers must react, it seems that increasing the number of officers should offset this effect and restore the efficacy of the reactive strategy. Unfortunately, the problem is that since cybercrime is increasingly automated, there is no longer a necessary one-to-one correlation between offender and offense;[460] cybercrime is becoming an "arms race" between criminals and law enforcement. Therefore, it cannot be combated effectively simply by hiring more law enforcement officers.[461]

If hiring more officers is not the answer, what is? Another strategy would be to combat fire with fire, i.e., to automate policing in cyberspace. This would involve using automated agents to react to completed cybercrimes and to "patrol" public areas of cyberspace in an effort to prevent the commission of cybercrime.[462] While automated cyberpolicing is certainly a logical alternative, its implementation is surrounded with technical and legal difficulties,[463] thus making it an unrealistic option for the foreseeable future.

A third alternative is to authorize civilian use of defensive technologies, i.e.,

---

[459] *See supra* notes 390-91 and accompanying text.

[460] *See supra* Part III(B).

[461] *Securing Our Infrastructure: Private/Public Information Sharing: Hearing Before the U.S. Senate Committee on Governmental Affairs* (May 8, 2002) (statement of Alan Paller, Director of Research, The SANS Institute), *available at* http://www.senate.gov/~gov_affairs/050802paller.pdf ("The fight against cybercrime resembles an arms race where each time the defenders build a new wall, the attackers create new tools to scale the wall."). *See generally supra* Part II(B)(2).

Another problem with the alternative discussed above is that since cybercrime disregards territorial boundaries, simply hiring more officers in no way guarantees that officers will be able to react effectively to particular cybercrimes. *See supra* Part III(A). The ultimate futility in this alternative is the fact that there simply are not enough resources available to fund hiring even a colorably adequate number of new officers to deal with cybercrime. *See, e.g., State Police Announce Promotions,* CHARLESTON GAZETTE, Jun. 26, 2003, *available at* 2003 WL 5473318 (lieutenant colonel said state police agency "is vastly underfunded, underequipped, [and] undermanned"); *see also* Gordon Dillow, *LA Wants to Spread Its Disease,* ORANGE COUNTY REGISTER, Jun. 15, 2003, *available at* 2003 WL 6999990 (noting the "undermanned and underfunded Los Angeles Police Department").

[462] *See, e.g.,* Manson, *supra* note 452, *at* http://www.dougmoran.com/tatzlwyrm/CACHE/Digital_Officer_Safety/Attachments/Robots_Wanderers_Spiders_and_Avatars.pdf (proposing the use of automated intelligent agents as cybercrime-fighters).

[463] *See, e.g., id.*, *at* http://www.dougmoran.com/tatzlwyrm/CACHE/Digital_Officer_Safety/Attachments/Robots_Wanderers_Spiders_and_Avatars.pdf ("Matters of comity, sovereignty and legal jurisdiction will . . . have to be resolved before intelligent agents begin coursing through servers in foreign universities, banks and government agencies.").

to let cybercrime victims use "'strike-back' or 'counterstrike' tools."[464] The rationale here is that victims react when they are the targets of cybercrime and thereby supplement the reactive capabilities of law enforcement personnel.[465] The premise is that a computer system which is "under attack automatically traces back the source and shuts down, or partially disables, the attacking machine(s)."[466] This alternative raises difficult legal questions,[467] but ultimately founders on the risks involved in authorizing victim self-help:

> Not all attacks will . . . reveal a path back to their source . . . . [T]racing an attack to an intermediate attacking machine, not to speak of the computer owned by the originator in a DDoS attack, may be impossible . . . . And intermediate machines . . . may be operated by hospitals, governmental units, and telecommunications entities . . . that provide connectivity to millions of people: counterstrikes which are not very, very precisely targeted . . . could easily create a remedy worse than the disease. Where the offense is spam . . . the trace will generally lead to an anonymous account on a server – a server which is legitimately used for other communications as well. Disabling that server is overkill.[468]

Since these three alternatives exhaust the available options for improving reactions to completed cybercrime, it seems this is not a viable way to improve law enforcement's ability to deal with cybercrime. The solution must therefore lie elsewhere. The conceptual alternative to the reactive model is a model based on crime prevention. While the reactive approach incorporates notions of crime prevention insofar as it is predicated on incapacitating and deterring offenders,[469] the alternative model is based on strategies that are designed to

---

[464] Curtis E.A. Karnow, *Strike and Counterstrike: The Law on Automated Intrusions and Striking Back*, Black Hat Windows Security (Feb. 27, 2003), *at* http://www.blackhat.com/presentations/win-usa-03/bh-win-03-karnow-notes.pdf.

> Content providers such as record labels and movie studios favor . . . federal legislation that would allow them to disable copyright infringers' computers. Software licensors endorse state laws that permit the remote disabling of software in use by the licensee when the license terms are breached. Internet security professionals debate the propriety and legality of striking back at computers which launch worms, viruses, and other intrusions.

Id.

[465] *See id.*

[466] *Id.*

[467] *See id.* ("While it is generally thought to be illegal to strike back, the rationale is usually based on the practicality of pinpointing the perpetrator, and killing the wrong machine or code. But . . . the accurate targeting of a perpetrator's machine itself presents serious legal issues: A host of statutes . . . make it illegal to attack or disable computers, including those connected to the Internet . . . .").

[468] *Id.*

[469] *See supra* notes 341-42 and accompanying text.

inhibit the commission of "crimes."[470] Known as "community policing," this real world model emphasizes "putting officers back on the streets," where they become "part of the fabric of the neighborhood, as a constant, known, dependable presence, instead of racing around the city in patrol cars, reacting to crimes that have already happened."[471] It also emphasizes cooperation between police and citizens in creating a climate where "crime" is not tolerated.[472] Community policing has had notable successes in the real world, but it can be difficult to implement, as it is labor-intensive, requires organizational restructuring, and can raise ethical issues about the allocation of scarce resources.[473]

There are at least two reasons why community policing has not been implemented in the cyber-world. One is that doing so would require assigning police officers to "patrol" areas of cyberspace, which would require hiring new officers and/or assigning officers who are currently dealing with real world "crime" to cyberspace. In an era of scarce resources, neither is a viable option.[474] The other reason is that there really are no "communities" in cyberspace, at least not the kind of communities that law enforcement officers

---

[470] *See, e.g.,* Lawrence Sherman, *Thinking About Crime Prevention, in* U.S. DEP'T OF JUSTICE: WHAT WORKS, WHAT DOESN'T, WHAT'S PROMISING (1997), *available at* http://www.ncjrs.org/works*; see also* CRIME COMMISSION REPORT 2003, § II ("Community Policing and Law Enforcement Organization"), *at* http://www.lancasteronline.com/crimereport/0302/comm_police.shtm.

[471] CRIME COMMISSION REPORT 2003, *supra* note 470, § 2.

[472] *See id.*

> [C]ommunity policing is a radical departure from the traditional, reactive model of policing. With that method of law enforcement, police are isolated from the community, shielded by their patrol cars . . . .
>
> [It] recognizes that the neighborhood is the point of coordination for . . . crime prevention . . . . [I]t further recognizes that although the police are there to support the citizens, it is the people who live in the neighborhoods . . . who must act to take back their own streets . . . .

Id.; see also Barry N. Leighton, *Visions of Community Policing: Rhetoric and Reality in Canada*, 33 CANADIAN J. CRIMINOLOGY 485, 487 (1991).

[473] *See, e.g.,* Leighton, *supra* note 472*,* at 496-98, 503-11; David Thacher, *Equity and Community Policing: A New View of Community Partnerships*, 20 CRIM. JUST. ETHICS 3 (2003); Gerasimos A. Gianakis & G. John Davis, III, *Reinventing or Repackaging Public Services? The Case of Community-Oriented Policing,* 58 PUBLIC ADMIN. REV. 485 (1998).

[474] *See supra* note 461. Many law enforcement agencies do have officers who are assigned to cybercrime, and many of these officers "patrol" certain areas of cyberspace. No agency, however, maintains a 24/7 presence in cyberspace and it is exceedingly unlikely that any will be able to do so in the foreseeable future. *See, e.g.,* Gary Nurenberg, *Cracking Down on Online Predators,* Tech TV (Aug. 27, 2002), *at* http://www.techtv.com/news/internet/story/0,24195,3397013,00.html; Molly Masland, *Stalking Child Molesters on the Net,* MSNBC (Sept. 4, 1998), *at* http://www.msnbc.com/news/192795.asp.

can effectively control. "Communities" in cyberspace tend to be defined by interests, not by territory.[475] They therefore attract people from various locations around the world and consequently defy the territorially-based assumptions that are an essential part of "community policing," at least as it has evolved in the real world.[476]

While we cannot extrapolate community policing to cyberspace, two aspects of the community policing model suggest an approach that can be used to address online "crime." The traditional, reactive model of law enforcement cannot deal effectively with cybercrime because cybercrime is a fluid, lateral phenomenon; it is, in effect, distributed "crime."[477] Since cybercrime is a lateral, pervasive phenomenon, it demands a lateral, pervasive solution. This solution can incorporate a reactive element but, as explained above, a purely reactive approach will be inadequate.[478] The solution therefore needs to be proactive; it must focus on preventing cybercrime, not merely reacting to it. The solution also needs to employ a collaborative approach, one that combines the efforts of civilians and law enforcement; this approach addresses the problem noted earlier, namely, that it is neither financially nor pragmatically possible to deploy enough law enforcement officers to maintain order in cyberspace.[479] Clearly, therefore, the way to address cybercrime is to utilize the community policing model's concepts of a proactive, collaborative approach to "crime."[480]

Doing this would seem to require creating a new model of law enforcement, one specifically directed at cybercrime. Actually, it requires disassembling assumptions and expectations predicated on the traditional model and replacing them with a different set of assumptions and expectations. As noted earlier, under the traditional model, citizens share no responsibility for reacting to "crime;"[481] consequently, they have come to think of law enforcement as the polices' exclusive responsibility.[482] The community policing model seeks to

---

[475] *See, e.g.,* Peter Kollock & Marc A. Smith, COMMUNITIES IN CYBERSPACE 3-28 (Marc A. Smith & Peter Kollock eds., 1998).

[476] *See, e.g.,* "Welcome to Communities.com," Communities.com, *at* http://www.communities.com ("Communities.com is a fun new online community where people from all over the world (now with members from 165 countries!) meet, chat and interact . . . .") (emphasis in the original) (last visited Nov. 24, 2003).

[477] *See supra* Part III.

[478] *See supra* Part III.

[479] *See supra* notes 461 and 475.

[480] *See supra* notes 471-73 and accompanying text.

[481] *See supra* Part II(B)(2)(b).

[482] *See, e.g.,* William D. Eggers & John O'Leary, *The Beat Generation: Community Policing at Its Best*, 74 POL'Y REV. 5, 6 (1995): ([T]he public began to forget its role in controlling crime and grew increasingly dependent on the police. Police departments became more professionalized and shifted . . . to crime fighting . . . . Americans began to

reverse this process, at least in part, by involving citizens in combating "crime" in their real world neighborhoods.[483] Community policing does this by putting officers in neighborhoods where they work to prevent "crime" by patrolling the area to discourage criminal activity and by encouraging citizens not to tolerate such activity.[484] Citizens are involved, but they still are not responsible for reacting to crime.

This particular model cannot be used to deal with cybercrime because, as was explained earlier, police cannot patrol "neighborhoods" in cyberspace.[485] This model relies on an active police presence, reinforced by neighborhood support, to control "crime" and maintain order. A variation on the community policing model, however, could be used to control cybercrime. This modified model does not rely primarily on an active police presence and only secondarily on citizen efforts; instead, it relies primarily on active citizen efforts and secondarily on police support of those efforts. It is not a *community* policing model; it is a *distributed* policing model in which citizens assume responsibility for discouraging the commission of cybercrime. It represents the disassembling of the traditional model of law enforcement insofar as citizens assume responsibilities with regard to a particular type of "crime."[486] It does not represent the re-establishment of the antecedent model because while citizens may have some role in reacting to completed cybercrimes, their primary responsibility is to prevent the commission of cybercrimes.[487] Citizen prevention serves both to maintain internal order and ward off external threats, since cyber-attacks, unlike conventional real world "crimes," can constitute acts of war or terrorism, as well as criminal activity.[488]

---

think of crimefighting as the job of police . . . .); *see also* Richard A. Leo, Some Thoughts about Police and Crime *in* THE CRIME CONUNDRUM, ESSAYS ON CRIMINAL JUSTICE 121, 121-22 (George Fisher & Lawrence M. Friedman eds., 1997).

[483] *See supra* notes 471-73 and accompanying text.

[484] *See supra* note 473.

[485] *See supra* notes 476-77 and accompanying text.

[486] *See supra* Part II(B)(2)(b).

[487] *See id*. As explained above, there are compelling legal and practical reasons why citizens should not react to cybercrime. *See supra* notes 468-69 and accompanying text.

[488] *See, e.g.,* Office of the President, *The National Strategy to Secure Cyberspace* 5-7, 37-41 (Feb. 2003), *at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf. This is another distinguishing aspect of cybercrime: Much of the conduct defined as cybercrime, and especially attacks on computer systems, can provide the predicate for threats to a system's ability to maintain external order, as well as its ability to maintain internal order. The distinction here is between attacks upon individual citizens of a social system ("crimes") and attacks on the social system itself ("terrorism"). It is true that acts which are encompassed by definitions of terrorism also represent "crimes;" Timothy McVeigh, for example, engaged in a terrorist act and, in so doing, committed murder and large-scale property damage and destruction. The critical difference between cybercrime-as-terrorism

Postulating this model raises two questions: Why should citizens assume responsibility for preventing cybercrimes when they have no such responsibility as to real world "crimes"? Moreover, assuming citizens should assume such responsibility, how is this to be achieved? That is, how are assumptions fostered by the traditional model of law enforcement to be displaced and new expectations to be inculcated? The sections below address these questions.

1. Why impose responsibility for prevention?

We in no way make citizens[489] responsible for preventing real-world "crimes." We take a laissez-faire attitude toward crime prevention in the real world.[490] I can go to work leaving my front door unlocked and a rear window open, feeling secure in the knowledge that if a burglar takes advantage of the situation to steal my television, my laptop and my stereo, I can call the police and they will make an effort to find the burglar and recover my property. It is, of course, possible that the officers involved may not put forth their best effort in doing so. They may make the burglary a lesser priority than other "crimes," perhaps out of a sense of frustration at my irresponsibility. I, however, will never know what the officers will do. They may well expend their best efforts to recovery my property and apprehend the perpetrator. The point is that my irresponsibility is legally irrelevant; criminal law does not require a blameless victim.[491] Criminal law disregards my carelessness because a "crime" is an offense against the authority of the state and therefore must be addressed by the state, without regard to the circumstances that contributed to its commission.[492] This proposition from the systemic need to maintain internal order and the empirical reality that deviant behavior constitutes a serious threat to such order.[493] Criminal law's disinclination to take victim blameworthiness into account is probably also attributable to the fact that it is no doubt easier to deal with "crimes" such as these is no doubt easier than trying to enforce laws

and "crimes"-as-terrorism is that "crimes" have to be executed within the physical boundaries of the system, whereas cybercrimes do not. *See generally Emerging Consensus,* 2 ILL. J.L. TECH. & POL'Y 1(2002).

[489] As used in this discussion, "citizens" denotes both individual and artificial members of a social system. Corporate and other artificial entities, like individuals, can be lax about cybersecurity, thereby providing an opportunity for a cybercriminal to exploit. *See, e.g.,* Office of the President, *supra* note 488, at x-xiii, 5-11.

[490] Tort law in many states does impose liability for failing to protect someone from "crime" under certain circumstances, such as where a landlord assumes a duty to protect residents from victimization. *See, e.g.,* Peter Everett, *Establishing a Duty: Reaching the Promised Land,* 36 APR TRIAL 33, 33-34 (2000).

[491] *See infra* Part IV(B)(2).

[492] *See id*.

[493] *See supra* Part II(A).

requiring people to maintain security.[494]

Why should citizen obligations be different with regard to cybercrime? The primary reason is that if I leave my front door unlocked and a rear window open and a burglar takes advantage of my carelessness, the only one harmed is me, the architect of my own victimization.[495] This is not necessarily true for cybercrime. Assume that instead of the scenario above, I access the Internet using an always-on broadband connection without using any security to prevent a hacker from hijacking my laptop.[496] I have opened my laptop up to attack, which creates a situation analogous to the burglary example: I have carelessly exposed myself to "harm" from a criminal. But I have also created the potential for "harm" to others – my carelessness has created a situation in which a hacker can take over my laptop and use it to victimize other individuals and entities.[497] In cyber world, my carelessness results in the

[494] Imposing an affirmative legal obligation to maintain personal security by, e.g., installing an alarm system, locking doors and taking other precautions to protect the security of one's property and the safety of one's person would impose another responsibility on an already-overwhelmed police force. In addition to having to react to completed "crimes," officers would be expected to enforce laws mandating security. This could mean that they would devote time which could more profitably be spent discouraging the commission of "crimes" and/or apprehending the perpetrators of "crimes" enforcing the laws that mandate security by, e.g., writing tickets to homeowners who had not installed alarm systems. More realistically, it would probably mean that officers would not make the enforcement of laws mandating security a priority, at least not unless and until such enforcement offered the opportunity to explore the commission of "crimes." *See, e.g.,* Stewart v. Trask, No. CIV.A. 02-7703, 2003 WL 21500018 *5 (E.D. Pa. Jun. 27, 2003) (citing seat belt violation as pretext for vehicle stop).

[495] My victimization does impose a cost on the law enforcement system in that officers will have to respond to my report of the "crime" and will have to expend at least some effort in endeavoring to find the perpetrator and recover the lost goods. And if they succeed in doing so, the criminal justice system will have to expend resources in prosecuting and, presumably, punishing the perpetrator. These costs are not significant, however, since it is likely that the perpetrator would have burglarized some other home had I not made mine such an inviting target, either because she is in the habit of robbing houses or because she was bent on such activity on this occasion. One cannot, in other words, say that my carelessness "caused" the burglary.

[496] *See, e.g.,* Office of the President, *supra* note 488, at 39; John Broughton, *Cable Modem and DSL Security Issues and Solutions,* BERKELY COMPUTING & COMMUNICATIONS, Apr-May 2000, *at* http://istpub.berkeley.edu:4201/bcc/Apr_May2000/sec.dsl.html.

[497] *See, e.g.,* Bob Sullivan, *Could Your Computer Be a Criminal?,* MSNBC (Jul. 15, 2003), http://www.msnbc.com/news/939227.asp:

> One thousand home computers hijacked and used to serve up pornography. Perhaps tens of thousands co-opted by the 'SoBig' virus, many . . . turned into spam machines. Hundreds of other home computers loaded with secret software used to process stolen credit cards. If your biggest computer crime fear was lost or stolen files, think again: Someone may be using your PC to commit crimes.

infliction of incremental "harms" that exceed those which I would suffer from any personal attack. A cybercriminal can use my laptop, along with other hijacked laptops, to launch a denial of service attack on an online business or a government website, shutting them down. To do this, the perpetrator requires access to a critical mass of zombie computers, which I have helped to supply.[498] The effects of my carelessness will be particularly egregious if terrorists or organized criminals use my laptop to attack my country's infrastructure; it is at this point that victim defaults threaten to jeopardize a system's ability to sustain both internal and external order.[499]

The most compelling reason for imposing responsibility for preventing cybercrimes on citizens, therefore, is that failure to secure their systems can result in "harm" to other members of their social system and can even threaten the security of the entire system. Another reason is that law enforcement is less effective in maintaining order in cyberspace than it is in real-space. In the real world example, police may well apprehend the burglar who stole my property because my neighbors saw him, because he left trace evidence in my house and/or because he tried to dispose of the property he took from me.[500] In the online example, the cyberperpetrator stands an excellent chance of avoiding apprehension, since he is able to act remotely and anonymously, and since he does not risk identification and apprehension if he elects to dispose of the electronic property he took from me.[501] In sum, citizens should assume a measure of responsibility for maintaining order, just as they have done in the past since (a) citizen lapses in security can endanger others and (b) law enforcement cannot, alone, maintain order in cyberspace.[502]

See also Office of the President, *supra* note 488, at 39; Mo Krochmal, *Distributed Denial of Service Threat Grows,* TECHWEB (Feb. 8, 2000), *at* http://www.techweb.com/wire/story/TWB20000208S0016.

[498] *See, e.g.,* Xianjun Geng & Andrew B. Whinston, Defeating Distributed Denial of Service Attacks, IT PRO, July/Aug. 2000, *at* http://cism.bus.utexas.edu/works/articles/defeating_ddos.pdf. As a subsidiary point, my carelessness has also undermined law enforcement's ability to maintain order in cyberspace: The denial of service attack is an example of automated "crime;" as explained earlier, the scale of automated "crime" puts an additional burden on investigating law enforcement personnel. *See supra* Part III(B)(2). The use of use of zombie computers also makes law enforcement's task that much more difficult; it is harder to trace an attack back along the path of the zombies to find the person ultimately responsible for the attack. *See, e.g.,* D. Ian Hopper, *Denial of Service Hackers Take on New Targets,* CNN.com (Feb. 9, 2000), http://www.cnn.com/2000/TECH/computing/02/09/denial.of.service.03/.

[499] *See supra* note 489 and accompanying text.

[500] *See supra* Part II(B)(1)(c).

[501] *See supra* Parts III(A)-(C).

[502] *See supra* Part II(B)(2)(b).

2. How is responsibility to be imposed?

If responsibility for preventing cybercrime is to be imposed, it becomes necessary to decide how that should be done. This necessitates the consideration of two dichotomies. The first deals with how a social system can make its constituents engage in a particular conduct. Conduct can be voluntary or obligatory. In this context, voluntary conduct is conduct in which the members of a social system engage because they believe that it is "right" or "appropriate." This belief that particular conduct is "right" or "appropriate" (and, conversely, that other conduct is "wrong" or "inappropriate") is based on norms which the members of the social system have internalized; this type of conduct is "voluntary" because it is the product of internal social control mechanisms.[503] Obligatory conduct, on the other hand, is the product of external social control mechanisms. It is conduct in which the members of a social system engage or avoid because they understand that their failure to conform to what is externally required can result in some form of sanctions by that system.[504] Obligatory conduct is thus voluntary in the sense that a member of a social system decides whether or not he or she will engage in the prescribed conduct. It is not "voluntary" in the sense used above, however, because the decision to behave in a particular way is prompted by the awareness of externally-imposed consequences for one's failure to do so.[505]

a. Voluntary approach to citizen responsibility

A voluntary approach to achieving citizen responsibility for preventing cybercrime would require establishing a norm to that effect. Once the members of a social system had internalized this norm, they would regard preventing cybercrime as the "right" or "appropriate" thing to do and would therefore endeavor to comply with the norm. How could such a norm be established? The process would involve educating the populace of a social system as to the need for preventative efforts; it could also educate them in the use of tools that can reduce or eliminate the risk of cybercrime.[506] It might appeal to their sense of system loyalty by emphasizing the impact cybercrime can have upon the system's economy and the potential for external threats to system infrastructures.[507] An approach such as this would be the most

[503] *See supra* notes 230-31 and accompanying text.

[504] *See supra* notes 230-31 and accompanying text*; see also* Hart, *supra* note 261, at 6-7.

[505] *See supra* notes 230-31 and accompanying text.

[506] The approach sketched out above would be functionally analogous to the "safe sex" campaigns that seek to reduce the spread of AIDS. *See, e.g.,* Press Release, Médecins sans Frontières, Médecins *sans* Frontières *Launches Safe Sex Campaign in Mongolia* (Dec. 1, 1999), *at* http://www.msf.org/countries/page.cfm?articleid=EFD71826-E65D-11D4-B2010060084A6370.

[507] *See, e.g.,* Office of the President, *supra* note 488, at 5-7, 37-41.

effective way to achieve citizen prevention of cybercrime, since the most effective means of channeling behavior into desired paths is not the "imposition of external sanction, but the inculcation of internal obedience."[508] The problem is that it can take a long time to establish a norm and inculcate an optimum level of obedience.[509] This is especially likely to be true for cybercrime prevention, because the conduct to be encouraged involves cyberspace, which is an alien environment for many members of contemporary social systems. Although citizens may believe that it is advisable to install alarm systems and "burglar bars" to ensure their safety from real-world threats,[510] they are unlikely to appreciate the very "real" dangers that are lurking in the virtual world of cyberspace.[511] The difficulty of establishing this norm is further exacerbated by the fact that it would, at least in part, have to displace a deeply embedded norm, namely, that addressing actual or potential criminal activity is the exclusive province of law enforcement.[512] For these reasons, and others, a purely voluntary approach is unlikely to be effective.[513]

---

[508] Harold Hongju Koh, *How Is International Human Rights Law Enforced?,* 74 IND. L.J. 1397, 1401 (1999); *see, e.g.,* TOM R. TYLER, WHY PEOPLE OBEY THE LAW 4 (1990).

[509] *See generally* Posner & Rasmussen, *supra* note 230, at 377-80. It can also be difficult to succeed in creating norms. *See, e.g.,* CINDY PATTON, FATAL ADVICE: HOW SAFE-SEX EDUCATION WENT WRONG 118-26 (1996*); see also supra* note 508.

[510] *See, e.g.,* Robyn Israel, *Guarding the Fort,* PALO ALTO WEEKLY (Sept. 18, 1998), *at* http://www.paloaltoonline.com/weekly/morgue/real_estate/1998_Sep_18.HOME18.html.

[511] One reason for the relative lack of concern about cybersecurity is no doubt the fact that the risks of individual physical injury associated with cybercrime are, so far, very minor. One can be injured by a person they met online and had a physical encounter with in the real-world, but the direct infliction of one-to-one physical injury is simply not possible.

[512] *See supra* Part II(B)(2)(b).

[513] The President's National Strategy to Secure Cyberspace, the final version of which issued in 2003, has been strongly criticized for relying upon a purely voluntary approach. *See, e.g.,* James A. Harvey, *An Early Look at the National Strategy to Secure Cyberspace,* Giga.Law.com, *at* http://www.gigalaw.com/articles/2003-all/harvey-2003-04-all.html (''cybersecurity is too tough a problem for a solely voluntary approach to fix . . . . Companies will only change their behavior when there are both market forces and legislation that cover security failures.") (quoting James Lewis, Director of the Center for Strategic and International Studies' Council on Technology and Public Policy) (last visited Nov. 24, 2003)*; see also* Robert Lemos & Declan McCullagh, *Cybersecurity Plan Lacks Muscle,* CNET News.com (Sept. 19, 2002), *at* http://news.com.com/2100-1023-958545.html?tag=rn ("'It has no teeth,' said Steven Kirschbaum, CEO of Secure Information Systems . . . . 'The first rule of . . . any security policy is you have to have enforcement. Without it, it's just a nice press release.'"). It is perhaps also worth noting that prior systems which depended on citizen participation to maintain internal order were predicated on obligatory, rather than voluntary, compliance. *See supra* Part II(B)(2).

b. Obligatory approach to citizen responsibility

This leaves the obligatory approach. An obligatory approach requires citizens to conduct themselves in certain ways or face sanctions;[514] the conduct required can take the form either of acting or not-acting.[515] An obligatory approach relies upon the law to establish the obligation to act or not to act,[516] which brings us to our second dichotomy. Such laws are of two types: "do" laws and "do not" laws.[517] "Do" laws impose an obligation to act and sanctions for a failure to discharge that obligation;[518] "do not" laws impose an obligation not to act and sanctions for committing the proscribed act.[519] The laws used to implement an obligatory approach can be civil or criminal in nature.[520] This discussion will assume that the laws that are used to impose an obligation to prevent cybercrimes impose criminal liability for failing to discharge that obligation.[521] It makes that assumption because criminal liability is generally more effective than civil liability in encouraging citizens to conform their conduct to a prescribed standard.[522] Use of that assumption is also predicated on adapting certain principles of criminal liability for this specific purpose.[523]

Before we can consider how principles of liability can be used for this purpose, we must resolve the second dichotomy. That is, we must decide whether the obligatory approach to achieving citizen participation in preventing cybercrime should be based on a strategy utilizing "do" laws or on one utilizing "do not" laws.

A strategy utilizing "do" laws would impose an obligation upon citizens to prevent cybercrime by taking measures to secure their computer systems and

---

[514] *See supra* notes 507-08 and accompanying text.

[515] *See, e.g.,* SCHAUER, *supra* note 87, at 7; Hart, *supra* note 261, at 28.

[516] *See, e.g.,* LAFAVE, *supra* note 254, § 6.2.

[517] *See id.* at 434-35 ("Most crimes are committed by affirmative action . . . . But there are . . . crimes which . . . may be committed . . . by failure to act under circumstances giving rise to a legal duty to act.").

[518] *See, e.g.,* RESTATEMENT (SECOND) OF TORTS §§ 314A, 322 (1965); MODEL PENAL CODE § 2.01(3) (1985).

[519] *See, e.g.,* RESTATEMENT (SECOND) OF TORTS § 21 (1965); MODEL PENAL CODE § 2.01(1) (1985).

[520] *See supra* notes 519-20 and accompanying text.

[521] *See infra* Part IV(B).

[522] *See, e.g.,* Geraldine Szott Moohr, *Federal Criminal Fraud and the Development of Intangible Property Rights in Information,* 2000 U. ILL. L. REV. 683, 730. Imposing duties supported by criminal liability can be an effective way to create a norm. *See, e.g.,* Lior Jacob Strahilevitz, *How Changes in Property Regimes Influence Social Norms: Commodifying California's Carpool Lanes,* 75 IND. L.J. 1231, 1278-79 (2000).

[523] *See infra* Part IV(B).

otherwise avoid online victimization.[524] A failure to discharge that obligation with the requisite degree of effectiveness would result in the imposition of a sanction, presumably a relatively minor one.[525] Seat belt laws provide a useful point of comparison: By 2002, forty-nine states and the District of Columbia had enacted such laws.[526] They require the occupants of a motor vehicle to use seat belts when the vehicle is in operation and impose sanctions, usually a fine, for failure to comply.[527] Seat belt laws impose a type of criminal liability, since the sanction is a fine levied by the state,[528] and they have proven effective in increasing seat belt use among American motorists.[529] One might conclude from this that a similar approach would prove effective in increasing American citizens' efforts to prevent cybercrime.

There are, however, important differences between the two types of security measures; these differences mean that the approach which encouraged seat belt use is unlikely to encourage cybercrime prevention. For one thing, federal law required that all vehicles manufactured after 1968 have seat belts, so when states began to require the use of seat belts, they were installed and readily available.[530] The duty imposed by the seat belt laws was consequently not an onerous one: to use a device that had already been provided and that required

---

[524] For individuals, an obligation of this type could include the following installing firewalls and other security measures on computers, installing, updating and using anti-virus software and keeping software updated. *See, e.g.,* Office of the President, *supra* note 488, at 39. For artificial entities, it could include the activities noted above and working to address insider threats and sharing information about known threats. *See id.* at 39-41. For individuals and artificial entities alike, the obligation could also include educating themselves about tactics such as "social engineering" and "phishing," since much cybercrime is the product of human, not machine, error. *See, e.g.,* Social Engineering Attacks via IRC and Instant Messaging, CERT Incident Note IN-2002-03 (Mar. 19, 2002), *at* http://www.cert.org/incident_notes/IN-2002-03.html; Jeordon Legon, *"'Phishing' Scams Reel in Your Identity,"* CNN.com (Jul. 22, 2003), *at* http://www.cnn.com/2003/TECH/internet/07/21/phishing.scam.

[525] The sanction would almost certainly be a fine, perhaps coupled with restrictions on computer use for intransigent violators. Laws of this type would presumably be structured to alleviate or eliminate liability for attacks that could not reasonably be prevented by the measures available to average citizens. *See infra* Part IV(B)(1).

[526] *See, e.g.,* David A. Mobley, *Revisiting Alabama's Seat Belt Defense: Is The Failure To Buckle Up A Defense In AEMLD Claims?,* 53 ALA. L. REV. 963, 969 n. 45 (2002).

[527] *See, e.g.,* CAL. VEHICLE CODE § 27315(d)-(i) (West 2000); MASS. GEN. LAWS ANN. ch. 90, § 13A (West 2000).

[528] *See, e.g.,* Lisa Ruddy, Note, *From Seat Belts To Handcuffs: May Police Arrest For Minor Traffic Violations?,* 10 AM. U. J. GENDER SOC. POL'Y & L. 479, 505-06 (2002).

[529] *See, e.g.,* Barry L. Huntington, Comment, *Welcome To The Mount Rushmore State! Keep Your Arms And Legs Inside The Vehicle At All Times And Buckle Up . . . Not For Safety, But To Protect Your Constitutional Rights,* 47 S.D. L. REV. 99, 104 (2002).

[530] *See, e.g.,* Mobley, *supra* note 527, at 996 (citing 23 C.F.R. § 255.21 (1968)).

no technical skill to implement. The duty imposed by the hypothesized cybercrime prevention laws is far more complex: Among other things, citizens would have to (a) identify and obtain the tools needed to protect their computers from cyber-attacks; (b) educate themselves about these tools so they could install them, utilize them and keep them updated; and (c) use these tools in an effective manner.[531] Since computer software and hardware is constantly being modified, tasks (a) and (b) would be ongoing obligations. One differentiating factor, therefore, is the relative complexity of the duty being imposed.

Another differentiating factor is the likelihood that law violators will be identified and sanctioned. Both the seat belt laws and the hypothesized cybercrime prevention laws establish a duty and impose sanctions in an effort to deter what society regards as "dangerous" behavior. The behavior to be deterred is, respectively, (a) not wearing seat belts and thereby exposing oneself to a risk of injury, and (b) not utilizing cybercrime preventative measures and thereby exposing oneself, others and the social system to cyber-attackers. The effectiveness of sanctions in deterring behavior is a function of the risk (perceived risk) of being apprehended and sanctioned; the deterrent effect thus increases as the risk (perceived risk) of being apprehended increases.[532] Seat belt laws apply to conduct that occurs in public; consequently, it is not particularly difficult for police officers to tell if someone is wearing a seat belt. Indeed, this is something they can observe in the course of carrying out their routine duties. This means the risk (perceived risk) of being apprehended is high; this, coupled with the ease with which one can conform one's conduct to the requirements of the law, makes seat belt laws an effective means of deterring the conduct noted above.

That would not be true of cybercrime prevention laws. They would for the most part address conduct occurring in very private places – one's home or office.[533] This means that absent some method of remote monitoring, which could raise Fourth Amendment issues,[534] it would be difficult for those charged with enforcing such laws to determine compliance. To do so, they would presumably have to conduct location-by-location checks, which would be extremely intrusive and labor-intensive. The consequent low risk (perceived risk) that violators would be identified and apprehended, coupled with the difficulty of complying, means that these hypothesized cybercrime prevention laws would not be an effective means of securing citizen collaboration in

[531] *See supra* note 525.

[532] *See, e.g.,* Linda S. Beres & Thomas D. Griffith, *Habitual Offender Statutes and Criminal Deterrence,* 34 CONN. L. REV. 55, 60-61 (2001).

[533] Since these laws would encompass preventative measures taken to secure laptops and other computers that could be used in "public" spaces, it is conceivable that an officer would observe a failure to implement such measures when a laptop was being used in public.

[534] *See, e.g.,* Kyllo v. United States, 533 U.S. 27, 35 (2001).

enhancing cybersecurity.[535]

This leaves the final strategy: the use of "do not" laws. "Do not" laws impose an obligation not to act and sanctions for committing the proscribed act.[536] They may seem a peculiar candidate for enlisting citizens in the fight against cybercrime, as they typically proscribe committing a "crime." Homicide laws ("do not take another person's life") and theft laws ("do not take another person's property") are examples of "do not" laws.[537] It would seem, therefore, that laws of this type would be quite inapplicable to the undertaking at hand. We are not, after all, talking about sanctioning citizens for committing cybercrime; we are talking about sanctioning citizens for not preventing cybercrime.

Actually, "do not" laws fit quite nicely into the calculus we are endeavoring to construct. One problem with using "do" laws to achieve the necessary behavioral change is that such an approach is fundamentally inconsistent with how we approach criminal liability. We do not, as was explained earlier, require citizens to prevent "crimes" in the real world; this means that an effort to impose a duty to prevent "crimes" in the cyberworld conflicts with norms and expectations that are firmly embedded in our culture, as least as to real world "crime."[538] Under the approach outlined earlier, we would impose a duty on citizens to take steps to prevent their being victimized by cybercriminals and impose sanctions if they failed to do so. This is inconsistent in two respects with the way we have traditionally approached criminal liability: (a) we would impose an unprecedented obligation to prevent "crime;" and (b) we would impose criminal liability for a failure to discharge that obligation *even though no "crime" has been committed.* We would, in effect, be imposing liability for a failure to prevent something that never happened. It is true that we impose criminal liability for "crimes" that are not committed, but we require that there have been some steps taken to accomplish a "crime" before such liability is imposed.[539]

---

[535] Yet another factor differentiating seat belt laws and the hypothesized cybercrime prevention statutes is that the former deal with hazards citizens understand and tend to appreciate, while the latter deal with dangers they generally under-estimate. *See supra* note 512 and accompanying text.

[536] *See supra* note 520 and accompanying text.

[537] *See, e.g.,* MODEL PENAL CODE §§ 210.1, 223.2 (1980).

[538] *See supra* Part IV(A)(1). Laws requiring the use of seat belts (and motorcycle helmets) are not concerned with preventing "crime," which is understood to be the province of the police. *See supra* Part IV(A). They are generally regarded as public health and safety measures. *See, e.g.,* Ilise Levy Feitshans, *Foreshadowing Future Changes: Implications Of The Aids Pandemic For International Law And Policy Of Public Health,* 15 MICH. J. INT'L LAW 807, 810 (1994).

[539] *See, e.g.,* MODEL PENAL CODE §§ 5.01-5.03 (1985) (defining attempt, conspiracy and solicitation).

The fact that the use of "do" laws to achieve citizen participation in the battle against cybercrime would violate traditional practice is important not because it goes against the way things have been done in the past. There is sometimes much to be said for changing how we approach things. The inconsistency with current and past practice is important because we are trying to use legal principles to establish a new pattern of behavior; if legal rules are inconsistent with traditional expectations and understandings, they are likely to meet with resistance.[540] The hypothesized "do" laws would probably be regarded as Draconian, intrusive and, given the public's current lack of awareness of the nature and extent of cybercrime threats, unnecessary.[541] If we are to succeed in using legal rules to un-do expectations about law enforcement's responsibility for dealing with "crime" and inculcate a sense of personal responsibility for preventing cybercrime, we need to use an approach that does less violence to societal expectations. As the next section explains, "do not" laws or, more properly, modified versions of traditional "do not" laws, can form the basis of such an approach.[542]

B. Distributed Security[543]

> *[A] centralized system is not going to work. We have got to think about distributed security.*[544]

As the previous section explained, criminal rules that take the form of "do not" laws can be used to inculcate a social climate in which citizens assume responsibility for preventing cybercrime without violating implicit social expectations as to the proper use and scope of criminal liability.[545] The sections below demonstrate how laws of this type can be used for that purpose; they examine two complementary possibilities.

The first is a specialized expansion of accomplice liability; it allows the imposition of criminal liability for conduct that promotes, facilitates or otherwise contributes to the successful commission of a cybercrime or an

---

[540] *See, e.g.,* BERGER & GREENBERG, *supra* note 283, at 14.

[541] Since "do" laws would be regarded as intrusive and unnecessary, norms of evasion analogous to those that emerged during alcohol Prohibition would likely appear. *See generally id*. Some individuals would decline to take the necessary security measures; others might use token compliance as an excuse, installing some minimal security measures and claiming they had satisfied their obligation. All of this would only make enforcement of the "do" laws that much more difficult, expensive and futile.

[542] *See infra* Part IV(B).

[543] For an explanation of this term, *see infra* Part V.

[544] *Cyber Security Hearing, supra* note 433, at 45, *available at* http://commdocs.house.gov/committees/science/hsy75565.000/hsy75565_0.HTM.

[545] *See supra* Part IV(A)(2)(b).

attempt to commit a cybercrime. This is essentially a "do not" law targeting affirmative conduct; it proscribes not the *failure to prevent* cybercrime but the act of *contributing to the commission* of a cybercrime. The distinction is important for two reasons: (1) it means criminal liability cannot be imposed unless and until a cybercrime has been committed; and (2) it means liability is imposed not for the act of becoming a victim (only) but for the consequential effect of contributing to another's victimization.[546] This alternative avoids the "overkill" problem discussed in the previous section: assessing criminal liability when no "crime" has been committed, solicited or attempted.[547] It is also consistent with traditional practice, and preserves the appearance of justice in predicating the imposition of liability upon the act of furthering a crime against someone else; imposing criminal liability for the act of becoming a victim is unlikely to be regarded as "fair" or "just."

The second alternative imports an attenuated version of tort law's assumption of risk principle into criminal law. The purpose here is to negate citizens' expectations that their victimization by cybercriminals will produce an effective reaction on the part of law enforcement officers. The attenuated assumption of risk principle is a way of emphasizing the need to protect oneself from the risks attendant upon venturing into cyberspace. This alternative does not impose criminal liability upon victims and it does not prevent the imposition of such liability upon their victimizers; it merely nullifies the contemporary commonsense default assumption of official reaction and redress. It operates as a correlate to the complicity principle: If Jane Doe ventures into cyberspace without taking necessary precautions and becomes a victim (only), she has no right to expect "justice" in the form of sanctions imposed upon her victimizer. If she ventures into cyberspace without taking necessary precautions, becomes a victim and, as a result of the carelessness that resulted in her victimization, contributes to another's victimization, then Jane Doe can be held criminally liable for facilitating the consequent cybercrime.

1. Complicity

As Part IV.A.1 explained, the goal of the alternatives discussed in this section and subsequent sections is to realign responsibility for preventing cybercrime by shifting it from the police (who prevent by reacting-apprehending-deterring offenders) to citizen users of technology. The goal is to impose criminal liability for failing to prevent personal victimization that

[546] *See infra* Part IV(B)(2)*; see generally* Scott C. Zimmerman et al., *Downstream Liability for Attack Relay and Amplification,* CERT (2002), *at* http://www.cert.org/archive/pdf/Downstream_Liability.pdf.

[547] *See supra* Part IV(A)(2)(b).

contributes to the commission of cybercrime against others.[548]

Complicity doctrines are an obvious choice for such an undertaking because they impute liability for another's criminal act to a non-actor (an accomplice) who facilitated the criminal act.[549] An accomplice who facilitates the commission of a "crime" can be held criminally liable for that "crime," just as if he actually committed it.[550] Accomplice liability is usually based on the accomplice performing an affirmative act, such as giving a weapon to a would-be robber. It can also be based on a failure to act: under the Model Penal Code, one is an accomplice if "having a legal duty to prevent the commission of the offense, [she] fails to make proper effort so to do."[551] This doctrine of complicity-by-omission has been used, for example, to hold parents liable for failing to prevent harm to their children.[552] For the doctrine to apply, the putative accomplice must have had a legal duty to prevent the commission of the "crime;" a moral duty is not enough.[553] Most criminal codes require that an accomplice have acted "with the purpose of . . . facilitating the commission of the" target crime."[554] There is some authority for the proposition that accomplice liability can be imposed on those who knowingly facilitates the commission of a "crime;"[555] and a general agreement that it cannot be predicated on reckless or negligent conduct.[556] Other codes are more lenient. The statute governing the proceedings of the International Criminal Tribunal for the Former Yugoslavia, for example, imposes complicity-by-omission liability upon commanders who recklessly or negligently failed to prevent their subordinates from committing war crimes.[557] This result is, as one author

---

[548] *See id*.

[549] *See, e.g.,* MODEL PENAL CODE § 2.06 (1985) (one is guilty as an accomplice if he, *inter alia*, promotes or facilitates the commission of an offense).

[550] *See, e.g.,* MODEL PENAL CODE § 2.06(1) (1985).

[551] *See, e.g.,* MODEL PENAL CODE § 2.06(3)(a)(iii) (1985)*; see also* LAFAVE, *supra* note 254, at 341-42 ("Thus, a conductor on a train might become an accomplice in the knowing transportation of liquor on his train for his failure to take steps to prevent the offense.").

[552] *See, e.g.,* State v. Tucker, 861 P.2d 37, 43-44 (Haw. App. 1993).

[553] *See* MODEL PENAL CODE § 2.06 cmt. at 320, n.63 (1985)*; see, e.g.,* Knox v. Commonwealth, 735 S.W.2d 711, 711-12 (Ky. 1987).

[554] *See, e.g.,* MODEL PENAL CODE § 2.06(3)(a) (1985).

[555] *See, e.g.,* LAFAVE, *supra* note 254, § 13.2(d) (citing Backun v. United States, 112 F.2d 635 (4th Cir. 1940)). *Cf.* United States v. Peoni, 100 F.2d 401, 402-03 (2d Cir. 1938).

[556] *See, e.g.,* LAFAVE, *supra* note 254, § 13.2(e). Some argue that reckless conduct should support the imposition of accomplice liability, at least for crimes in which the requisite mental state is recklessness. *See also* Sanford H. Kadish, *Reckless Complicity,* 87 J. CRIM. L. & CRIMINOLOGY 369, 373, 381 (1997). For the proposition that such liability is absent from the criminal codes of other nations as well, *see, e.g.,,* Mirjan Damaska, *The Shadow Side of Command Responsibility,* 49 AM. J. COMP. L. 455, 464-67 (2001).

[557] *See, e.g.,* Damaska, *supra* note 556, at 463*; see also* International Criminal Tribunal

noted, "troubling to national [legal] systems because they all subscribe to the general principle that people should be held accountable according to their own actions and their own mode of culpability."[558]

The insistence on "intention" (i.e., purpose and, perhaps, knowledge) found in the Model Penal Code and in domestic criminal codes is the product of two considerations. One is a concern that "otherwise everyday lawful activities would be made perilous;"[559] if simple negligence sufficed for act-of-commission complicity, selling lawful products could result in the imposition of criminal liability if the products were used to commit "crimes." The other consideration is "the belief that people's freedom to act within the law should not be restrained by considerations of wrongs others might commit;"[560] in other words, I should not be held liable for the intervening volitional act of one over whom I exercise no command or control. This is what differentiates the "command complicity" found in the statute governing the International Criminal Tribunal for the Former Yugoslavia from the codes that govern average citizens; civilians, unlike military commanders, generally do not have the authority to control the actions of others.[561]

At first glance, it might seem that complicity-by-omission liability for one's failure to prevent consequent victimization[562] is quite an unacceptable prospect because it violates certain basic tenets of accomplice liability: It imposes omission liability in the absence of a legal duty to act, and it contravenes the two considerations noted above. In fact, with some modifications, complicity-by-omission liability can be used for this purpose.

The first and most problematic hurdle is the conduct upon which liability is to be predicated. If we use the Model Penal Code's formulation of complicity, an omission cannot support the imposition of accomplice liability unless a duty to act is imposed by law.[563] One solution to the difficulty noted above is, therefore, to establish a legal duty to prevent oneself from becoming the victim of a cybercriminal.[564] In establishing such a duty, we must resolve two issues:

---

for the Former Yugoslavia, Amended Statute art. 7 ¶ 3 (1993), *available at* http://www.un.org/icty/legaldoc/index.htm.

[558] Damaska, *supra* note 556, at 464*; see also* Kadish, *supra* note 556, at 372.

[559] Kadish, *supra* note 556, at 382.

[560] *Id.* at 391. *See also supra* note 556 and accompanying text.

[561] *See generally* Damaska, *supra* note 556, at 463-64.

[562] "Consequent victimization" is personal victimization that contributes to the commission of cybercrimes against others. *See supra* Part IV(B).

[563] *See supra* note 553 and accompanying text. Absent a legal duty there is, of course, no obligation to prevent a "crime." *See supra* Part IV(A)(1).

[564] Since such a duty did not exist at common law, it would have to be statutorily imposed. This could be done *seriatim,* by having states adopt laws to this effect. Alternatively, it might be possible to enact such a duty at the federal level, given the deleterious effects cybercrime and cyberterrorism have upon interstate commerce. *See*

(1) the scope of the duty; and (2) the extent of the obligation one bears in discharging it. As to the first issue, it is sufficient and reasonable to limit the duty to preventing one's personal victimization; allowing myself to be attacked is, after all, how I contribute to the victimization of others.[565] This limited duty is sufficient because if I protect my computer from attack, I thereby prevent its being used to attack others. Conversely, if I do not protect my computer from attack, I have created at least the possibility that it can be used to attack others. Making this limited duty the predicate for accomplice liability is reasonable because by failing to secure my computer I have created the conditions a cybercriminal can exploit to victimize others.[566] If a cybercriminal takes advantage of the opportunity I have supplied, it is reasonable to hold me liable, at least to some extent, for the resulting cybercrimes.[567] As to the second issue, the duty would have to specify the extent of the obligation one bears to avoid being victimized. It could impose strict liability, which would make one categorically liable for consequent victimization; but the more reasonable approach is to incorporate a negligence standard. Strict liability would undermine the incentive to take precautions, since one would be held liable for consequent victimization regardless of the efforts he took to avoid being personally victimized.[568] Under a negligence standard, liability would be imposed for a failure to take all precautions a reasonable person should have known were necessary to protect the system(s) at issue.[569] The determination as to whether particular measures were necessary would have to include a temporal element; that is, it would have to focus on contemporaneously available security measures.[570]

---

generally Joseph P. Bauer, *The Erie Doctrine Revisited: How A Conflicts Perspective Can Aid the Analysis,* 74 NOTRE DAME L. REV. 1235, 1243 n. 34 (1999).

Another possibility, using the Model Penal Code's approach to complicity, would be to declare that the failure to prevent a cybercrime which results in the victimization of others is itself enough to establish complicity. *See* MODEL PENAL CODE § 2.06(3)(b) (1985) (one is an accomplice if "his conduct is expressly declared by law to establish his complicity.").

[565] It is also possible that I can be victimized as the result of my own gullibility, i.e., as the result of succumbing to "social engineering" and other tactics. *See infra* note 580.

[566] *See supra* Part IV(A)(1).

[567] The precise nature and extent of the liability to be imposed is discussed below. *See infra* notes 585-92 and accompanying text.

[568] *See, e.g.,* LAFAVE, *supra* note 265, § 5.5(c).

[569] *See* MODEL PENAL CODE § 2.02(2)(d) (1985). A negligence standard would also encompass reckless, knowing and purposeful failures to carry out the duty to prevent personal victimization. *See id.* § 2.02(5). Purposeful and knowing conduct is also discussed below. *See infra* note 594 and accompanying text.

[570] It might also be advisable to incorporate the type of user into the standard so that, for instance, corporate entities are held to a higher level than individual, home users of computer technology.

The imposition of such a duty is, in a sense, implementing a "do" rule under the scheme outlined earlier;[571] it imposes an affirmative obligation to institute and maintain security measures that are designed to fend off attacks by cybercriminals.[572] This duty differs from the implementation of a "do" rule, however, in that criminal liability is not imposed for the mere failure to discharge the duty:[573] If someone becomes the victim of a cybercrime, she will not be held liable as an accomplice to her own victimization.[574] The sanction for her default in carrying out the duty to prevent cybercrime is that she will be deemed to have assumed the risk of her own victimization.[575] Criminal liability – in the form of complicity – is imposed only if she fails to discharge her duty to prevent herself from becoming the victim of a cybercrime and thereby contributes to the victimization of another or others. This result is consistent with traditional principles of criminal liability because she is being sanctioned for playing a causal role in the commission of a "crime" against someone else.[576]

That brings us to the second hurdle: the considerations which have heretofore dictated that accomplice liability must be based on "intentional" (purposeful or knowing) conduct.[577] We address the second consideration, as it is the more challenging of the two. The second consideration dictates that we require purpose or at least knowledge for the imposition of accomplice liability because doing otherwise runs the risk of holding citizens liable for the intervening volitional act of one over whom they exercise neither command nor control.[578] This may seem a fatal objection to the type of accomplice liability postulated here: The scenario encompassed by this type of liability involves a cybercriminal (X) who victimizes A and then uses his victimization of A to consummate his victimization of B (and C and D and so on).[579] It seems inconceivable that we should hold A liable for this anonymous cyber-miscreant's successful attacks on B (and C and D . . .).[580] If we assume the

[571] *See supra* Part IV(A)(2)(b).

[572] *See id*.

[573] Practical problems entailed by enforcing criminal liability for the failure to prevent cybercrime are the primary objection to relying on "do" rules. *See id*.

[574] *See* MODEL PENAL CODE § 2.06(6)(a) (1985) (victim is generally not an accomplice).

[575] *See infra* Part IV(B)(2).

[576] *See supra* Part IV(A)(2)(b).

[577] *See supra* notes 559 and accompanying text.

[578] *See supra* notes 559-61 and accompanying text.

[579] The scenarios discussed above assume that X uses A's computer as the vector from which to launch attacks on others; it is also possible that A contributes to the victimization of others by falling prey to "social engineering" and comparable tactics. *See supra* note 525.

[580] If we require that A have acted with the purpose of facilitating X's attacks or that he knew his default would facilitate X's attacks, we establish a connection between the two that makes it reasonable to impute liability for X's actions to A. *See supra* note 560 and

most difficult scenario,[581] in which A does not know X, has no control over X's actions and was merely negligent in not preventing X's gaining access to his computer, it seems we are holding A liable for nothing more than failing to prevent a stranger of whose identity and activities he is ignorant and over whom he exercises no control from attacking other strangers.

This may, at first glance, seem as unreasonable as holding a liquor store clerk liable as an accomplice if a customer to whom she sold a bottle of whiskey uses it to (a) incapacitate a young woman whom he rapes or (b) enter a state of gross intoxication in which he batters his wife to death.[582] But there are important differences between the two: In the second scenario, the clerk is being held liable for the purely volitional and consequently quite unforeseeable "bad acts" of another human being, one whose predilections are entirely unknown to her. The clerk has no capacity to control what the purchaser does after he leaves the store. In the first scenario, A is being held liable not for failing to control X (which is impossible given that A does not know X and has no authority to control X's actions) but for failing to prevent equipment and processes that are within A's control from being attacked and compromised to the detriment of others.[583] We cannot hold A liable for what X does on the theory that A should have prevented X from attacking others; but we can hold A liable for giving X access to the tools he needs to victimize others by defaulting on his obligation to prevent his computer system from being compromised.[584] The latter theory is consistent with traditional accomplice

accompanying text.

[581] Other scenarios would involve instances in which A knew that he might be subject to an attack from X or in which A exercised some control over X, perhaps as X's employer, whom he know to have a predilection for cyber-misconduct.

[582] Civil liability can be imposed for selling statutorily-controlled products, such as weapons and ammunition, to minors. *See,* Robert M. Howard, Note, *The Negligent Commercial Transaction Tort: Imposing Common Law Liability On Merchants For Sales And Leases To 'Defective' Customers,* 1988 DUKE L.J. 755, 758. The only avenue for imposing criminal liability is complicity which, as noted above, is not available unless the clerk acted with the purpose of aiding the commission of the customer's subsequent "crimes" or with the knowledge that she was doing so.

[583] As to the standard A must meet, *see supra* notes 569-71 and accompanying text.

[584] An imperfect source of analogy, perhaps, are the laws that impose liability upon a parent for the parent's failure to prevent a child from obtaining access to a weapon and using it to commit a "crime." In State v. Wilchinski, 700 A.2d 1 (Conn. 1997), for example, a father was charged with criminally negligent storage of a firearm after his son found his handgun and used it to kill another child. *See id.* at 4*; see also* CONN. GEN. STAT. ANN. § 53a-217a(a) (West 2003) ("A person is guilty of criminally negligent storage of a firearm when he violates the provisions of section 29-37i and a minor obtains the firearm and causes the injury or death of himself or any other person."). The father claimed that the criminally negligent storage statute impermissibly held gun owners liable "for the acts of another without requiring the state to prove that the owner was an accessory" under the state's

liability in that A is held liable for contributing to the success of the criminal venture.

Some may still find this outcome unpalatable, since it would result in A's being held liable for the cybercrimes X committed against B (and C and D . . .).[585] This is an undeniably harsh result, which is no doubt why criminal law has historically insisted upon purposive (or at least knowing) conduct as the basis for imposing accomplice liability. The harshness of this result can be alleviated by implementing yet another modification. Instead of holding A liable as an accomplice to X's cybercrimes, A can be held liable as a criminal facilitator of those crimes. New York and several other states have a separate "criminal facilitation" offense; under these statutes, one who provides another with the means and/or opportunity to commit a "crime" can be held liable as a facilitator of that "crime."[586]

The difference between criminal facilitation and accomplice liability is that the facilitator is not held liable for the "crimes" she promoted; she is instead held liable for criminal facilitation, which can be a relatively minor offense.[587] New York, for example, divides criminal facilitation into four degrees: criminal facilitation in the first degree (a class B felony);[588] criminal facilitation in the second degree (a class C felony); [589] criminal facilitation in the third degree (a class E felony);[590] and criminal facilitation in the fourth degree (a class A misdemeanor).[591] Criminal facilitation liability, or an analogue thereof, could be used to impose criminal liability upon those who default on their duty to avoid becoming a cybercriminal's victim and thereby facilitate their victimization, without the harsh results entailed by employing accomplice liability. The sanctions for this kind of criminal facilitation of cybercrime[592] should probably be a fine or perhaps a fine coupled with another

complicity statute, which predicates accomplice liability only upon affirmative acts taken to facilitate the commission of a "crime." *See Wilchinski*, 700 A.2d at 12. The Connecticut Supreme Court disagreed: "Although criminal liability under § 53a-217a does not attach . . . until a minor injures or kills himself or another person, the offense . . . is not the resulting injury or death but, rather, is the improper storage of the weapon that led to the tragedy." *Id.*

[585] *See* MODEL PENAL CODE § 2.06(1) (1985).

[586] *See, e.g.,* LAFAVE, *supra* note 254, § 13.2(d).

[587] *See, e.g., id*.

[588] *See* N.Y. PENAL LAW § 115.08 (2003).

[589] *See* N.Y. PENAL LAW § 115.05 (2003).

[590] *See* N.Y. PENAL LAW § 115.01 (2003).

[591] *See* N.Y. PENAL LAW § 115.00 (2003). For the distinctions responsible for the different offense see, for example., Stephen Cordovani et al., Annotation, *Statutory Classification and Designation; Degrees of Offense*, 35 N.Y. JUR. 2D CRIMINAL LAW § 3652 (West 2003).

[592] Since some codes use criminal facilitation to reach complicitous conduct that is predicated on knowledge, but not purpose, other, more serious types of activity could

minor sanction, such as a restriction of access to computers or the requirement that an offender take a course in cyber-security.[593] True accomplice liability could be reserved for those who purposefully or knowingly contribute to the commission of cybercrimes against others, and would permit the imposition of more severe sanctions, such as incarceration.[594]

2. Assumption of Risk[595]

Criminal law does not require a blameless victim,[596] but should things be different in cyberspace? Should "assumption of risk" be incorporated into the criminal law that governs cyberspace? Why would we consider doing such a thing? How would such an option fit into the present discussion? Assumption of risk, after all, is a doctrine that bars victims from obtaining redress – it negates liability, it does not impose it.

"Assumption of risk" could not be incorporated into criminal law as it is applied in tort law. In tort, if one is found to have assumed the risk of harm that caused her injury, she is barred from obtaining redress for the injury.[597] If we were to import this notion whole into the criminal law, the consequence would be that those who assumed the risk of their victimization would be denied justice. The effect would be to give cybercriminals a "Get out of jail free card" for victims who did not or could not protect themselves. This result is unacceptable. One of the purposes of the criminal law is to maintain order by protecting members of society, including the young, the disadvantaged and the elderly.

But what about incorporating the concept, not the tort rule? That is, what about incorporating an assumption of risk principle that does not absolve the perpetrator of liability for his or her crimes, but that can be used to underscore the fact that there may well be no official redress for "harms" inflicted in cyberspace?

There is no guarantee of redress for real world "crime". Prosecutors have always had the discretion to decline prosecuting offenses that are brought to

provide the basis for a criminal facilitation of cybercrime charge. *See, e.g.,* LAFAVE, *supra* note 254, § 13.2(d).

[593] *See generally* United States v. Ristine, 335 F.3d 692 (8th Cir. 2003) (sentence included restrictions on use of computer and access to Internet). New York's criminal facilitation offenses are not sources of guidance on this issue because they require "intentional" conduct. *See supra* notes 589-91.

[594] *See, e.g.,* MALAYSIA COMPUTER CRIMES ACT 1997 § 7(1) ("abetments . . . punishable as offenses"), *available at* http://www.geocities.com/Tokyo/9239/comcrime.html.

[595] A more detailed treatment of this alternative can be found in *A New Model of Law Enforcement, supra* note 11.

[596] *See supra* Part IV(A)(1).

[597] *See, e.g.,* RESTATEMENT (SECOND) OF TORTS §§ 496B-C (1965).

their attention.[598] Real world "crimes" and cybercrimes differ, however, as to the factors that result in a lack of prosecution. Declination decisions for real world "crimes" are based on specific factors, such as a prosecutor's doubt that an accused is guilty, an accused's cooperation in apprehending others, the extent of the harm caused by the offense, and the likelihood of prosecution in another jurisdiction. In these instances, prosecution is declined because a prosecutor has determined that it would be unjust or unnecessary. The declination decision thus represents a considered decision not to prosecute when prosecution is a viable option. Conversely, prosecution is often not an option for cybercrimes because of the difficulties involved in apprehending cybercriminals.[599] This is the critical difference between real world "crimes" and cybercrimes: Declination decisions are a sign that the justice system is functioning effectively as to real world "crimes;" having the ability to prosecute, the system chooses not to. The justice system's inability to prosecute cybercrimes, on the other hand, indicates that it is not functioning effectively in this area. Since this state of affairs will continue, if not worsen, we need to ensure citizens realize that when they venture into cyberspace, they enter an insecure environment in which the implicit guarantees of redress applicable to the real world no longer apply. They must therefore become the guarantors of their own safety online.

An attenuated assumption of risk principle could be used to accomplish this goal. Such a principle would include two components: (1) a proposition negating the current default expectation of an effective law enforcement reaction to victimization; and (2) a declaration that the negation of such a generalized expectation does not prevent the investigation and prosecution of cybercriminals. It might look something like this:

> 1. One who [understanding the risk of harm to self or property] accesses or employs cyberspace to engage in commercial or other activity without having taken all reasonable, available measures to protect herself and her property from being victimized by online criminal actors during the course of and with regard to any matters related to such activity, shall be deemed to have assumed the risk of that victimization. Such a victim should report the offense(s) to the appropriate law enforcement agency. The filing of such a report in no way obligates the agency to investigate or otherwise pursue the matter; domestic law enforcement agencies have full discretion to determine what, if any, action will be taken as the result of their receiving such a report. Law enforcement agencies are under no obligation to take action with regard to offenses targeting those who assumed the risk of becoming a victim online, though they may do so.

---

[598] *See, e.g.,* Chris Zimmerman, *Prosecutorial Discretion,* 89 GEO. L.J. 1229, 1229 (2001).

[599] *See supra* Part III.

> 2. The fact that a person or entity assumed the risk of being victimized pursuant to paragraph (1) above creates no enforceable rights in the party or parties who are in any way responsible for that victimization. The principles set forth in paragraph (1) above cannot be used as an affirmative defense in a prosecution for offenses committed against one who assumed the risk of being so victimized and they in no way restrain law enforcement's ability to initiate the investigation and prosecution of those responsible for such offenses.

The bracketed language in the first paragraph creates the option of structuring the principle so that one must understand the risk he/she assumes; this is a traditional component of the tort law principle.[600] If this criminal law principle is to achieve the desired result, however, it must impose strict liability. The assumption of risk must arise from the act of venturing into cyberspace without having taken adequate precautions; knowledge of the risk being assumed should not be required because the purpose is to encourage citizens to learn about risks and take steps to avoid them. Incorporating knowledge of the risk nullifies the efficacy of the principle without increasing the fairness of the result. The tort principle incorporates knowledge of the risk assumed because the consequence of assuming a civilly-defined risk is that the victim loses the right to seek redress for resulting injuries; requiring notice is therefore simply a matter of fairness.[601] In the criminal context, the victim loses, at most, the expectation of a law enforcement response to her victimization; since this expectation may be quite unrealistic, the victim actually "loses" nothing. The assumption of a criminally-defined risk does not bar the victim from seeking damages in a civil action brought against an appropriate party, nor does it preclude the apprehension and prosecution of the victimizer. It merely negates the supposition that one's victimization triggers an entitlement to a law enforcement response that is instantaneous and efficacious.

This is where assumption of risk fits into the model being explored in this article. As explained earlier, the goal is to recruit citizens into the battle against cybercrime by encouraging them to take all necessary and available steps to prevent their being the target of a cybercriminal. The complicity principle discussed in the previous section does this by imposing a different kind of assumption of risk – the risk of criminal liability for facilitating a cybercrime.[602] This type of liability will be reserved for egregious cases; it is neither reasonable nor possible to impose accomplice liability upon everyone whose negligence somehow promotes the commission of a cybercrime.[603] The

---

[600] *See, e.g.,* RESTATEMENT (SECOND) OF TORTS § 496C(1) (1965).

[601] *See, e.g.,* RESTATEMENT (SECOND) OF TORTS § 496D, cmt. b (1965).

[602] *See supra* Part IV(B)(1).

[603] *See id.*

assumption of risk principle, however, applies automatically to anyone who becomes the victim of a cybercriminal. It requires no law enforcement effort to implement, nor does it affirmatively impose liability upon victims; but it can serve to underscore the risks attendant upon venturing into cyberspace without taking the necessary precautions.

The goal is to make it clear to citizens that their victimization will be, at most, a low priority for law enforcement. This merely reflects what is already occurring: Police cannot, for example, seek justice for everyone who foolishly sent someone, somewhere, $45 for a Beanie Baby that was advertised on eBay but was never delivered (and probably never existed).[604] Police and prosecutors know that cases like this stand no chance of being prosecuted, but they have no viable way to communicate this to the public. In a system that assumes the effectiveness of the traditional, reactive model of law enforcement, it would not be a wise career move for a county prosecutor to inform his constituents that if they are victimized in certain ways while online, his office will not pursue those cases. An attenuated assumption of risk principle such as the one set out above could be used to make the public understand the risks they face online and their evolving responsibility to prevent their victimization.

V. CONCLUSION

"public power into private hands . . . ."[605]

The premise driving the alternatives presented in Part IV.B is that the only way to effectively address cyber-threats is through a system of distributed security. This system of distributed security supplements the traditional reactive approach to criminal activity, at least as to cybercrime.[606] The goal of a system of distributed security is to adopt or modify rules so as to create incentives for users of computer technology to ensure a baseline, minimal level of safety as to the technologies they use. It is a "bottom-up," rather than a "top-down," approach to cybersecurity;[607] it uses lateral rules that specify

---

[604] CANTOR, *supra* note 229, at 200*; see also id.*; *see, e.g.,* Stefani Eads & Paul M. Eng, *Bidding in an Online Auction? Beware of Scams,* BUSINESS WEEK ONLINE, Nov. 3, 1998, at http://www.businessweek.com/bwdaily/dnflash/oct1998/sr81103b.htm (woman paid $1,800 for a fake Beanie Baby).

[605] Norman F. Cantor, The Civilization of the Middle Ages 200 (1994).

[606] As noted earlier, it is still necessary to retain a reactive apparatus to deal with real world "crime," which continues to be territorially based. *See supra* note 455 and accompanying text. A reactive apparatus is also necessary to apprehend perpetrators of cybercrime whenever they are successfully identified.

[607] *See generally* Drew Clark, *House Passes Law Enforcement Information-Sharing Bill,* GovExec.com (Jun. 26, 2002), *at* http://www.govexec.com/dailyfed/0602/062602td2.htm.

options and consequences to encourage the development of new behaviors among the general populace.

Distributed security is a necessary consequence of the continuing evolution and proliferation of technology. The traditional model of law enforcement is the product of an era when nation-states ruled supreme; nation-states are defined by and primarily operate within specific territorial boundaries. Nation-states maintain internal order by implementing the constitutive and proscriptive rules discussed earlier;[608] they maintain external order by protecting their citizens from "outside" threats, which have historically been encroachments by other nation-states.[609] The primary challenges nation-states have heretofore faced are, therefore, internal "crime" and external warfare; nation-states deal with both challenges by monopolizing power, or force. Internally, nation-states set up hierarchical organizations ("police") to which they delegate a measure of authority and the ability to use force against citizens who threaten internal order by committing "crimes" within the nation-state's physical boundaries. These organizations maintain internal order by reacting to threatened and completed "crimes."[610] The reaction is assumed to maintain order by (a) removing the authors of disorder (actual or attempted); and (b) using their removal to deter them and others from engaging in similar activity.[611] This system works reasonably well as long as "crime" is domestic "crime;" once "crime" begins to bleed across territorial boundaries, the effectiveness of this approach begins to erode.[612]

Cyberspace transcends territorial boundaries and consequently erodes the basic assumption animating this model of law enforcement, namely, that policing organizations can exert a sufficient measure of control over deviant behaviors within a nation-state's populace to maintain internal order.[613] Cyberspace lets external actors threaten internal order by committing "crimes"

---

[608] *See supra* Part II(A).

[609] *See generally id*.

[610] *See supra* Part II(B)(2). To maintain external order, nation-states create analogous organizations ("military") and assign them the task of resisting threats from "outside" the system, i.e., threats emanating from outside the nation-state's territorial boundaries. Until recently, the external threats nation-states faced were each other (war); that has changed with the permeability of cyberspace. Nation-states now find themselves confronting an additional type of external threat: the non-state actor. Either type of external threat – the alien nation-state threat and the non-state actor threat – can be delivered via cyberspace. The distributed security approach proposed above as a means for dealing with threats to internal order ("crimes") can also help nation-states to resist these new external threats.

[611] *See id*. Removing offenders also contributes to the maintenance of internal order by incapacitating them from committing further offenses.

[612] *See supra* Part III.

[613] *See id.; see also supra* Part II.A.

against the members of a nation-state's populace;[614] it also lets internal actors evade or overwhelm the efforts of traditional policing organizations.[615] Both trends are already apparent; the effects of both will become more pronounced as technology continues to evolve. It therefore becomes necessary to move from the old state-monopolized-reactive model to a new model, at least as to technologically-facilitated crime.[616] This requires a shift in emphasis – from deterrence to prevention. It also requires distributing a substantial part of the responsibility for prevention among the members of a nation-state.[617] It requires, in effect, shifting from a model of security analogous to the Maginot Line strategy that proved so disastrous for the French in World War II[618] to a model in which the obligation to resist and avoid cyber-threats is pervasive throughout a society.[619]

Shifting to this new model requires altering the focus of criminal law with regard to conduct involving the use of computer technology. Traditionally, criminal law has focused on perpetrators only. It has operated on the premise that targeting perpetrators for retribution, deterrence, incapacitation, and, at some moments in history, rehabilitation is an effective way of maintaining internal order in a society. This premise gave rise to the traditional, reactive model of law enforcement that has proved sufficient, or at least has been perceived as sufficient, for dealing with real world "crime."

The concept of a criminal law for cyberspace proposed in this article focuses both on the advertent perpetrators of cybercrimes and on citizens who inadvertently but nevertheless contribute to the commission of online "crimes."[620] The perpetrator rules remain essentially the same (so far, anyway). The citizen rules focus on the victims of cybercrimes, dividing them into two categories: "mere" victims and victim-facilitators. Both, in a sense, assume the consequences attendant on their victimization: "mere" victims

---

[614] *See supra* Part III.

[615] *See id.*

[616] *See supra* Part IV(A).

[617] *See generally* Office of the President, *supra* note 488, at 57-58.

[618] *See, e.g., Cyber Security Hearing, supra* note 433, at 48-49 (Statement of Dr. William A. Wulf, President, National Academy of Engineering).

> [T]he basic model . . . is flawed. I call it the maginot line model. It is a perimeter defense model . . . . It is a notion that there is bad stuff out there and good stuff in here and we want to protect what is in here against the bad guys out there. That model doesn't work.

Id. at 44. *See generally* VIVIAN ROWE, THE GREAT WALL OF FRANCE: THE TRIUMPH OF THE MAGINOT LINE (1961).

[619] *See, e.g., Cyber Security Hearing, supra* note 433, at 52 (Statement of Dr. William A. Wulf, President, National Academy of Engineering) (noting that "[m]uch better models: are available, "especially models like the immune system response that distribute the responsibility for protection and defense rather than concentrating it at the Maginot Line.").

[620] *See supra* Part IV(B).

assume the "harm" resulting from their victimization, as they have no cognizable expectation that the social system will seek redress for that "harm;" victim-facilitators assume the risks both of the "harm" resulting from their personal victimization and of criminal liability for facilitating consequent victimization resulting from their failure to protect themselves from cyberattacks.

This new model does not shift the obligation to prevent cybercrime entirely to citizens. The public sector – the nation-state – still has a role in this model of online law enforcement. Its obligation is to:

- monitor cyberspace in an effort to identify cybercrime patterns;[621]

- impose liability on cybercrime perpetrators and facilitators;[622]

- pursue cybercriminals to the extent possible, prioritizing the pursuit by (a) the systemic harm inflicted or threatened by specific cybercrimes; (b) the scale of cybercrimes committed by particular perpetrators;[623] (c) attacks on those who did not assume the risk of being victimized;[624] and (d) attacks on those who did assume the risk of being victimized;[625]

- develop and encourage the development of increasingly sophisticated security measures;[626] and

- promote the distribution of security measures and citizen training in their implementation.[627]

In discharging their obligation to avoid becoming the victims of cybercrime, individuals may find it advantageous to affiliate with commercial or non-commercial entities as a way of ensuring the security of their online activities.

---

[621] *See supra* Part III(D).

[622] *See supra* Part IV(B)(2).

[623] "Scale" would presumably be defined in terms of the number of victims, the cumulative extent of the loss attributable to a series of cybercrimes and/or the geographical scale of victimization.

[624] As noted earlier, the obligation placed on citizens to avoid becoming victims of cybercrime would not impose strict liability; it would require that they take all reasonable, state-of-the-art measures to avoid being victimized. *See supra* Part IV(B)(2). It follows that those who have taken such measures will still be victimized, since average citizens cannot be expected to defeat emerging tactics utilized by ambitious, technologically-adept cybercriminals. One of the virtues of implementing the assumption of risk doctrines set out in Part IV.B.2 is that they in effect create a triage system; that is, the state can focus its efforts on reacting to and otherwise dealing with cybercrimes committed against those who did not assume the risk of their commission, since these clearly represent the most dangerous threats to a social system. *See id.*

[625] *See generally* Office of the President, *supra* note 488, at 57-58.

[626] *See id.*

[627] *See id.*

One can see cyberspace, at least for the foreseeable future, as analogous to the world of the early Middle Ages: a world in which there were no nation-states to establish order over segments of territory and therein create a generally secure environment. Medieval citizens coped with this lack of internal order by grouping together in towns, cities and fortresses for security.[628] Something similar may evolve online; individuals and their families could use secure portals provided by collective entities as their gateways to cyberspace.[629] The collective entities would assume the obligation of ensuring users the level of security necessary to prevent their being victimized online (which would negate both victim assumption of risk and victim-facilitator liability).[630] Employees might, for instance, use a corporate employer's system as their individual (and family) portal to cyberspace; the benefit for the employees would be that they could use the corporate entity's presumably superior security systems instead of trying to protect themselves severally. This could perhaps become a benefit of employment, available either gratis or for a relatively modest fee.[631] Similarly, access via secure portals could be offered by government entities, educational institutions, commercial services and religious or other groups. A potential downside of this alternative is that these portals could provide tempting targets for cybercriminals – a readily identifiable collection of potential victims. This should not, however, prove to be a major problem: The portals would offer sophisticated technical security measures that should protect their users from cyber-attacks; they could also provide educational and informational programs to help their users avoid becoming the victims of online scams and other lapses in judgment.[632]

It is, of course, a perilous undertaking to speculate as to how human collectivities will organize themselves in the future. From the vantage point of the early twenty-first century, it seems clear that a system of distributed security is a superior way to address cyber-threats. Indeed, as technology continues its advance, we may conclude, as one expert noted, that "the

---

[628] *See, e.g.,* CANTOR, *supra* note 229, at 185-204.

[629] *See generally Highly Secure Web Based Collaboration Portal Used to Coordinate TOPOFF 2, The National Terrorism Response Exercise in Seattle, Chicago and Washington,* ITSecurity.com (May 22, 2003), *at* http://www.itsecurity.com/tecsnews/may2003/may216.html.

[630] At a minimum, the portals would only have to offer the reasonable level of security needed to protect users from victim assumption of risk and victim-facilitator liability. *See supra* Part IV.B.2. Portals could certainly offer higher levels of security and, indeed, might find financial incentives to do so. Subscription portals could develop which offered superior levels of online security for subscription fees.

[631] The benefit for the employer could be protecting its employees from personal victimization and personal criminal liability. Maybe also minimize the risk that the employee's (or family's) victimization could implicate the employer?

[632] *See supra* note 525.

monopolization of policing by government is an aberration."[633]

[633] DAVID H. BAYLEY & CLIFFORD D. SHEARING, U.S. DEP'T OF JUSTICE, THE NEW STRUCTURE OF POLICING: DESCRIPTION, CONCEPTUALIZATION, AND RESEARCH AGENDA 1 (2001), *available at* http://www.ncjrs.org/pdffiles1/nij/187083.pdf.