NANOCRIME?

Susan W. Brenner†

TABLE OF CONTENTS

Abstract

This article analyzes the use of nanotechnology to commit crimes. A great deal has been written about the societal implications of nanotechnology, and what has been often notes that criminals will exploit the technology for antisocial ends. But while many clearly believe the technology has the capacity for a dark side, no one has focused on how that dark side might manifest itself and on the legal issues the misuse of nanotechnology may generate. This article undertakes both tasks.

It begins with the premise that nanotechnology—like computer technology—is likely to be a profoundly transformative technology. It explains

† NCR Distinguished Professor of Law & Technology, University of Dayton School of Law. Email: susanwbrenner@yahoo.com.

why nanotechnology is likely to have wide-ranging effects across various sectors of society and speculates that nanocrime may evolve in a fashion analogous to computer crime. The article then analyzes how nanotechnology might be used to commit crimes of various types and argues that if and when nanocrime emerges, we should not respond—as we did to computer crime—by adopting technologically specific criminal statutes. Instead, we should, insofar as possible, integrate nanocrime into existing criminal law.

I. INTRODUCTION

> [I]t would be . . . reckless to attempt to list all the different kinds of crimes that might involve nanotechnology.[1]

This article deals with something that does not exist and probably will not exist for years, perhaps decades: using nanotechnology to commit crimes.

A great deal has been written about the societal implications of nanotechnology.[2] The books, articles and websites that deal with nanotechnology often note that criminals will exploit the technology for their own antisocial ends. But while many clearly believe the technology has the capacity for a dark side,[3] no one has focused on how that dark side might manifest itself and on the legal issues the misuse of nanotechnology may

1. PATRICK M. BOUCHER, NANOTECHNOLOGY: LEGAL ASPECTS 218 (CRC Press 2008).

2. *See, e.g.*, DEB BENNETT-WOODS, NANOTECHNOLOGY: ETHICS AND SOCIETY 10 (CRC Press 2008) (describing the societal implications of nanotechnology); BOUCHER, *supra* note 1, at 218 (discussing legal aspects of nanotechnology); K. ERIC DREXLER, ENGINES OF CREATION 172–73 (Anchor Press 1986) (describing the dangers of nanotechnology); J. STORRS HALL, NANOFUTURE: WHAT'S NEXT FOR NANOTECHNOLOGY 63–74 (Prometheus Books 2005) (exploring the implications of nanotechnology); RAY KURZWEIL, THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY 226–58, 398–400 (Viking 2005) (discussing the intersection of information and the physical world as it relates to nanotechnology and exploring the intertwined potentials of creativity and new dangers); DOUGLAS MULHALL, OUR MOLECULAR FUTURE: HOW NANOTECHNOLOGY, ROBOTICS, GENETICS, AND ARTIFICIAL INTELLIGENCE WILL TRANSFORM OUR WORLD 113–19 (Prometheus Books 2002) (discussing how nanotechnology and other things will change the world); TOBY SHELLEY, NANOTECHNOLOGY: NEW PROMISES, NEW DANGERS 4–35, 75–95 (Zed Books 2006) (exploring the promises and dangers of nanotechnology); SOCIETAL IMPLICATIONS OF NANOSCIENCE AND NANOTECHNOLOGY (Mihail C. Roco and William Sims Bainbridge, eds. 2001) (containing a collection of essays discussing different societal implications of nanotechnology); NAT'L SCI. FOUND. & NANOSCALE SCI., ENG'G, & TECH. SUBCOMM., REPORT OF THE NATIONAL NANOTECHNOLOGY INITIATIVE WORKSHOP, NANOTECHNOLOGY: SOCIETAL IMPLICATIONS – MAXIMIZING BENEFITS FOR HUMANITY (Mihail C. Roco & William Sims Bainbridge eds., 2003) (containing entries of several authors detailing nanotechnology), *available at* http://www.nsf.gov/crssprgm/nano/reports/nni05_si_societal_implications_2005.pdf. *See also* U.N. EDUC., SCIENTIFIC AND CULTURAL ORG., THE ETHICS AND POLITICS OF NANOTECHNOLOGY (2006) (examining future potential issues that may arise with the expanded prevalence of nanotechnology).

3. *See, e.g.*, BOUCHER, *supra* note 1, at 218 (discussing the gamut of crimes that may be committed with nanotechnology). *See also* STORRS HALL, *supra* note 2, at 232–34 (discussing nanotechnology and terrorism); Press Release, World Future Society, Futurist: Cybernetic Nanocrime A Future Threat to Public Safety (June 16, 2009), *available at* http://www.prleap.com/pr/137072/ (noting how nanotechnology is transforming the wired Internet); *Results of Our Ongoing Research*, CENTER FOR RESPONSIBLE NANOTECHNOLOGY, http://www.crnano.org/dangers.htm (discussing dangers of molecular manufacturing); Gene Stephens, *Cybercrime in the Year 2025*, REDORBIT (July 2, 2008), http://www.redorbit.com/news/technology/1459525/cybercrime_in_the_year_2025/index.html (detailing the interaction of nanotechnology and cyberspace).

generate.[4]

Those are the topics I examine in this article. The analysis is prospective and therefore speculative to a certain extent because nanocrime apparently has yet to manifest itself.[5] Some may question the utility of writing about a phenomenon that does not exist, but I think it is a useful endeavor.

I believe nanotechnology is at a point in its development that is analogous to where computer technology was in the 1950s.[6] In the 1940s and 1950s, mainframe computers were found only in government and university computer labs, and computer crime did not exist.[7] It did not emerge until the 1960s, when mainframes moved into the private sector and employees began using them to facilitate embezzlement and fraud crimes.[8] Computer crime became more common—and more complex—as the technology increasingly permeated the fabric of our daily lives.[9]

As I explain in more detail in Part III.A, I suspect something similar will occur with nanotechnology, which has already begun moving into the private sector.[10] My theory is that although nanotechnology has been moving into the private sector for years, it is still early in that process, so early no one is seriously considering the prospects for and likely implications of nanocrime. I think that is unfortunate: we had no basis for anticipating how computer technology could be misused, and while we had experience with the misuse of earlier, simpler technologies, the unprecedented capabilities and evolving complexity of computer technology made it difficult to foresee how it would be misused.

Some may argue that we are in a similar position with regard to nanotechnology, but I disagree. As I explain in Part III, I believe we can use our experience with computer crime to anticipate how law should deal with nanocrime, once it begins to appear. The two technologies differ in functionality and therefore in their capacity for misuse, but as I have argued elsewhere,[11] I do not think law should take a technology-specific approach to crimes the commission of which is facilitated by computer or other technology. In Part III, I use our experience with computer technology as an analogy from which to extrapolate how law can deal with the phenomenon on nanocrime,

---

4. More has been written about the military uses of nanotechnology. *See, e.g.*, JÜRGEN ALTMANN, MILITARY NANOTECHNOLOGY: POTENTIAL APPLICATIONS AND PREVENTIVE ARMS CONTROL (Routledge 2006) (providing a comprehensive presentation of the potential military applications of nanotechnology); STORRS HALL, *supra* note 2, at 227–39 (discussing how nanotechnology could be used in creating weapons).

5. "Nanocrime" is a neologism for which I cannot claim responsibility. The term was in use by 1998, but probably originated earlier. *See, e.g., Infowar: Are You Ready?*, NANOTECH (1998), http://www.nada.kth.se/~asa/InfoWar/nano.html (discussing nanocrimes and noting "nanocrime tracking").

6. *See* discussion *infra* Part III.A.

7. *See, e.g.*, SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 9–11 (Praeger 2010) (explaining the history of mainframe computers) [hereinafter BRENNER I].

8. *See id*. at 9–12 (detailing how computer crime developed alongside the development of mainframe computers).

9. *See id*. at 9–38 (describing the evolution of computer crime over time).

10. *See* discussion *infra* Part III.A.

11. SUSAN W. BRENNER, LAW IN AN ERA OF "SMART" TECHNOLOGY 137–81 (Oxford Univ. Press 2007) [hereinafter BRENNER II].

once it begins to emerge.[12]

First, though, I need to describe the technology itself; Part II gives an overview of nanotechnology. Part III postulates how nanotechnology can be misused and outlines the contours of a law of nanocrime. Section IV provides a brief conclusion.

II. NANOTECHNOLOGY

> [N]anotechnology is expected to bring about a technological revolution.[13]

This section explains what nanotechnology is and why many believe it will usher "in the second industrial revolution."[14] A study from the Hastings Center explains that nanotechnology "is expected to become a key transformative technology of the twenty-first century":[15]

> Nanotechnology is considered a general use or enabling technology because it has applications that span science and engineering fields, in areas as diverse as health care, energy storage, agriculture, water purification, computing, and security. Many experts predict nanotechnology will be as significant as the steam engine, the transistor, and the Internet in terms of societal impact.[16]

The term commonly used to denote transformative technologies is "general purpose technology" (GPT), and it refers to "a special type of technology that has broad-ranging enabling effects across many sectors of the economy."[17]

---

12. As an expert on nanotechnology noted, the "lessons of past technological revolutions are our best guide as we face the next." K. Eric Dressler, *Foreword* to J. STORRS HALL, NANOFUTURE: WHAT'S NEXT FOR NANOTECHNOLOGY 10 (Prometheus Books 2005).

13. ALTMANN, *supra* note 4, at 1.

14. Gregory Mandel, *Nanotechnology Governance*, 59 ALA. L. REV. 1323, 1329 (2008).*See also* K. Eric Drexler, *Foreword* to J. STORRS HALL, NANOFUTURE 9 (Prometheus Books 2006) (suggesting others have touted nanotechnology as a second industrial revolution); Ankan Bhattacharya, *Nano-Manufacturing: Government and Firm Incentives*, 4 NANOTECHNOLOGY L. & BUS. 199, 199 (2007) (describing the general perception of nanotechnology as the coming of the second industrial revolution); David L. Wallace & Nicholas Booke, *Industrial Revolution Redux, Nanotechnology: Law and Business at One-Billionth of a Meter*, 26 LJN'S PRODUCT LIABILITY L. & STRATEGY, Jan. 2008 (indicating nanotechnology's emerging prominence). Since nanotechnology is a complex phenomenon, this section does not purport to offer a comprehensive treatment of the technology itself. For more on that, the reader should consult the sources in note 2, *supra*.

15. Evan S. Michelson et al., *Nanotechnology, in* FROM BIRTH TO DEATH AND BENCH TO CLINIC: THE HASTINGS CENTER BIOETHICS BRIEFING BOOK FOR JOURNALISTS, POLICYMAKERS, AND CAMPAIGNS 111, 111 (Mary Crowley ed., Garrison 2008), *available at* http://www.thehastingscenter.org/Publications/BriefingBook/Detail.aspx?id=2192. Another report describes nanotechnology as "a 'platform' technology" because "it readily merges and converges with other technologies and could change how we do just about everything." KAREN F. SCHMIDT, NANOFRONTIERS: VISIONS FOR THE FUTURE OF NANOTECHNOLOGY 8 (Woodrow Wilson Int'l Ctr. for Scholars - Project on Emerging Nanotech. 2007), *available at* http://www.nanotechproject.org/process/assets/files/2704/181_pen6_nanofrontiers.pdf.

16. Michelson et al., *supra* note 15, at 111. *See also* Linda K. Breggin & Leslie Carothers, *Governing Uncertainty: The Nanotechnology Environmental, Health, and Safety Challenge*, 31 COLUM. J. ENVTL. L. 285, 288 (2006) ("Nanotechnology is what some term a 'general purpose technology' much like the Internet, electricity, or steam power.").

17. Richard S. Whitt & Stephen J. Schultze, *The New "Emergence Economics" of Innovation and Growth, and What It Means for Communications Policy*, 7 J. TELECOMM. & HIGH TECH. L. 217, 276 (2009) [hereinafter *New "Emergence Economics"*].

The term was introduced by Timothy Bresnahan and Manuel Trajtenberg in their 1995 article *General Purpose Technologies "Engines of Growth"?*[18]

They explained that GPTs act as "'enabling technologies' by opening up new opportunities rather than offering complete, final solutions."[19] Bresnahan later noted that the "most economically important use" of a GPT may not be determined by those who invented the technology "but rather by the inventors of complements, applications."[20] This aspect of GPTs means that the extent to which a particular technology qualifies as a general purpose technology may not be apparent when it is introduced. As one article notes, "when a new 'general purpose technology' is developed, such as the railway, the automobile, the telegraph and telephone, or the Internet, uncertainty is created as to how deeply the technology will transform the economy" and society.[21]

Notwithstanding this aspect of general-purpose technologies, many have already identified nanotechnology as a GPT.[22] Some go even further and characterize it as a uniquely complex GPT.[23] At this point, however, it is impossible to predict the extent to which nanotechnology will be a transformative technology . . . just as it was impossible for those who introduced personal computing in the 1980s to foresee the profound effects that technology would have on societies around the globe.[24]

For the purposes of this analysis, I will simply assume that nanotechnology qualifies as a GPT and consequently has the eventual capacity to transform societies in ways that are analogous to the changes wrought by antecedent GPTs such as electricity and personal computing. This assumption establishes the conceptual foundation for our inquiry into the likelihood and potential varieties of nanocrime. Before we embark on that inquiry, though,

---

18. Timothy F. Bresnahan & M. Trajtenberg, *General Purpose Technologies "Engines of Growth"?,* 65 J. ECONOMETRICS 83, 83 (1995).

19. *New "Emergence Economics", supra* note 17, at 276.

20. Timothy Bresnahan, *Creative Destruction in the PC Industry, in* PERSPECTIVES ON INNOVATION 105, 114 (Franco Malerba & Stefano Brusoni eds., 2007). Personal computers are one of the best examples of this aspect of GPTs. *See, e.g.*, Paul Osterman, *The Wage Effects of High Performance Work Organization in Manufacturing*, 59 INDUS. & LAB. REL. REV. 187, 189 (2006) (noting a study that found a positive relationship between wages and new technology such as the personal computer).

21. Patrick Bolton et al., *Pay for Short-Term Performance: Executive Compensation in Speculative Markets*, 30 J. CORP. L. 721, 723 (2005).

22. *See, e.g.*, Dumas Garrett, *Break-Out in Nanotech—The Next Potential Wave of IPOs*, 2 NANOTECH. L. & BUS. 274, 274 (2005) (proclaiming nanotechnology as a general purpose technology); Thomais Liota & Vassilios Tzitzios, *Investing in Nanotechnology*, 3 NANOTECH. L. & BUS. 521, 531 (2006) (classifying nanotechnology as a general purpose technology). *See also supra* note 16 and accompanying text.

23. *See, e.g.*, Dana Nicolau, *Challenges and Opportunities for Nanotechnology Policies: An Australian Perspective*, 1 NANOTECH. L. & BUS. 446, 451 (2004) ("Nanotechnology is a general purpose technology so pervasive that it . . . has sub-fields in physics, chemistry, biology and computing."). *See also* Stuart J.H. Graham & Maurizio Iacopetta, *Nanotechnology and the Emergence of a General Purpose Technology* 12 (Working Paper, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1334376 (noting predictions that nanotechnology will "evolve a level of complexity bringing benefits equal to those of information and communication technologies . . . or biotechnology").

24. *See, e.g.*, MARTIN CAMPBELL-KELLY & WILLIAM ASPRAY, THE COMPUTER: A HISTORY OF THE INFORMATION MACHINE 233–300 (1996) (chronicling the history of the personal computer). *See also* BRENNER II, *supra* note 11, at 105–10 (discussing how personal computers evolved to enable vast communication networks). *See generally* EDWARD E. GORDON, THE 2010 MELTDOWN: SOLVING THE IMPENDING JOBS CRISIS 45 (2005) (describing the wave of technological change provided by the personal computer age).

we need to review three prefatory issues: Part II.A, below, provides an overview of nanotechnology as a technology. Part II.B briefly reviews the literature addressing the potential risks of nanotechnology and Part II.C reviews proposals for using civil regulatory law to diminish the impact of those risks.

A. Technology

K. Eric Drexler uses a dichotomy to distinguish nanotechnology from the technologies that preceded it: He characterizes the antecedent technologies as "bulk technologies" because they all involve manipulating atoms and molecules in bulk; carpenters, potters, machinists, weavers and even the manufacturers of computer chips work with materials that are composed of trillions of discrete atoms.[25] Until relatively recently, we were limited to working with disparate assemblages of atoms because we did not have the ability to manipulate individual atoms.[26] Nanotechnology gives us that ability, which is why Drexler refers to it as "molecular technology."[27]

Writing in 1990, Drexler concluded that "[w]e can use the terms 'nanotechnology' and 'molecular technology' interchangeably" to describe the new non-bulk technologies.[28] That is still true, at least to some extent, perhaps because we unfortunately do not have a good definition of nanotechnology.[29]

As various sources note, the term has been defined in at least two different ways: one defines nanotechnology as any technology which deals with structures that are 100 nanometers or less in size; the other, older definition characterizes it as "building things from the bottom up, with atomic precision."[30] The validity of the older definition has eroded as nanotechnology research increasingly began to focus on top-down, as well as bottom-up, manufacturing.[31] The newer definition is therefore the more accurate of the

---

25. DREXLER, *supra* note 2, at 4 (1986) (describing technologies where trillions of atoms are manipulated as "bulk technologies").

26. *See id. See also* STORRS HALL, *supra* note 2, at 11–15 (describing briefly the historical progression of nanotechnology).

27. DREXLER, *supra* note 25, at 4 (noting that we now have the ability to "handle individual atoms and molecules with control and precision").

28. *Id.* at 5. *See also* STORRS HALL, *supra* note 2, at 15–23 (discussing different definitions of the term "nanotechnology").

29. *See* MULHALL, *supra* note 2, at 38 (noting that "a standard for 'nanotechnology' doesn't exist"). *See also* Nikolas J. Uhlir, Note, *Throwing a Wrench in the System: Size-Dependent Properties, Inherency, and Nanotech Patent Applications*, 16 FED. CIR. B.J. 327, 329–31 (2007) (discussing conflicting definitions of technology).

30. STORRS HALL, *supra* note 2, at 21; *What is Nanotechnology?*, CTR. FOR RESPONSIBLE NANOTECH., http://www.crnano.org/whatis.htm (last visited Feb. 22, 2011). This definitional confusion is at least in part a function of the fact that the term nanotechnology currently "refers to a broad collection of mostly disconnected fields." *Id.*

31. *See* Albert C. Lin, *Size Matters: Regulating Nanotechnology*, 31 HARV. ENVTL. L. REV. 349, 352 (2007) ("Nanotechnology includes both traditional 'top-down' manufacturing methods . . . as well as 'bottom-up' methods of building things on an atom-by-atom or molecule-by-molecule basis."); *What is Nanotechnology?*, *supra* note 30. A law review article explains the differences between the two:

> Traditional manufacturing processes employ top-down manufacturing. Top-down manufacturing essentially means that one takes larger objects and makes smaller objects out of them. For example, creating a sculpture from a large block of stone is a primitive type of top-down manufacturing. The

two, given the current state of nanotechnology.

A British study parsed the term further by distinguishing nanotechnologies from nanoscience.[32] According to this study, nanotechnologies encompass "the design, characterisation, production and application of structures, devices and systems by controlling shape and size at nanometre scale," while nanoscience is "the study of phenomena and manipulation of materials at atomic, molecular and macromolecular scales, where properties differ significantly from those at a larger scale."[33]

The British study's definition of nanotechnologies is consistent with the first definition given above. It explains that "one nanometre (nm) is equal to one-billionth of a metre" and atoms are less than "a nanometre in size, whereas many molecules . . . range from a nanometre upwards."[34] The study notes that while it defines nanotechnologies broadly, as encompassing "nanometre scale" activity, the size range that "holds so much interest" for those working with nanotechnology is "typically from 100nm down to the atomic level (approximately 0.2nm), because it is in this range . . . that materials can have different or enhanced properties compared with the same materials at a larger size."[35] The British study explains that the "two main reasons for [the] change in behaviour are an increased relative surface area, and the dominance of quantum effects."[36]

Experts divide nanotechnologies—or nanostructures—into four "generations," two of which—"passive" and "active" nanostructures—already exist.[37] Passive, or steady function, nanostructures incorporate nanoscale materials into existing products in order to improve their performance.[38] Passive nanostructures have been integrated into "products ranging from clothing and sporting goods to personal care and nutritional products."[39] Active, or evolving function, nanostructures are "biologically or electronically

---

> sculptor must chisel, grind, shape, and sand the block of stone until he obtains the desired configuration. . . .
>
> Bottom-up manufacturing . . . takes smaller objects and creates larger objects. The smaller objects can be individual atoms and molecules. By multiplying and manipulating these atoms and molecules in a particular way, one can create a desired object. Living organisms, such as plants or human beings, are essentially created in this manner.

Nicholas M. Zovko, Comment, *Nanotechnology and the Detrimental Use Defense to Patent Infringement*, 37 MCGEORGE L. REV. 129, 134 (2006) (footnotes omitted). The methods are not mutually exclusive. *See, e.g.*, THE ROYAL SOC'Y & ROYAL ACAD. OF ENG'G, NANOSCIENCE AND NANOTECHNOLOGIES: OPPORTUNITIES AND UNCERTAINTIES 29 (July 29, 2004), *available at* http://www.nanowerk.com/nanotechnology/reports/reportpdf/report14.pdf [hereinafter NANOSCIENCE AND NANOTECHNOLOGIES] (describing a convergence of top-down and bottom-up techniques).

32. *See* NANOSCIENCE AND NANOTECHNOLOGIES, *supra* note 31, at 5 (differentiating the terms "nanoscience" and "nanotechnology").

33. *Id*.

34. *Id.* Molecules are made up of atoms. *See generally* T.L. BROWN, CHEMISTRY – THE CENTRAL SCIENCE, (Prentice Hall eds. 9th ed. 2003); *Molecule*, WIKIPEDIA, http://en.wikipedia.org/wiki/ Molecule (last visited Feb. 7, 2011) (defining a molecule in part as a "group of at least two atoms").

35. NANOSCIENCE AND NANOTECHNOLOGIES, *supra* note 31, at 5.

36. *Id.*

37. INT'L RISK GOVERNANCE COUNCIL, NANOTECHNOLOGY RISK GOVERNANCE 8 (2007), *available at* http://www.irgc.org/IMG/pdf/PB_nanoFINAL2_2_.pdf; *What is Nanotechnology?*, *supra* note 30.

38. Michelson, *supra* note 15; INT'L RISK GOVERNANCE COUNCIL, *supra* note 37, at 7.

39. INT'L RISK GOVERNANCE COUNCIL, *supra* note 37 at 7.

dynamic,"[40] that is, they "can change their state during operation."[41] One report lists various types of active nanostructures: self-healing materials, "targeted drugs and chemicals," "light-driven molecular motors" and "adaptive nanostructures."[42]

The two remaining generations are projected to emerge at varying points over the next decade.[43] The third generation—which is projected to emerge some time after 2010—consists of "integrated nanosystems" or systems of nanosystems, i.e., "networking at the nanoscale."[44] Third generation nanostructures could be used to develop "artificial organs and . . . skin tissues" and/or "devices based on states other than that of the electric charge."[45] The fourth and final generation—which is expected to emerge some time after 2015—consists of "heterogeneous molecular nanosystems" in which nanosystem components "are reduced to molecules" that can "be used as devices or engineered to assemble on multiple length scales."[46] Fourth generation nanostructures could be used for "atomic and molecular-level assembly;"[47] potential applications of this generation of nanotechnology include "nanoscale genetic therapies and supramolecular components for transistors."[48]

B. Risks

For years, various observers have noted that nanotechnology—like many antecedent technologies—may bring risks as well as rewards.[49] As a result of the concerns that have been expressed, government agencies, private entities and individual researchers are devoting a great deal of time and effort to exploring the potential environmental, health and safety (EHS) risks of

40. Michelson, *supra* note 15, at 111.

41. INT'L RISK GOVERNANCE COUNCIL, *supra* note 37, at 7.

42. Vrishhali Subramanian, Active Nanotechnology: What Can We Expect? Program on Nanotechnology Research and System Assessment 1 (Mar. 2009) (unpublished paper) http://www.cherry.gatech.edu/PUBS/09/STIP_AN.pdf. *See also* INT'L RISK GOVERNANCE COUNCIL, *supra* note 37, at 7 ("Typical applications are expected to be in device and system components such as sensors with a reacting actuator or drug delivery multi-component particles that change their structure as they reach their intended target.").

43. *See, e.g.*, INT'L RISK GOVERNANCE COUNCIL, *supra* note 37, at 7 (discussing the various extant and upcoming generations of nanotechnology products and processes). *See also What Is Nanotechnology?*, *supra* note 30 (summarizing the four theorized generations of nanotechnology development).

44. INT'L RISK GOVERNANCE COUNCIL, *supra* note 37, at 7.

45. *Id*.

46. *Id*.

47. Michelson, *supra* note 15, at 111.

48. INT'L RISK GOVERNANCE COUNCIL, *supra* note 37 at 7. For more on the potential uses of all four generations of nanostructures, *see, e.g.*, SCHMIDT, *supra* note 15, at 5–8 (discussing the potential applications and nanotechnology).

49. *See, e.g.*, Bill Joy, *Why the Future Doesn't Need Us,* 17 ETHICS & MEDICINE 13, 23–24 (2001) (discussing the concerns raised over nanotechnology from the 1960s to the turn of the century); Jon Ronald, *Nanotechnology: The Promise and Peril of Ultratiny Machines*, 25 FUTURIST 28 (1991) (discussing the potential benefits and risks of nanotechnology); Rick Weiss, *Nanotechnology Risks Unknown*, WASH. POST, Sept. 26, 2006, at A12 (describing the balance between the advancing science in nanotechnology and the lack of regulation over its environmental, health, and safety risks).

nanotechnology.[50] As one report explained:

> Some of the unique properties of nanoscale material—e.g., small size, high surface area-to-volume ratio—have given rise to concerns about their potential implications for health, safety, and the environment. While nanoscale particles occur naturally and as incidental by-products of other human activities (e.g., soot), EHS concerns have been focused primarily on nanoscale materials that are intentionally engineered and produced.[51]

According to this report, the "EHS risks of nanoscale particles in humans and animals depend in part on their potential to accumulate, especially in vital organs such as the lungs and brain, that might harm or kill, and diffusion in the environment that might harm ecosystems."[52]

Nanoparticles enter an individual's or animal's body via "three primary vectors—inhalation, ingestion, and through the skin."[53] While scientists know little about the long-term effects of exposure to nanoparticles, studies have shown that very small nanoparticles can penetrate the skin and then enter the bloodstream, and inhaled nanoparticles can move "from the nasal region to the brain through the olfactory bulb, thus bypassing the blood-brain barrier" and possibly entering the brain.[54] Nanoparticles can also "pass through lung and

---

50. *See, e.g.*, *NNI Environmental, Health and Safety Research*, NAT'L NANOTECH. INITIATIVE, http://www.nano.gov/html/society/EHS.html (noting the U.S. government's "commitment to nanotechnology-related EHS research dates back to the inception of the National Nanotechnology Initiative, the multi-agency framework created in 2001 to coordinate . . . nanotechnology research and development"). *See also* Susan M. Wolf, Rishi Gupta & Peter Kohlepp, *Gene Therapy Oversight: Lessons for Nanobiotechnology*, 37 J.L. MED. & ETHICS 659, 676 (2009) (providing an overview of gene therapy and the use of nanotechnology in the field); *Aim of ENPRA*, RISK ASSESSMENT OF ENGINEERED NANOPARTICLES (ENPRA), http://www.enpra.eu/About.aspx (suggesting a new methodology for risk determination in the field of nanotechnology). *See generally* JOHN F. SARGENT, JR., CONG. RESEARCH SERV., RL34511, NANOTECHNOLOGY: A POLICY PRIMER 9 (2010), *available at* http://www.fas.org/sgp/crs/misc/RL34511.pdf (discussing the federally-funded National Nanotechnology Initiative and the "environmental, health, and safety implications" of nanotechnology). In 2009, Chinese researchers discovered that "a class of nanoparticles being widely developed in medicine . . . cause lung damage by triggering a type of programmed cell death known as autophagic cell death." *Health Risks of Nanotechnology*, SCIENCE NEWS (June 11, 2009), http://www.sciencedaily.com/releases/2009/06/090610192431.htm. This was apparently the first time researchers had identified "a mechanism by which nanoparticles cause lung damage." *Id*.

51. SARGENT, *supra* note 50, at 9 (footnotes omitted). *See also* Wolf et al., *supra* note 50, at 676 ("Nanoparticles have been categorized as either 'incidental nanoparticles' or 'engineered nanoparticles.' Incidental nanoparticles are naturally occurring particulates on the order of 100 nm in size, such as diesel exhaust or welding fumes, and are often irregularly shaped. Engineered nanoparticles . . . are designed to have regular shapes (spheres, tubes, rings, etc.). Recent risk research has centered on the latter.").

52. SARGENT, *supra* note 50, at 10 (noting an identified instance of this type of danger).

53. Wolf et al., *supra* note 50, at 676.

54. *Id*. The blood-brain barrier "is a separation of circulating blood and cerebrospinal fluid" that protects "the brain from many common bacterial infections." Wikipedia, *Blood-brain Barrier*, http://en.wikipedia.org/wiki/Blood-brain_barrier (last visited Feb. 22, 2011); *see also* David Darling, *Blood-brain barrier (BBB)*, THE INTERNET ENCYCLOPEDIA OF SCIENCE, http://www.daviddarling.info/encyclopedia/B/blood-brain_barrier.html (providing an overview of the blood-brain barrier and its functions) (lat visited Feb. 22, 2011). Most traditional contaminants cannot cross the blood-brain barrier. *See, e.g.*, Albert C. Lin, *Size Matters: Regulating Nanotechnology*, 31 HARV. ENVTL. L. REV. 349, 358–59 (2007) ("[U]nlike most contaminants, nanoparticles may cross the blood-brain barrier and enter the central nervous system through neuronal pathways leading from the respiratory tract to the brain."). For a fictional account of how nanoparticles could cross the blood-brain barrier, *see* EDWARD M. LERNER, SMALL MIRACLES 210–38 (2009) (discussing a potential use of nanotechnology in a futuristic setting).

liver tissue."[55]

While researchers have identified these and other potentially dangerous aspects of nanotechnology, the precise nature and magnitude of the threat the technology poses remains uncertain. As one author noted, risk "to human health and the environment is the most pressing issue in the governance of novel technologies", but the "definition and measures of risk are challenged with nanotechnologies" because:

> [Nanotechnology] techniques and products are often combined with other technologies, making it difficult to categorize products by intended use, much less to tease out specific effects. Interactions between components of a technology at the nanoscale or between nanomaterials and human tissue may not be linear, and most testing logics reduce interactions to single-outcome measurements. Predictive algorithms may also be questionable, as many nano-techniques rely on the ability of materials to behave differently at the nanoscale than at larger, more familiar scales.[56]

While assessing the risks associated with nanotechnology is, and is likely to continue to be, an extraordinarily complicated task, many who are involved with the technology believe it is a task we must master. A survey of "business leaders in the field of nanotechnology" found that "nearly two-thirds" of them believed we do not understand the risks the technology poses to human life and environmental integrity; those surveyed also believed it is "important" for the government to conduct a meaningful assessment of these risks in order to protect "human health, safety, and the environment".[57]

The efforts that are currently being made to assess the risks associated with our use of nanotechnology tend to focus on the inadvertent and therefore unintended consequences of incorporating nanotechnology into consumer products, manufacturing and medical care.[58] As a United Nations study explained, there are two concerns:

> [T]he hazardousness of nanoparticles and the exposure risk. The first concerns the biological and chemical effects of nanoparticles on human bodies or natural ecosystems; the second concerns the issue of leakage, spillage, circulation, and concentration of nanoparticles that would cause a hazard to bodies or ecosystems.[59]

As I noted earlier,[60] the process of assessing these concerns is more

---

55. Maksim Rakhlin, *Regulating Nanotechnology: A Private-Public Insurance Solution*, 2008 DUKE L. & TECH. REV. 2, 5 (2008) [hereinafter *Regulating Nanotechnology*]. *See supra* note 50 and accompanying text (setting forth the various entities that are studying the potential risks of nanoparticles, such as lung damage).

56. Linda F. Hogle, *Science, Ethics, and the "Problems" of Governing Nanotechnologies*, 37 J.L. MED. & ETHICS 749, 753 (2009). *See* David L. Wallace, *Mediating the Uncertainty and Abstraction of Nanotechnology Promotion and Control: "Late" Lessons from Other "Early Warnings" in History*, 5 NANOTECH. L. & BUS. 309, 310 (2008) ("[T]he risks and benefits [of nanotechnology] are largely undefined and unknown, rendering their full quantification largely impossible.").

57. SARGENT, *supra* note 50, at 10.

58. *See, e.g.*, Wolf et al., *supra* note 50, at 676.

59. UNITED NATIONS EDUC., SCIENTIFIC & CULTURAL ORG., THE ETHICS & POLITICS OF NANOTECHNOLOGY 14 (2006).

60. *See supra* note 56 and accompanying text.

complex than the process of assessing similar concerns for non-nanotech materials. The tendency to utilize nanomaterials in conjunction with other technologies is only one of the factors that exacerbate the difficulty of this process.[61] Another is the unique properties of nanoparticles:[62] They tend "to persist [in the body] for longer periods as nanoparticles" because of the way they are designed, and they may "be better able to evade the body's defenses because of their size or protective coatings."[63] Nanoparticles may also be able to persist for longer periods in the environment.[64] A third factor that exacerbates the difficulty of identifying and assessing potential threats is that nanotechnology—like computer technology—is inherently unstable, i.e., it continues to evolve. As one scientist noted, "[w]ith researchers in 40 countries creating new nanoparticles every day," it is "difficult to assess each particle individually" in order to determine its characteristics and risk potential.[65]

In sum, while we know little about the specific risks associated with nanotechnology, those who study the technology are certain it will generate hazards that are both unprecedented and elusive.[66] It is, however, not enough simply to identify risks; we need risk control strategies, as well. The current risk assessment process focuses exclusively on what I call "civil" nanotech risks; that is, it focuses on hazards that are an inadvertent and therefore unintentional byproduct of legitimate uses of the technology. As a result, nanotechnology risk assessment and control strategies focus on how civil regulatory law can be used to ensure integrity in the production and implementation of the technology. The next section reviews the prospects for

---

61. *See supra* note 56 and accompanying text.

62. Some say "the 20th-century emphasis on a classically linear, expert-driven . . . approach to technological risk assessment" is not suitable for evaluating nanotechnology because of 'the unique nature and scale" of the technology." Wallace, *supra* note 56, at 309.

63. Lin, *supra* note 31, at 356–57. There are various types of nanoparticles, many of which may be hazardous. *See, e.g.*, Kevin Rollins, *Nanobiotechnology Regulation: A Proposal for Self-Regulation with Limited Oversight*, 6 NANOTECH. L. & BUS. 221, 225 (2009) ("Carbon nanotubes and gold/silver nanoparticles are not the only nanomaterials that might pose a risk to humans; just the most famous. Studies also suggest that buckyballs, diamond nanoparticles, iron nanoparticles, cobalt-doped tungsten carbide nanoparticles, and silica nanoparticles may also be harmful.") (footnotes omitted). *See also EPA Issues Fact Sheet on Nanomaterials*, 27 HAZARDOUS WASTE CONSULTANT, no. 6, 2009, at 1.9 (listing types of nanoparticles).

64. *See, e.g.*, Barbara P. Karn & Lynn L. Bergeson, *Green Nanotechnology: Straddling Promise and Uncertainty*, 24 NAT. RESOURCES & ENV'T 9, 10–11 (2009) (discussing the current uncertainty of the effects of nanoparticles); Mandel, *supra* note 14, at 1365 (stating that "engineered nanoparticles . . . may be designed to persist").

65. Elizabeth Bahm, *New Study Shows Possibilities and Dangers of Nanotechnology*, MEDILL REPORTS (Apr. 8, 2010), http://news.medill.northwestern.edu/chicago/news.aspx?id=162744&print=1.

66. One, perhaps apocryphal, nanotechnology risk has been discredited. In 1990, in his book *Engines of Creation*, Eric Drexler introduced the "grey goo" scenario. Kevin Bonsor & Jonathan Strickland, *How Nanotechnology Works*, HOW STUFF WORKS, http://www.howstuffworks.com/nanotechnology.htm/printable (last visited Feb. 21, 2011); *Grey Goo*, WIKIPEDIA, http://en.wikipedia.org/wiki/Grey_goo (last visited Jan. 27, 2011). Drexler postulated a scenario in which "out-of-control self-replicating [nano-]robots" multiply with exponential rapidity and quickly "consume all matter on Earth while building more of themselves." *Id*. *See* DREXLER, , *supra* note 2, at 56–58 (discussing the potential rate at which nano-sized machines may be able to replicate). The scenario has been discredited; in 2004, Drexler himself published an article in which he declared that the runaway replicators scenario was "quite obsolete" given the current state of nanotechnology. *See* Liz Kalaugher, *Drexler Dubs "Grey Goo" Fears Obsolete*, NANOTECHWEB.ORG (June 9, 2004), http://nanotechweb.org/cws/article/indepth/19648 (explaining how Drexler "now believes that self-replication . . . is not an essential part of the molecular manufacturing process").

using regulatory law to control the risks associated with nanotechnology.

C. Regulation

In the United States, as in other countries, no existing regulatory program "squarely addresses nanotechnology or its applications."[67] There is disagreement as to how this regulatory vacuum should be addressed; as one expert noted, risk control proposals "run the gamut from completely banning nanotechnology production to eliminating all regulation."[68]

Since it is highly unlikely that either extreme constitutes a viable way to resolve the problem, the solution will almost certainly involve a compromise that reconciles the pressure to implement nanotechnology with the need to regulate its production and use. The critical issue here seems to be deciding whether to (i) adapt existing regulatory law so it encompasses nanotechnology or (ii) adopt new nanotechnology-specific regulatory laws.[69] We will use the current state of U.S. law to explore the viability of each alternative.

1. Existing Law

While the United States has no nano-specific regulatory structure, three federal agencies claim the ability to regulate certain aspects of nanotechnology.[70] The first, the Environmental Protection Agency [EPA], "attempts to regulate nanomaterials" under the Toxic Substances Control Act [TSCA], "which was enacted to ensure that adequate safeguards are put in place before new chemicals are marketed to consumers."[71]

---

67. Scott H. Segal, *Environmental Regulation of Nanotechnology: Avoiding Big Mistakes for Small Machines*, 1 NANOTECH. L. & BUS. 290, 295 (2004). *See also* Diana M. Bowman & Graeme A. Hodge, *A Small Matter of Regulation: An International Review of Nanotechnology Regulation*, 8 COLUM. SCI. & TECH. L. REV., 1, 30–36 (2007) (discussing various approaches to regulating nanotechnology); Jordan Paradise et al., *Developing U.S. Oversight Strategies for Nanobiotechnology: Learning From Past Oversight Experiences*, 37 J.L. MED & ETHICS 688, 690–91 (2009) [hereinafter Paradise et al., *Developing Oversight*] (discussing the proper role of oversight).

68. Rakhlin, *supra* note 55, at 23.

69. *See id.* at 12–21 (discussing both existing laws and new laws specific to nanotechnology). *See also* Linda F. Hogle, *Science, Ethics, and the "Problems" of Governing Nanotechnologies,* 37 J.L. MED. & ETHICS 749, 750 (2009) (claiming that "many continue trying to fit . . . issues related to nanobiotechnologies into . . . frameworks that . . . may no longer work"); J. CLARENCE DAVIES, MANAGING THE EFFECTS OF NANOTECHNOLOGY 16–24 (Woodrow Wilson Int'l Ctr. For Scholars – Project on Emerging Nanotech. 2006), *available at* http://www.nanotechproject.org/process/assets/files/2708/30_pen2_mngeffects.pdf (discussing existing and potential new laws). *But see* John Bashaw, *Regulation of Nanoparticles: Trying to Keep Pace with a Scientific Revolution*, 6 NANOTECH. L. & BUS. 475, 482 (2009) ("Since the existing regulatory structure can be adapted to handle current challenges associated with nanoparticles, wholesale new regulation . . . does not appear to be necessary . . . ."); Mandel, *supra* note 14, at 1363 ("Not only would designing a new statutory scheme to regulate nanotechnology appear impossible due to the substantial current unknowns, but any such regulation would not confront the problems of insufficient science and limited detection capabilities.").

70. *See* Rakhlin, *supra* note 55, at 13–20 (discussing regulations put in place by different federal agencies).

71. *Id.* at 8 (citing DAVIES, *supra* note 69, at 13). The EPA would also have authority to regulate nanotechnology under the Clean Air Act, 42 U.S. Code §§ 7401-7671q, to the extent that nanoparticles constituted a threat to "outdoor air quality." Mandel, *supra* note 14, at 1352–53. But as this author notes, "[t]he substantial limits on scientific knowledge concerning the risks of [airborne] nanoparticles" [and] "deficiencies in the ability to detect nanoparticles in the air" make regulation under the Clean Air Act highly

The TSCA at least arguably applies to chemical substances "manufactured at the nanoscale level,"[72] but actually applying it to nanomaterials can be dicey because the TSCA regulates materials based on their molecular identity, not on their size.[73] This approach can become problematic in the nanocontext because "what makes nanoparticles . . . unique are their physical attributes . . . not . . . their molecular identity."[74] This means the EPA might refuse to regulate a nanoparticle because its molecular identity does not establish it as a new chemical subject to regulation under the TSCA standard.[75] That possibility has prompted some to demand that TSCA regulations be revised to "explicitly address nanomaterials."[76]

The second agency that claims some authority to regulate nanotechnology is the U.S. Department of Labor; more precisely, it is the Department of Labor's Occupational Safety and Health Administration (OSHA). Under the Occupational Health and Safety Act ("the Act"),[77] OSHA "sets standards for hazardous airborne particles"[78] that are intended "'to provide safe or healthful'" workplaces.[79] OSHA sets "permissible exposure limits ('PELs') for each" hazardous material and uses administrative and engineering controls and protective equipment to keep worker exposure to PELS within acceptable limits.[80] OSHA has not issued specific guidelines regarding nanomaterials, so they are governed under the Act's "general duty clause, which states that an employer must provide a workplace 'free from recognized hazards.'"[81] As many have noted, this approach is not well suited for dealing with nanomaterials:

> OSHA almost surely cannot keep pace with the proliferation of different types of nanomaterials . . . . [T]he uncertainty surrounding the health and environmental effects of nanomaterial exposure would make it virtually impossible to meet the statutory thresholds for regulation. Moreover, it is not clear how effective . . . workplace health standards would be. Little information is available regarding the effectiveness of engineering controls and protective equipment in controlling nanomaterial exposure . . . .[82]

---

problematic. *Id.* at 1353. The Federal Insecticide, Fungicide and Rodenticide Act, 7 U.S. C. §§ 136-136v, the Resource Conservation and Recovery Act, Pub. L. No. 94-580, 90 Stat. 2, 795 (1976), and/or the Clean Water Act might give the EPA regulatory authority over other aspects of nanotechnology. *See* Mandel, *supra* note 14, at 1353–57 (discussing these three Acts).

72. Rakhlin, *supra* note 55, at 8.

73. Bashaw, *supra* note 69, at 477.

74. *Id.* at 478.

75. *Id.*

76. David B. Fischer, *Nanotechnology—Scientific and Regulatory Challenges*, 19 VILL. ENVTL. L.J. 315, 327 (2008).

77. 29 U.S.C. §§ 651–78 (2006).78.Rakhlin, *supra* note 55, at 9.

78. Rakhlin, *supra* note 55, at 9.

79. Lin, *supra* note 31, at 370 (quoting 29 U.S.C. § 652(8) (2006)).

80. *Id.*

81. Mandel, *supra* note 14, at 1361 (quoting 29 U.S.C. § 654(a)(1)). The National Institute for Occupational Safety and Health has begun to implement a research agenda addressing the occupational safety and health aspects of nanotechnology, but it has no authority to regulate the technology. *Id.* at 1362.

82. Lin, *supra* note 31, at 371. One author identified an additional problem: OSHA's "determination of an acceptable quantity of toxic airborne substances applies [only] to macro-particles," so nanoparticles may be

The third and final agency is the Food and Drug Administration (FDA).[83] The "use of nanoparticles in food, drugs and cosmetics is covered by the Food, Drug and Cosmetics Act" (FDCA).[84] The FDA's "informal adoption" of the U.S. National Nanotechnology Initiative's definition of nanotechnology, which recognizes that nanomaterials can have "novel properties and functions because of their small size," seems to acknowledge "the fundamentally different characteristics of nanoparticles", but that attitude is not evident in the FDA's approach to testing methodologies and standards.[85] As one author noted, its "testing methodologies are based on bulk material or larger particles," which makes them ill-suited for dealing with nanotechnology.[86]

In 2007, the FDA's Nanotechnology Task Force[87] issued a report that analyzed the potential challenges nanotechnology posed for the agency's ability to implement its agenda.[88] The report concluded that neither "a new regulatory framework" nor "special regulations for nanotechnology" were necessary "at that time," but noted that the FDA should "keep abreast of the science in order to appropriately apply regulations in the future."[89] The FDA has yet to take any meaningful steps toward developing a coherent nanotechnology policy.[90] One article lists several factors that are likely to impair the FDA's effectiveness in regulating nanotechnology, including:

> [L]ack of financial resources. While the FDA has one of the largest budgets of any federal agency, their responsibilities are vast. Another

---

outside its regulatory authority. Rakhlin, *supra* note 50, at 9.

83. Rakhlin, *supra* note 50, at 9.

84. Bashaw, *supra* note 69, at 476 (citing 21 U.S.C. §§ 301–399a (2006)).

85. George A. Kimbrell, *Governance of Nanotechnology and Nanomaterials: Principles, Regulation, and Renegotiating the Social Contract*, 37 J.L. MED. & ETHICS 706, 710 (2009). For the U.S. National Nanotechnology Initiative, see *supra* note 50.

86. *Id.* at 710. *See also* Donald R. Johnson, Note, *Not in My Makeup: The Need for Enhanced Premarket Regulatory Authority over Cosmetics in Light of Increased Use of Engineered Nanoparticles*, 26 J. CONTEMP. HEALTH L. & POL'Y 82, 104 (2009) ("The testing methods currently used by the FDA rely on the macro-scale equivalents to the nanoparticles in question and thus must be altered to take into account the differences between nanoscale and macro-scale particles . . . .").

87. *Nanotechnology Task Force*, FOOD & DRUG ADMIN., (Apr. 9, 2010), http://www.fda.gov/ScienceResearch/SpecialTopics/Nanotechnology/NanotechnologyTaskForce/default.htm (describing the purposes and responsibilities of the task force).

88. FOOD AND DRUG ADMINISTRATION, NANOTECHNOLOGY TASK FORCE, NANOTECHNOLOGY (2007), *available at* http://www.fda.gov/downloads/ScienceResearch/SpecialTopics/Nanotechnology/ucm110856.pdf [hereinafter NANOTECH TASK FORCE].

89. Jordan Paradise et al., *Evaluating Oversight of Human Drugs and Medical Devices: A Case Study of the FDA and Implications for Nanobiotechnology*, 37 J. L. MED. & ETHICS 598, 603 (2009) [hereinafter Paradise et al., *Evaluating Oversight*] . *See* NANOTECH. TASK FORCE, *supra* note 88, at ii – iii (acknowledging the need to focus on improving knowledge of nanotechnology to ensure the agency's effectiveness, but describing the agency's then-existing authority as "generally comprehensive."). The Task Force Report explained that nanomaterials "present regulatory challenges similar to those posed by . . . other emerging technologies", but cautioned:

> [C]hallenges may be magnified both because nanotechnology can be used in, or to make, any FDA-regulated product, and because, at this scale, properties of a material relevant to the safety and (as applicable) effectiveness of FDA-regulated products might change repeatedly as size enters into or varies within the nanoscale range.

Id. at ii.

90. *See, e.g.*, Kimbrell, *supra* note 85, at 717–18 (discussing the FDA's need for meaningful policy and oversight measures with respect to nanotechnology); Paradise et al., *Evaluating Oversight*, *supra* note 89 at 621–22; (questioning the FDA's ability to effectively oversee nanotechnology products).

> hurdle will be that the . . . century-old definitional frameworks for classifying a product as a drug, device, or biologic may be ill equipped to handle the convergence of properties at the nanoscale . . . [T]he FDCA may not sufficiently distinguish products at the nanoscale. Rapidly developing applications in nanomedicine . . . will likely add another layer to the classification challenge . . . . Questions include whether this requires a distinct regulatory definition for nanotechnology for drug and medical device products; how this definition will vary from applications in other technical fields regulated by other federal agencies; and . . . whether distinctions between "chemical" and "mechanical" action need to be reassessed at the nanoscale.[91]

It seems, then, that the regulatory frameworks currently in place in the United States (and elsewhere)[92] are ill-equipped to deal with integrating nanotechnology into consumer and other products. As one author observed, the existing system is "too weak and cumbersome to analyze and manage the potential risks posed by nanomaterials."[93] Some, including this author, believe the current approach—which diffuses regulatory authority among a variety of agencies—is archaic and consequently inadequate to deal with "something as . . . dynamic as nanoscale science."[94] Those who take this view argue that an approach that was devised to regulate the implementation of discrete technologies—each with a fixed, limited function—is inherently incapable of dealing with nanotechnology, the pliancy and pervasiveness of which is likely to surpass anything mankind has yet encountered.[95] They conclude that the solution is to devise a nanotechnology-specific regulatory framework, an issue we address in the next section.

2. New Law

According to one report, nanotech-specific regulatory legislation would

---

91. Paradise et al., *Evaluating Oversight*, *supra* note 89, at 621.

92. *See, e.g.*, Bowman, *supra* note 67 (surveying nanotechnology regulation internationally).

93. Lin, *supra* note 31, at 351.

94. Wallace, *supra* note 56, at 310.

95. *See id.* (discussing the inherent problems with the existing regulatory framework). One report pointed out some of the difficulties that would arise if we attempted to update the current approach to allow it to address nanotechnology:

> There . . . would be the . . . problem of deciding how to define what is covered. Is it possible to define NT [nanotechnology] just by the size of the material? What if the NT material is combined with a non-NT material? If one manufacturer makes carbon nanotubes and another . . . makes a textile that incorporates the tubes, do you regulate both? If the nanotubes are used in a medical device, what role would FDA play? What happens . . . when NT is combined with genetic engineering? . . . Even assuming that existing laws could be amended to clarify . . . their coverage of NT—and that the patchwork of existing laws could be stitched together in a coordinated framework that would perform better than it has for biotech—one still would be left with the weaknesses . . . in these laws . . . . TSCA still would lack authority to require risk data. FDA still would not be able to review and regulate the ingredients of cosmetics. OSHA still would lack resources . . . . It would be easier, politically and substantively, to draft and enact a new law focused on NT.

DAVIES, *supra* note 69, at 17; *see also* Lin, *supra* note 31, at 374 ("[G]iven the pace of technological development, and the evidentiary burdens the statutes place on . . . agencies, it is unlikely that existing statutes will ever provide a complete and adequate response.").

have "two major advantages": It would "avoid some of the pitfalls of previous . . . laws" and could be "tailored to the particular characteristics" of nanotechnology.[96] So far, proposals for new, nanotech-specific regulatory law tend to focus on regulating products that contain nanomaterials, rather than on the nanomaterials themselves.[97]

Under one proposal, all *products* containing nanomaterials would be regulated because "exposure and toxicity are not predictable from" the materials alone; exposure and toxicity can depend on how nanomaterials are used in the product.[98] This proposal would impose testing and reporting obligations on the manufacturers of products containing nanomaterials and would put the "burden of proof for showing that [a] product does not pose unacceptable risks. . ." on the user of that product.[99]

Another proposal would establish a two-tiered system in which (i) all products containing nanomaterials "would be subject to mandatory notification and labeling requirements" and (ii) products containing "free nanomaterials"[100] would also "be subject to a screening process, post-market monitoring, and bonding requirements."[101] This proposal regulates products containing free nanomaterials more stringently because nanomaterials "found in a free form, as opposed to those embedded in composite materials, pose the greatest potential for negative health and environmental effects."[102]

The notification requirement would compel manufacturers and distributors to provide the nano-regulatory agency with a notice that described the nanomaterial(s) included in a product, the process used to manufacture the product, by-products of its manufacture, and any "available information on health and environmental effects . . . ."[103] The labeling requirement would compel manufacturers and distributors to label products as products that

96. DAVIES, *supra* note 69, at 21. *See also* INT'L CTR. FOR TECH. ASSESSMENT, PRINCIPLES FOR THE OVERSIGHT OF NANOTECHNOLOGIES AND NANOMATERIALS, 7 (2007), *available at* http://www.icta.org/nanoaction/doc/nano-02-18-08.pdf ("A . . . nano-specific regulatory scheme must be an integral aspect of the development of nanotechnologies."). One author takes a broader view, suggesting that "the question of nanotechnology oversight creates a golden opportunity to ameliorate long-festering problems in U.S. oversight structures." Kimbrell, *supra* note 85, at 713.

97. *See* Lin, *supra* note 31, at 391 (proposing a statute recognizing the distinction between nanomaterials found in free form and those embedded in other products); DAVIES, *supra* note 69, at 18 (recommending that the definition of nanotechnology products encompass all products containing nanotech materials, as well as nanotech materials themselves). One proposal would exclude products regulated by other frameworks provided that the regulation was "adequate to protect the public"; this proposal would not automatically apply the new law retroactively to products already on the market. *See id.* at 19.

98. DAVIES, *supra* note 69, at 18–19 ("The exposure and toxicity of a carbon nanotube or a titanium nanoparticle, for example, will depend on what structure it is shaped in, what other materials it is used with, and how it is used.").

99. *Id.* A subsequent review process would determine whether a product's risk was acceptable or not, and might provide companies with tax and other incentives for developing safe products. *See id.* at 20 (discussing the benefits of a subsequently review process).

100. Free nanomaterials "are not fixed or embedded in another substance and can thus move freely within the medium into which they are introduced." Johnson, *supra* note 85, at 89. *See* NANOSCIENCE AND NANOTECHNOLOGIES, *supra* note 31, at vii-x (describing nanomaterial). "An example of a free nanomaterial is titanium dioxide, which is used extensively in cosmetics and sunscreens." Johnson, *supra* note 86, at 89. .

101. Lin, *supra* note 31, at 391.

102. *Id.*

103. *Id.*

contain nanomaterials, to identify the "specific nanomaterial[s] [it contains], and to provide a brief comparison of the nanomaterial with the bulk version of the material."[104] The labeling requirement is intended to:

> [F]acilitate more efficient functioning of the market through better informed consumer choice . . . . [It] would enable consumers to decide whether to purchase conventional products, whose risks may be better known, or "new and improved" products containing nanomaterials, whose health effects are more uncertain. Likewise, better-informed workers may demand greater safety precautions or wage premiums in exchange for occupational health uncertainty. In addition, workers may monitor their health more closely, and any workers who do become ill as a result of exposure to nanomaterials will be in a better position to demonstrate that such exposure caused their illness.[105]

As noted above, products containing free nanomaterials would also be subject to "screening, bonding, and monitoring."[106] Screening would be designed to bypass the delays involved in extensive analysis of particular materials and exclude "materials that appear most likely to be toxic."[107] Products that passed the screening "could be introduced into commerce, subject to the bonding and monitoring requirements . . . ."[108] Products that failed the screening would not be barred from commercial use; the manufacturer of such a product would bear the burden of demonstrating that it could be used safely.[109] Manufacturers or distributors whose products passed the screening and were introduced into commerce would have to post an assurance bond to cover damages that might result from their use.[110] Products would also be monitored to detect possible long-term risks resulting from "cumulative exposure to different nanomaterials, or risks to the environment."[111]

The authors of both proposals suggest that the measures for which they respectively advocate should, insofar as possible, be coordinated with similar efforts in other countries. Both endorse the use of an international agreement—or agreements—to ensure consistency across national nano-regulatory schemes.[112] Other countries are in varying stages of deciding how they should address the need for nanotechnology regulation;[113] some

104. *Id.* at 393.
105. *Id.* at 393 (footnotes omitted).
106. *Id.* at 395–96.
107. *Id.* at 396.
108. *Id.*
109. *Id.* at 396–97.
110. *Id.* at 397–98.
111. *Id.* at 397. Aside from the labeling requirement, this proposal does not address workplace exposure to nanomaterials. *See id.* at 404–05 (describing the screening process).
112. *Id.* at 407; DAVIES, *supra* note 69, at 19–20. The Australian government is apparently "considering nano-specific regulation," and in 2005 the European Economic and Social Committee of the European Parliament recommended that the European Commission propose European nanotechnology guidelines by 2008. Paradise et al., *Developing Oversight*, *supra* note 67, at 691. The European Parliament apparently has yet to act on that recommendation. *Id.*
113. *See* Paradise et al., *Developing Oversight*, *supra* note 67, at 691 ("The Australian government is considering nano-specific regulation following a . . . report by Monash University scholars concluding that

commentators believe the only effective approach is one that relies on transnational regulatory frameworks.[114]

3. Assessment

Nano-specific regulation seems advisable given the apparently unique aspects of the technology at issue, but it actually may not be the best approach. Nano-specific regulation presumably means that one agency would be responsible for assessing the risks of utilizing nanotechnologies in various contexts (e.g., medicine, transportation, agriculture, energy, construction, communication, manufacturing, etc.).[115] The agency's primary focus would be on nanotechnology, which no doubt means that individuals whose expertise was in nanotechnology would play a major role in making this assessment. The question is whether the assessment should be made by those whose focus is on the technology or by those whose focus is on the idiosyncratic issues that arise in a specific context, e.g., medicine or agriculture.

It is probably much too early for us to be able to answer that question. The answer depends on the extent to which nanotechnology proves to be a transformative technology, the pervasiveness and complexity of which exceed that of antecedent technologies. It is easy to overstate the impact an emerging technology is likely to have on our lives; something similar occurred with computers[116] and, as we will see in the next section, resulted in legislation that

existing regulatory frameworks contain numerous gaps when applied to nanotechnology."); Public Consultation: Australian Government Proposes Legislation of Nanomaterials, NANOTECH. INDUS. ASS'N (November 20, 2009), http://www.nanotechia.org/news/global/public-consultation-australian-government-propose (describing the discussion paper). *See also* Robert Lee & Elen Stokes, *Twenty-first Century Novel: Regulating Nanotechnologies*, 21 J. ENVTL. L. 469, 470 (2009) (stating that "until very recently, there was no nano-specific legislation either in the UK or the EU (and, even now, there are currently only two such provisions)").

114. *See, e.g.*, Gary E. Marchant & Douglas J. Sylvester, *Transnational Models for Regulation of Nanotechnology*, 34 J. L. MED & ETHICS 714, 717–23 (2006).

115. *See, e.g.*, James R. Brindell, *Nanotechnology and the Dilemmas Facing Business and Government*, 83 AUG. FLA. B.J. 73, 76 (2009) (explaining how "it is clear that U.S. federal and state governments have been disinclined to establish a comprehensive notification of use or regulatory program for nanomaterials"); Lin, *supra* note 31, at 392 (discussing the benefits of adopting legislation requiring notification requirements for manufacturers of nanomaterials); Lindsay V. Dennis, Comment, *Nanotechnology: Unique Science Requires Unique Solutions*, 25 TEMP. J. SCI. TECH. & ENVTL. L. 87, 110–11 (2006) (stating examples of how one agency would be responsible for assessing the risks of utilizing nanotechnologies in various contexts). *See generally* Joel Rothstein Wolfson, *Social and Ethical Issues in Nanotechnology: Lessons from Biotechnology and Other High Technologies*, 22 BIOTECHNOLOGY L. REP. 376, 385 (2003) (discussing regulation of nanotechnologies). For some of the currently foreseeable applications of nanotechnology, *see, e.g.*, *Nanotechnology Applications*, UNDERSTANDING NANOTECHNOLOGY (Feb. 22, 2011), http://www.understandingnano.com/ nanotech-applications.html; *List of nanotechnology applications*, (last visited Feb. 22, 2011) WIKIPEDIA, http://en.wikipedia.org/wiki/List_of_nanotechnology_applications.

116. *See infra* Part III.A. A 1979 article described computer technology in terms essentially identical to those now being used to describe nanotechnology:

> The author of the best-seller Future Shock said the world is beginning to undergo massive changes that will pave the way for a third wave of human development. The first wave was the advent of agriculture more than 10,000 years ago. The second was the industrial revolution. The third is the emerging era of computers and instant communication.

Martin Dewey, *Toffler Sees Industrial Breakup*, GLOBE & MAIL (Canada), May 3, 1979. *See* Alan M. Kriegsman, *Future Peril, Future Promise*, WASH. POST, Jan. 14, 1979, at P3 ("[T]he computer . . . will alter life ahead in profound and mysterious ways. . . ."); *They're Ours, But Do They Work?,* THE ECONOMIST, Mar.

tended to over-emphasize the role computers would play in crime.

However we resolve the issue of nanotechnology regulation, civil regulatory measures will be of little utility in analyzing the issues we address below because they are designed to address risks that are the product of inadvertence, not intention.[117] I included this brief treatment of how we may approach regulation for two reasons: One is that it illustrates the operational tension between technology-specific and technology-neutral control measures. The other is that it illustrates the types of risks associated with various uses of nanotechnology. In the next section, we take up advertent nanotech risks, i.e., intentional abuse of the technology.

III. TECHNOLOGY AND CRIME

> Consider . . . a person who uses nanotech drug-delivery techniques to apply a very targeted poison in committing a murder. . . .[118]

The two sections below address distinct aspects of our inquiry into nanocrime: The first examines technology-facilitated crime as an empirical phenomenon: Part III.A.1 reviews the evolution of cybercrime; Part III.A.2 examines how nanotechnology could be used to facilitate the commission of various crimes. Part III.A.2 utilizes principles of criminal law in assessing the potential for various types of nanocrime to manifest themselves. Part III.B analyzes the extent to which our experience with cybercrime should structure our response to nanocrime, if and when such a response becomes necessary.

Before we take up those issues, I need to outline the conceptual framework that will structure our inquiries. It was developed as a tool for analyzing cybercrime—crimes the commission of which involves the use of computer technology.[119] While the framework was created for the specific purpose of analyzing computer-facilitated crimes, it can also be used to analyze how other technologies facilitate crimes. The framework can be generalized because it is designed to identify the role a particular technology plays in various types of criminal activity; the analysis that results from applying the framework to computer technology probably cannot be extrapolated to the nanotechnology context, but I see no reason why the basic structure of that analysis cannot. The goal in both instances is to assess (i) how a technology can be used to facilitate the commission of crimes and (ii) how, if at all, law should address the contributions the technology makes.

The framework divides cybercrimes into three categories: (i) a computer

---

4, 1978, ("IBM has been making . . . rapid progress on a revolutionary computer brain . . . ."). Compare these sources with *supra* notes 14–16 & accompanying text (putting nanotechnology in much the same terms).

117. *See supra* note 67 & accompanying text (discussing the threat that oversight could miss unforeseen risks).

118. Boucher, *supra* note 1, at 219.

119. *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659, 660 (2005) (defining cybercrime).

is the target of the crime; (ii) a computer is a tool that is used to commit a traditional crime such as theft or fraud; and (iii) a computer plays an incidental role in committing one or more crimes.[120] Each category is described below.[121]

A computer is the *target* of criminal activity when the perpetrator attacks the computer by breaking into it, introducing code that damages it or bombarding it with data.[122] Cybercrimes that involve breaking into a computer involve accessing a computer without being authorized to do so (outsider crime) or by exceeding the scope of one's authorized access to a computer (insider crime). Access can be an end in itself or it can be used to commit another crime (e.g., damaging or stealing data from a computer). Code target crimes involve creating, disseminating and using malware:[123] viruses, worms and other malicious code that damages a computer system or extracts data from it. The final type of target crime involves blasting a computer linked to the Internet with so much data it essentially goes offline in what is known as a distributed denial of service (DDoS) attack; the computer receives so many malicious signals from the attacker that no legitimate traffic can reach it.[124]

---

120. *See* Susan W. Brenner, *Defining Cybercrime: A Review of State and Federal Law*, *in* CYBERCRIME: THE INVESTIGATION, PROSECUTION AND DEFENSE OF A COMPUTER-RELATED CRIME 12–16 (Ralph D. Clifford ed., 2001) [hereinafter Brenner III] (discussing the categories of cybercrime). The cybercrime framework seems to have been developed by attorneys for the U.S. Department of Justice. *See, e.g.*, Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 934 (1996) (discussing the Department of Justice's Computer Crime Initiative); Scott Charney, The *Justice Department Responds to the Growing Threat of Computer Crime*, 8 COMPUTER SECURITY J. 1–12 (Fall 1992) (describing an example of how the cybercrime framework seems to have been developed by attorneys for the U.S. Department of Justice).

121. The description of the three categories is taken from Brenner III, *supra* note 120, at 12–16 (citations omitted). For a more detailed discussion of the categories, *see*, BRENNER I, *supra* note 7, at 39–47.

122. The computer's role is, in a sense, the "victim" of the crime.

123. *See* Robert Moir, *Defining Malware: FAQ*, MICROSOFT (last visited Feb. 22, 2011), http://technet.microsoft.com/en-us/library/dd632948.aspx (describing that malware "is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, et al."). As Wikipedia explains, the term "malware" encompasses various types of computer code:

> Malware, short for *malicious software*, is software designed to infiltrate a computer system without the owner's . . . consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term 'computer virus' is sometimes used as a catch-all phrase to include all types of malware . . . . Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, crimeware, most rootkits and other malicious and unwanted software.

Malware, WIKIPEDIA, http://en.wikipedia.org/wiki/Malware (last visited Feb. 7, 2011). Some of the laws criminalizing malware refer to it as a "computer contaminant." *See, e.g.*, Ari. Rev. Stat. § 13-2301(E)(4) (defining computer contaminant as "any set of computer instructions that is designed to modify, damage, destroy, record or transmit information within a computer"); NEV. REV. STAT. § 205.4737 (defining computer contaminant, in part, as "any data . . . that is designed or has the capability" to "[c]ontaminate, corrupt, . . . destroy, disrupt, modify [or] record" other data). *See also* Fla. Stat. Ann. § 815.03(3); N.H. REV. STAT. § 638:16(IV); TENN. CODE ANN. § 39-14-601(4) (defining computer contaminant as any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the authorization of the owner of the information).

124. CNET News.com Staff, *How a 'denial of service attack' works*, CNET NEWS (Feb. 9, 2000, 4:00 PM), http://news.cnet.com/2100-1017-236728.html. *See also Denial-of-Service Attack*, WIKIPEDIA, http://en.wikipedia.org/wiki/Denial_of_service_attack (last visited Feb. 22, 2011).

> A . . . distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. . . . [I]t generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. . . .

A computer can also be a *too*l used to commit a traditional crime, such as theft or fraud; here, the computer's role is analogous to the role a telephone plays when a fraudster uses it to trick victims into parting with their money or property. In both instances, the use of a particular technology facilitates the commission of the crime but does not alter the nature of the offense. Computers can be used to commit most of traditional crimes, including fraud, embezzlement, theft, arson, forgery, riot, assault, rape and homicide.[125]

Finally, a computer can play an *incidental* role in the commission of a crime. This encompasses a variety of activity, such as a blackmailer's using a computer to email his victim and a drug dealer's using a computer and Excel to track his inventory and drug transactions. In these and similar instances the computer's role in the crime is as a source of evidence, nothing more. That role, however, can be important; computers can, in effect, become the crime scene. The evidence investigators find on the drug dealer's computer may play an essential role in convicting him of his crimes.

This trichotomy plays two roles in analyzing cybercrimes: Investigators use it to assess how they should draft search warrants and otherwise incorporate computer technology into their investigative process. Lawyers and legislators use it to determine if existing law is adequate to criminalize how a computer was used in a given instance; if it is not, then courts or legislators may need to extend the reach of existing law or adopt new law.[126]

The sections below use the trichotomy for two related purposes: The first section uses it to order our analysis of the ways in which nanotechnology could be used to facilitate criminal activity; this discussion focuses on the technology's role in facilitating existing types of criminal activity and in facilitating new types of criminal activity. The next section uses the trichotomy to order a parallel analysis of the extent to which these criminal uses of nanotechnology can be addressed with existing criminal law or will require modifying existing law or adopting new law.

> One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. . . .

Id. As I have explained elsewhere, DDoS attacks constitute a "new" crime. *See* Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1, at 73–76 (2001) [hereinafter Brenner IV] (requiring the adoption of new, DDoS-specific laws since they are a new crime and noting that statutes criminalizing DDoS attacks focus on denying access to a computer). *See, e.g.*, N.C. GEN. STAT. ANN. § 14-456 (defining that it is a crime to "willfully and without authorization" cause the denial of computer or network services by launching DDoS attack); 18 PA. CONS. STAT. ANN. § 7612 (defining that it is a crime to knowingly launch a DDoS attack that is designed to "block, impede or deny" access to a computer). For the federal DDoS provision, *see* 18 U.S.C § 1030(a)(5)(A) (defining fraud and related activity in connection with computers).

125. For what I mean by "traditional crimes," see, for example, Susan W. Brenner, *Fantasy Crime: The Role of Criminal Law in Virtual Worlds*, 11 VAND. J. ENT. & TECH. L. 1, 7–8 (2008) [hereinafter Brenner V]. For a listing of offenses that qualify as traditional crimes, *see, e.g.*, 4 WILLIAM BLACKSTONE, COMMENTARIES, Chapters IV-XVII. For an expanded list of mostly traditional crimes, *see, e.g.*, ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW xvii–xxvii (3d ed. 1982).

126. *See infra* Part III(B) (discussing lessons learned from technology and crime).

A. Analogy

As I noted at the beginning of this article, any discussion of nanocrime is speculative because nanocrime is a phenomenon that apparently has yet to manifest itself.[127] As I also noted, I believe the explanation for its failure to appear to this point lies in what will emerge as an analogy between the rise of cybercrime and the eventual rise of nanocrime.[128] I trace the rise of cybercrime in Part III.A.1, below; in Part III.A.2, I use our experience with cybercrime as the basis for speculating about how nanotechnology will be used to facilitate criminal activity.

1. Cybercrimes

If it is permissible to analogize something that does not exist to something that has existed for years, then I believe nanocrime can be analogized to cybercrime. Both involve (or, more properly, one involves and one will involve) exploiting a technology for unlawful ends. Criminal exploitation of technology is not a new phenomenon; in a study done several years ago, professors at the Naval Postgraduate School found that historically the "bad guys" are among the first adopters of a new technology, at least once the technology becomes publicly available.[129]

Unlike many technologies, personal computers and, ultimately, nanotechnology are "democratic" technologies: though each began as a "laboratory" technology that was used exclusively by specialists, each evolved (or, in the case of nanotechnology, will evolve) into a technology used by "consumers," i.e., the general public.[130] The egalitarian aspect of the technologies makes them more accessible to criminals and more attractive as criminal tools.

To understand why that is true, we need only to compare computer technology with nuclear technology. Nuclear technology has never been a "democratic" technology; its use for civil and military purposes has been highly regulated and access to nuclear materials has been highly controlled.[131] The inaccessibility of the technology has so far prevented criminal (and/or terrorist) use of nuclear materials.[132] Even if the materials were available,

127. *See supra* note 5 and accompanying text (discussing the term nanocrime).

128. *See supra* Part I (introducing the topic of nanocrime).

129. *See* NATIONAL DEFENSE RESEARCH INSTITUTE, NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME, AND MILITANCY 313 (John Arquilla & David Ronfeldt eds., RAND 2001) (stating the possibility that bad guys have an easier time utilizing cutting edge innovations).

130. *See* BRENNER II, *supra* note 11, at 75–121 (discussing nanotechnology as a "democratic" technology).

131. *See, e.g.*, *Promoting Nuclear Security — IAEA Action Against Terrorism*, INT'L ATOMIC ENERGY AGENCY (June 1, 2004), http://www.iaea.org/NewsCenter/Features/NuclearSecurity/terrorism.html (discussing a global plan to fight nuclear terrorism). *See also* Rohan Perera, *International Convention for the Suppression of Acts of Nuclear Terrorism*, UNITED NATIONS AUDIOVISUAL LIBRARY OF INT'L LAW (Apr. 13, 2005), http://untreaty.un.org/cod/avl/ha/icsant/icsant.html (outlining the suppression of nuclear terrorism).

132. Other factors also frustrate criminal and/or terrorist use of nuclear material. *See, e.g.*, Pam Benson, *Official: Terrorists Seek Nuclear Material But Lack Ability to Use It*, CNN (Apr. 13, 2010, 10:00 AM), http://www.cnn.com/2010/US/04/13/nuclear.terrorists/index.html (discussing factors that prevent terrorist use

criminals might not find them a particularly attractive criminal tool, since there is little profit in mass destruction and most crime is committed for financial gain or out of passion.[133]

This does not mean that nuclear technology can never become a tool of criminal activity. Criminals could use nuclear materials in extortion plots, threatening to destroy life and property unless they were paid what they demanded; they could also steal nuclear materials and hold them for ransom.[134] The use of the technology in these scenarios, however, is purely indirect; the nuclear material is not being utilized as a technology but rather as a generic item of value that can be exchanged for money. Terrorists, on the other hand, are very likely to exploit the technology as a technology. Terrorism is ideologically motivated crime and, as such, finds utility in death and destruction.[135] Terrorists see nuclear technology as a useful way to pursue their goals; it would allow them to pursue death and destruction on a scale exceeding that which they have so far attained.[136]

My point is that even if nuclear materials were more accessible than they currently are, the extent to which they would be exploited for criminal purposes would be limited, and probably specialized. Criminals are likely to approach nuclear materials as a commodity they can exploit for profit; terrorists are likely to approach them as engines of surpassing destruction. Both are the equivalent of using networked computers to send emails planning a physical bank robbery, rather than using them to hack bank computers and transfer funds to offshore accounts.[137]

Now, contrast nuclear technology with two well-established "democratic" technologies: motor vehicles and personal computers. In the 1930s, bank robbers and other criminals used motor vehicles to avoid being apprehended after they had committed a crime.[138] The criminals tended to have faster

---

of nuclear material).

133. *See, e.g.*, Kirk W. Munroe, *Surviving the Solution: The Extraterritorial Reach of the United States*, 14 DICK. J. INT'L L. 505, 513 (1996) (noting the "pecuniary motives of most crimes"). *See also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1, 57 n.331 (2004) [hereinafter Brenner VI] (discussing the motives of crimes).

134. *See, e.g.*, *A First: Criminals Steal Nuclear Material, Than Demand Ransom for Its Return*, HOMELAND SECURITY NEWSWIRE (Oct. 17, 2009), http://homelandsecuritynewswire.com/first-criminals-steal-nuclear-material-demand-ransom-its-return (noting that Argentinian criminals stole radioactive material in an extortion plot). Criminals could also acquire nuclear materials and sell them to terrorists or others who wanted them for various uses. Benson, *supra* note 132.

135. *See, e.g.*, 18 U.S.C. § 2332b(g)(5)(B) (listing the destructive acts that constitute the federal crime of terrorism). *See also* Leonie Huddy et al., *Fear and Terrorism: Psychological Reactions to 9/11*, *in* FRAMING TERRORISM: THE NEWS MEDIA, THE GOVERNMENT, AND THE PUBLIC 255, 255 (Pippa Norris et al. eds., 2003).

136. *See, e.g.*, Inal Ersan, *Al Qaeda Says Would Use Pakistani Nuclear Weapons*, REUTERS (June 22, 2009, 2:39 AM), http://in.reuters.com/article/worldNews/idINIndia-40495320090621 (detailing the remarks of an Al-Qaeda leader who wishes to use nuclear weapons in an attack on the United States).

137. *E.g.*, John Leyden, *Kentucky Payroll Phishing Scam Nets Small Fortune*, THE REGISTER (July 3, 2009), http://www.theregister.co.uk/2009/07/03/kentucky_payroll_phishing_scam/ (reporting on a phishing scam where criminals made off with $415,000). In other words, neither criminals nor terrorists are likely to exploit the distinctive aspects of nuclear technology as a technology, aside from its exceptional qualities as an engine of destruction.

138. *See, e.g.*, SUSAN W. BRENNER, CYBERTHREATS: EMERGING FAULT LINES OF THE NATION STATE 25–28 (Oxford University Press 2009) (discussing the problems novel use of automotive technology posed to law enforcement in the early part of the 1900s).

automobiles than the police, and were adept at using those vehicles to cross jurisdictional borders and otherwise evade capture by the police.[139] Motor vehicles were readily accessible to criminals as well as to law-abiding citizens, and their general availability meant that the skills needed to operate them were effectively in the public domain; i.e., most people knew or could easily learn how to drive a car. Their unique value as criminal tools lay in the extent to which they facilitated escape, but auto theft also became a new and serious crime during this era.[140] The former exploited the distinct capabilities of automotive technology as a technology; the latter simply approached automobiles as a generic item possessing value.

Something similar to criminals' use of automotive technology occurred with computer technology, though its migration into the public and criminal spheres took decades.[141] The first published reports of computers being used to commit crimes appeared in the 1960's, when computers were large mainframe systems.[142] The history of modern computing dates back to the nineteenth century, but the development of the mainframe business computer did not begin until after World War II.[143] In 1946, several companies began working on a commercial mainframe, and by 1951 the UNIVAC, created by the company of the same name, was being used by the Census Bureau.[144] In 1951, CBS used a UNIVAC to predict the outcome of the presidential election, which popularized the new technology.[145] By 1960, 5,000 mainframes were in use in the United States; by 1970, almost 80,000 were in use in the United States and another 50,000 were in use abroad.[146] Given the tremendous increase in the number of computers, it is not surprising that computer crime began to become an issue in the 1960s.

Computer crime in the 1960s and 1970s was very different from the

139. *Id.* at 25–26.

140. *See, e.g.*, Brooks v. United States, 267 U.S. 432, 438 (1925) ("Elaborately organized conspiracies for the theft of automobiles and the spiriting them away into some other state . . . have roused Congress to devise some method for defeating the success of these widely spread schemes of larceny.").

141. BRENNER I, *supra* note 7, at 9–37 (describing the evolution of cybercrime).

142. ULRICH SIEBER, LEGAL ASPECTS OF COMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY 19 (1998). *See also* DONN B. PARKER, CRIME BY COMPUTER x–xi (Charles Scribner's Sons 1976) (discussing the beginnings of the study of computer crime and "computer abuse."). I suspect, but cannot confirm, that computer crime was occurring as far back as the 1940s, when mainframes were used only in laboratories and other research facilities.

I base that suspicion on the fact that mainframe crime was manifesting itself in the 1950s and was becoming a serious problem by the 1960s and 1970s. I imagine mainframe crime in the 1940s was very limited and probably took the form of minor harassment, e.g., deleting or altering data stored in or being entered into a mainframe for analysis. I infer that from the modest capabilities of the early mainframes; as I note later in the text above, even the evolved mainframes in use by the1960s had what we would consider minimal capacities for criminal exploitation. My speculation about computer crime in the 1940s is likely to remain just that; as I note later in the text, the 1960s and 1970s victims of computer crimes often did not report their victimization to the authorities because they were concerned about negative publicity. I suspect that my hypothesized victims of 1940s computer crime did not report their victimization to the authorities because the incidents were trivial and because the concept of "computer crime" had not yet been created.

143. *See, e.g.*, CAMPBELL-KELLY & ASPRAY, *supra* note 24, at 106–07 (Basic Books 1996) (describing the entry of new firms into the burgeoning computer industry in the late 1940s and early 1950s).

144. *See id.* at 117–21 (describing the development of the UNIVAC computer).

145. *Id.* at 121–23.

146. *Id.* at 130.

cybercrime we deal with today. There was no Internet, and mainframes were not networked to other computers. In 1960, a typical mainframe cost several million dollars, needed an entire room to house it and a special air conditioning system to keep its vacuum tubes from overheating and frying the data it stored.[147] Only select researchers were allowed to use a mainframe.[148] To access a mainframe, a researcher gave the data he wanted the computer to analyze to a keypunch operator, who used a machine to punch holes in cards; the holes encoded the data into a form the mainframe could read.[149] The keypunch operator then gave the cards to another operator, who fed them into a machine that transmitted the information to the mainframe for processing; the researcher would eventually receive a printout showing the machine's analysis of his data.[150]

Because mainframes were not networked and the only way to access one was by using this cumbersome process, only a few people were in a position to commit computer crime.[151] This limited the type and amount of crimes that were committed in this era. Insiders might spy on other employees by reading their confidential files; and they might sabotage a computer or the data it contained as retaliation for being fired or disciplined.[152] These crimes occurred, but the most common type of computer crime in this era was financial; insiders used their access to a mainframe computer to enrich themselves.

For example, a California teller used his access to the bank's computer to embezzle over $100,000; instead of turning him in to the police, the bank promoted him to a higher-paying position on the condition he never explain what he did to other tellers.[153] Bank employees were not the only insiders committing computer crimes in the 1960s. In 1964, executives of Equity Funding Corp., an insurance company, began using the company's computers to inflate its earnings.[154] At first, they simply entered false commission income—eventually totaling $85 million—into the computerized accounting system. Since blatant false entries were relatively risky, they later moved to a different approach: showing the company had sold more policies than it actually had. When the scheme collapsed in 1973, Equity computers said the

147. STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 19 (Dell 1984).

148. *Id.* at 18–25.

149. *See* BRENNER I, *supra* note 7, at 11 (describing the development of mainframe computers).

150. *Id.*

151. *See* Mark D. Rasch, *Criminal Law and the Internet*, *in* THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES ch. 11, § II (The Computer Law Association, Inc. 1996), *available at* http://www.swiss.ai.mit.edu/6805/articles/computer-crime/rasch-criminal-law.html (describing the problems in prosecuting computer crimes under the common law before the development of computer crime laws).

152. *See* GERALD MCKNIGHT, COMPUTER CRIME, 97–112 (Walker and Company 1973), for an account of some computer sabotage cases from this era. *See also id.* at 114–18 (describing a case in which the employees of a company's computer department successfully extorted higher salaries by subtly threatening to erode the computer's performance).

153. David Pauly et al., *Crime in the Suites: On the Rise*, NEWSWEEK, Dec. 3, 1979, at 114. *See also* Allan J. Mayer, *The Computer Bandits*, NEWSWEEK, Aug. 9, 1976, at 58 (describing how law enforcement deals with white-collar computer crimes).

154. *See* PARKER, *supra* note 142, at 118–74 (describing the Equity Funding Corporation of America fraud in detail).

company had sold 97,000 insurance policies, but it had actually sold less than 33,000. Federal investigators said two thirds—or 2 billion dollars' worth—of the insurance the company claimed to have written was fraudulent.[155] After the fraud was discovered, Equity went bankrupt—in what was then the second largest bankruptcy ever—and 22 of its officers and employees were convicted on federal criminal charges.[156]

While embezzlement and fraud were the most common crimes, employees found other ways to profit from their access to a mainframe. Some stole information and sold it; they usually took trade secrets, but in one case employees of the Drug Enforcement Administration stole the names of informants and information about pending investigations and sold it to drug dealers.[157] Other employees had their company's mainframe issue phony payroll checks to nonexistent employees, which the employees, of course, cashed.[158] Another, less common tactic was to misappropriate company data and hold it for ransom.[159]

The computer crimes committed in this era all had one thing in common: the victims were a company or government agency because large entities were the only ones who used mainframe computers. Also, mainframes were generally incapable of inflicting "harm" on an individual; it might have been possible for an insider to manipulate mainframe data to fire someone improperly, but that would have been a very risky crime. The victim would probably complain, triggering an inquiry that could lead to the unraveling of this scheme and any others in which the perpetrator was involved. Using computers to "harm" individuals did not become a problem until the 1980s, when the "personal computer" and the Internet appeared.[160]

The serendipitous introduction of those innovations at around the same time transformed computer technology from a "laboratory" technology into a "democratic" technology.[161] More and more people began using computers and as a result, computer-facilitated crime increased in incidence and in

155. *See* Donald C. Bacon, *New American Way of Life*, U.S. NEWS & WORLD REP., May 31, 1976, at 29 (reporting on white-collar crimes in the U.S.).

156. *Id*.

157. United States v. Lambert, 446 F. Supp. 890, 890 (D. Conn. 1978).

158. *See, e.g.*, Donald L. Adams, *"The Nagging Feeling" of Undetected Fraud,* U.S. NEWS & WORLD REP., Dec. 19, 1977, at 42 (discussing junior accountant at small firm who enriched himself by having a computer issue checks to fictitious employees, which he cashed himself).

159. *See, e.g.*, Bernard D. Nossiter, *Scotland Yard Deprograms Great Computer Tape Heist*, WASH. POST, Jan. 14, 1977, at A15 (discussing man who stole computer tapes from company and demanded half a million dollars for their return).

160. *See* BRENNER I, *supra* note 7, at 23–37, 73–102 (discussing modern ways that computers are used to commit crimes and how that came to be).

161. As noted earlier, by the 1960s mainframe computers were no longer used exclusively in laboratories; they had migrated into the corporate and financial sectors. This limited migration did not transform computer technology into a "democratic" technology; computers were still used exclusively by specially-trained employees whose only legitimate role was to utilize the mainframe for specific tasks authorized by their employers. At the time, some thought the lack of access to computer technology coupled with the "power" computers exercised over workers and others might lead to widespread violence against them. *See, e.g.*, MCKNIGHT, *supra* note 152, at 97–112 ("revolt against the machine"). The possibility of that scenario's being realized ended, of course, with the emergence of the personal computer.

complexity.[162]

In the 1960s and 1970s (and perhaps earlier), computer crime was a relatively simple phenomenon: mainframes were used as tools to commit traditional crimes such as fraud, embezzlement, extortion and the theft of information and/or trade secrets.[163] Computer crime was therefore limited to a basic (albeit often profitable) set of tool crimes. Target crimes do not seem to have existed in this era; there are no reported instances of a mainframe's being used to damage itself and since mainframes were not networked, there was no way one mainframe could be used to damage another.[164] These early tool crimes did implicate the third category in the trichotomy outlined earlier; investigators used the mainframe involved in such a crime as a source of evidence to be used in identifying and prosecuting the perpetrator(s).[165]

The demise of the mainframe began in 1971 with the invention of the microprocessor, which dramatically decreased the size and cost of computers.[166] It was not until 1975 that the first microprocessor-based computer—the Altair 8800—made its debut on the cover of *Popular Electronics*."[167] The Altair was a primitive device but it generated interest in personal computers; hundreds of companies sprang up to customize the Altair or market their own versions.[168] In 1976, Steve Jobs and Stephen Wozniak created the Apple II.[169] Their competitors were focused on creating products for computer enthusiasts,[170] but Jobs realized a computer could be a popular consumer product if it were appropriately packaged:

> [T]he microcomputer would have to be . . . a self-contained unit in a plastic case, able to be plugged into a standard household outlet . . . ; it would need a keyboard to enter data, a screen to view the results of a computation, and some form of . . . storage to hold data and programs . . . . [T]he machine would need software . . . .[171]

Commodore Business Machines adopted a similar strategy and in 1977, when the Apple II and Commodore PET went on the market, both "were instant hits" with the public.[172] The expanded variety of software that was available by 1980 further increased interest in personal computers, as did IBM's

---

162. *See* BRENNER I, *supra* note 7, at 23–37, 73–102 (discussing the development of computer facilitated crimes phone phreaking, casino hacking, identity theft).

163. *See supra* text accompanying notes 153–159 (discussing computer crimes in the 1960s and 1970s).

164. In the early 1970s, there were a few attempts to sabotage mainframes; they met with varying degrees of success and were the product of varying motives, some personal, some political. MCKNIGHT, *supra* note 152, at 83–108.

165. *See, e.g.*, AUGUST BEQUAI, COMPUTER CRIME 22–23 (1978) (suggesting manner in which investigators should investigate security breaches).

166. *See* CAMPBELL-KELLY & ASPRAY, *supra* note 24, at 229 (stating that the microprocessor was invented in 1971).

167. *Id*. at 240.

168. *See id.* at 240–44 (discussing shortcomings of Altair 8800 and how, despite those shortcomings, it sparked substantial interest in personal computers).

169. *Id.* at 246–47.

170. *See id.* at 237–44 (discussing early computer hobbyists).

171. *Id.* at 246.

172. *Id.* at 247.

introduction of its Personal Computer in 1981.[173]

The popularization of computers took a huge step forward with the rise of the Internet.[174] Its precursor—the ARPANET—went online in 1969 but the ARPANET "did not interact easily with . . . networks that did not share its [networking] protocol."[175] The Internet, as such, began in 1983, when the ARPANET protocol was changed to TCP/IP.[176] The World Wide Web—a "system of interlinked hypertext documents accessed via the Internet"—went online in 1991.[177] The first graphical web browser, Mosaic, went online in 1993 and vastly increased use of the Internet.[178]

As anyone who has seen the 1983 film *War Games*[179] knows, networked computer crime (or cybercrime) had emerged long before 1993. The movie depicts what happens when David Lightman "hacks" his way into WOPR, a NORAD supercomputer, and starts a game of "global thermonuclear" war with the computer.[180] The concepts of "hacking" and "hackers" were so new in the early 1980s that the film was originally conceived very differently—as involving a relationship between a genius and an adolescent boy.[181] But once the screenwriter met a researcher at the Stanford Research Institute, and learned about the "new subculture of extremely bright kids" who were

173. *See id.* at 248–57 (discussing "the reemergence of IBM" and the popularity of software such as VisiCalc).

174. *See Computer*, WIKIPEDIA, http://en.wikipedia.org/wiki/Computer (last visited Feb. 22, 2011) (claiming that "[w]ith the evolution of the Internet, personal computers are becoming as common as the television and the telephone in the household"); Anja Emerson, *How the Internet has made the World a Smaller Place*, HELIUM (Aug. 8, 2009) http://www.helium.com/items/1545634-how-the-internet-has-made-the-world-a-smaller-place (discussing generally the impact the Internet has had on computers and people's lives). "The Internet . . . is the publicly available worldwide system of interconnected computer networks that transmit data by packet switching using a standardized Internet Protocol (IP) and many other protocols." *History of the Internet*, EDINFORMATICS, http://www.edinformatics.com/inventions_inventors/internet.htm (last visited Feb. 22, 2011).

175. *History of the Internet*, *supra* note 174.

176. *Id.*

177. *World Wide Web*, WIKIPEDIA, http://en.wikipedia.org/wiki/World_wide_web (last visited Feb. 22, 2011). *See Web Architecture*, W3C, http://www.w3.org/standards/webarch/ (last visited Feb. 22, 2011) (describing the general architecture of the Web).

178. *Internet*, WIKIPEDIA, http://en.wikipedia.org/wiki/Internet (last visited Feb. 22, 2011); *Mosaic (Web Browser)*, WIKIPEDIA, http://en.wikipedia.org/wiki/Mosaic_%28web_browser%29 (last visited Feb. 22, 2011); *Mosaic Web Browser History*, LIVINGINTERNET.COM, http://www.livinginternet.com/w/wi_mosaic.htm (last visited Feb. 22, 2011).

179. WARGAMES (Metero-Goldwyn-Mayer 1983), *See also WarGames*, WIKIPEDIA, http://en.wikipedia.org/wiki/WarGames (last visited Feb. 22, 2011) (describing a movie where "a young hacker . . . unwittingly accesses . . . a United States military supercomputer"); *WarGames*, IMDB, http://www.imdb.com/title/tt0086567/ (last visited Feb. 22, 2011) (same).

180. *WarGames*, WIKIPEDIA, http://en.wikipedia.org/wiki/WarGames (last visited Feb. 22, 2011); *WarGames*, IMDB, http://www.imdb.com/title/tt0086567/ (last visited Feb. 22, 2011). For definitions of hacking and hacker, see, e.g., *Hacker (Computer Security)*, WIKIPEDIA, http://en.wikipedia.org/wiki/Hacker_%28computer_security%29 (last visited Feb. 22, 2011) ("[A] hacker is a stereotypical person who breaks into computers and computer networks, either for profit or motivated by the challenge."). Hacking is the conduct involved in breaking into a computer, and the term "hack" refers to a successful break-in. *See, e.g.*, THE CHAMBERS DICTIONARY 771–72 (2000) (defining hacking as "to use a computer with skill, especially to obtain unauthorized access to (someone else's computer files)").

181. *See* Scott Brown, *WarGames: A Look Back at the Film that Turned Geeks and Phreaks into Stars*, WIRED (July 21, 2008), http://www.wired.com/entertainment/hollywood/magazine/16-08/ff_wargames?currentPage=all (stating that the original concept of the movie had nothing to do with technology).

becoming hackers, the movie shifted focus to deal with this new phenomenon.[182]

War Games brought hacking—which was already popular in certain circles—into the popular consciousness.[183] As a 1983 *New York Times* article explained, the number of "young people roaming without authorization through" the country's computers was in the thousands and growing "with the boom in personal computers."[184] The article also noted that the "hackers" were also using the electronic bulletin boards that were a precursor of the Internet.[185]

War Games-style cybercrime—breaking into computers to satisfy one's curiosity and perhaps play a prank—was the dominant mode of computer crime over the next few years.[186] It survived into the 1990s, but by then adults had essentially taken over cybercrime. Adults had realized computer crime could be a profitable endeavor; the Internet was beginning to link everything, which meant the new cybercriminals had thousands, and eventually millions, of targets. Most organizations were not aware of the need to secure their systems, so most of the targets were easy pickings for even a semi-talented cybercriminal. This led to an explosion in tool crimes—primarily in financially motivated tool crimes. The difference between these tool crimes and mainframe tool crimes was that the cyber-tool crimes were committed in a wholly unbounded context; anyone with access to the Internet could strike at a target across the street or halfway around the world. That created additional incentives to commit financial tool crimes; a clever cybercriminal could attack a target, make a profit and stand very little chance of being apprehended (unlike the insiders who committed mainframe tool crimes).

Financial tool cybercrimes—online theft, fraud, extortion, embezzlement, forgery and identity theft—exploded. By the mid-1990s, financial tool cybercrimes were increasingly the province of adults; by the twenty-first century, they were increasingly the province of organized criminal groups. The democratization of computer technology created vast new opportunities for those willing to break the law for financial gain; in so doing, it may have induced people to commit crimes who might otherwise not have done so.[187]

The democratization of computer technology also created new opportunities for other types of criminal activity. Child pornography, which had been a relatively insignificant crime prior to the Internet, exploded online; those who would never have been willing to seek out child pornography in the physical world found they could easily, and anonymously, acquire it online, which reduced their risk of being identified and prosecuted. The production, distribution and possession of child pornography became another popular tool

182. *Id.*

183. *See id.* ("[*War Games*] introduced the world to the peril posed by hackers.").

184. Joseph B. Treaster, *Hundreds of Youths Trading Data on Computer Break-Ins*, N.Y. TIMES, Sept. 5, 1983, at 1.

185. *Id.* at 34. *See also* THE BBS CORNER (last updated Mar. 7, 2010), http://www.bbscorner.com (describing the technology that early hackers used to communicate).

186. The description in the following paragraphs of how cybercrime evolved from the 1980s to the twenty-first century is taken from BRENNER I, *supra* note 7, at 9–37.

187. S*ee id.* at 9–37, 73–102 (providing a more detailed description of the evolution of tool crimes).

cybercrime. Child pornography is a tool cybercrime that mixes financial and non-financial motives; there are, and have long been, websites that sell child pornography, but there are also sites where it is traded for free.[188]

The democratization of computer technology also made it easier for individuals to inflict "harms" of varying types—usually non-physical—on each other. Online stalking, harassment, bullying, defamation, imposture and invasion of privacy became increasingly common. The commission of most of these crimes was relatively unusual prior to the rise of the Internet; these personal "harm" tool crimes exploded online because it became possible to inflict any or all of the "harms" they encompass with relatively little risk of being identified and prosecuted. Those who stalked or harassed others in the physical world were likely to be prosecuted; those who do so online have a good chance of facing no consequences for their actions. The crimes in this category are also tool cybercrimes.

Tool cybercrimes are probably the most commonly committed types of cybercrime, perhaps because there are so many types of tool cybercrimes. As I have noted elsewhere, I believe all the traditional crimes except for rape and bigamy can be committed online;[189] we so far do not have a documented case in which the Internet was used to commit murder, but we have a case in which that may have been the perpetrator's goal.[190] And it is reasonable to assume that the Internet could, under certain circumstances, be used to commit the ultimate crime.[191]

Target crimes—attacks on a computer—have grown in frequency and complexity. People still hack computer systems, though today they are more likely to do so as part of a scheme to commit some other crime, such as identity theft or extortion.[192] The newer target crimes—creating and disseminating malware and launching distributed denial of service (DDoS) attacks—are increasingly common and are often committed as part of a scheme to carry out a tool crime. The democratization of computer technology has

188. On a related note, the Internet effectively created the new crime of "luring" a child for the purposes of having sexual activity. *See, e.g.*, Susan Hanley Duncan, *MySpace Is Also Their Space: Ideas for Keeping Children Safe from Sexual Predators on Social-Networking Sites*, 96 KY. L. J. 527, 527–28 (2007–2008) (discussing the effects of social-networking sites on the ability of child predators to attract victims); Kurt Eichenwald, *From Their Own Online World, Pedophiles Extend Their Reach*, N.Y. TIMES, Aug. 21, 2006, at A1, *available at* http://www.nytimes.com/2006/08/21/world/americas/21iht-web.0821porn.2548212.html (explaining how social-networking sites have evolved from permitting the exchange of child pornography to facilitating real-life child predation).

189. Brenner IV, *supra* note 124, at 110–14. This does not mean that a rape cannot be solicited or arranged via the Internet. It certainly can. *See, e.g.*, William Browning, *Internet "rape fantasy" case moves closer to trial*, BILLINGS GAZETTE (May 8, 2010, 11:00 pm), http://billingsgazette.com/news/state-and-regional/wyoming/article_2040ba76-5b19-11df-9959-001cc4c03286.html (describing a rape case based in an online solicitation). My point is that neither rape nor bigamy—at least as they have been traditionally defined by criminal law—can actually be carried out via computer technology. If we decide to change how we define either or both crimes, so they then encompass virtual activity, then these crimes, too, could be carried out via cyberspace.

190. *See* BRENNER I, *supra* note 7, at 101–02 (describing an incident where a criminal defendant hacked into a hospital compute and changed a patient's prescription to include medicine that could have caused the patient serious harm).

191. *Id.*

192. *See id.* at 49–71 (providing more information on target crimes).

expanded the pool of those who commit target crimes; in the mainframe era, only insiders could attack a computer. Today, anyone—insider or outsider—can do so, and the attacks are more complex. Extortionists often use DDoS attacks to take a particular target—say, an online casino—offline as part of an extortion scheme; the casino operators are told that unless they pay a substantial sum (which they usually do), the attacks will continue. Malware can be used in a similar fashion but can also be used to siphon valuable information from the victim computer system. Malware and DDoS attacks can also be used to carry out a "pure" target crime, i.e., for the sole purpose of taking target computer offline.

There are many other permutations of tool and target cybercrimes, but I believe this summary illustrates how democratizing computer technology opened it up to be exploited for criminal purposes. That brings me to the third and final category in the trichotomy I outlined earlier: the computer as playing an incidental role in the commission of the crime.

This category encompasses cases in which a computer is used to commit a crime, but its use is so trivial that it does not transform the crime into a tool crime. In a tool crime, the use of the computer is integral to the commission of the crime, i.e., the crime could not have been committed when and as it was without the use of the computer. The best way to explain the difference between the two is by using examples. Assume that a blackmailer uses his home computer to write and print a blackmail letter he then mails to his victim; here, the computer played a role in the commission of this crime, but the role was so trivial this does not qualify as a tool cybercrime. The same is true in the example I noted earlier:[193] a drug dealer uses a laptop and Excel to track his purchases, sales and inventory. Here, again, the computer plays a role in the commission of the crime, but the role is too minor for this to constitute a tool cybercrime.[194]

Crimes in which the computer's role is merely incidental are included in the trichotomy because even when a computer's role is trivial, evidence of the crime will be found on the computer.[195] That is important for those who investigate cybercrime and for those who enforce the laws that limit what investigators can do in the course of investigating cybercrimes, but it is generally not important for those who adopt or interpret the legislation that defines cybercrimes. In other words, because the computer's role here is merely evidentiary, its use does not require assessing—or reassigning—how law defines a particular crime.[196]

That has often been the case with tool and target crimes; since the computer plays a significant role in the commission of these cybercrimes, those who adopt or enforce criminal statutes have often found it necessary to incorporate the computer's role in committing an offense into how the law

193. *See supra* Part III.

194. *See* BRENNER I, *supra* note 7, at 45–47 (giving further examples of the incidental role of computers in crime).

195. *See id.* at 103–19 (giving examples of the use of computers as evidentiary sources in crimes).

196. *Id.* at 45–47.

defines, and punishes, that crime. That may necessitate revising existing law or adopting new, cybercrime-specific law. Stalking statutes, for example, had to be revised to encompass online stalking because most of them were drafted in the 1980s when stalking was a purely real-world activity.[197] Statutes that defined stalking as following the victim or engaging in other activity in the real-world did not encompass the type of activity involved in online stalking,[198] which meant perpetrators could engage in that type of activity with impunity.

In the next section, we consider the possibility that nanotechnology will evolve in a fashion analogous to computer technology, i.e., that it will evolve from a "laboratory" technology into a "democratic" technology. If nanotechnology persists as a "laboratory" technology, its role in facilitating the commission of traditional and/or novel crimes is likely to be minimal, at best. If it becomes a "democratic" technology, its potential for crime facilitation is likely to be much more significant. The next section primarily focuses on the second scenario, i.e., it speculates about how nanotechnology could be used to facilitate various types of criminal activity. In focusing on those issues, it implicitly considers the likelihood that nanotechnology will move into public use and become a "democratic" technology.

2. Nanocrimes

As I noted at the beginning of this article, authors often caution that nanotechnology will become an implement of crime but they rarely, if ever, elaborate on its possibilities for such use. Since I believe nanotechnology will evolve in a fashion analogous—but not identical—to that of computer technology, I decided the best way to structure speculation into how nanotechnology could facilitate crimes of various types is to use the cybercrime framework outlined above.[199] In this section, then, we will consider the possibilities for nanotechnology target and tool crimes, as well as nanotechnology's capacity to play an incidental role in facilitating offenses.

Before we embark on that endeavor, I need to include one more prefatory observation. It is impossible at this point in time to know, or even to speculate with any degree of confidence, whether nanotechnology will actually evolve from a "laboratory" technology to a "democratic" technology. It took decades for computer technology to evolve from mainframes to personal computers; for most of that period, most never imagined computers would become a consumer product.[200] We tend to view nanotechnology in a similar fashion: we

197. *See* Susan W. Brenner & Megan Rehberg, *"Kiddie Crime"? The Utility of Criminal Law in Controlling Cyberbullying*, 8 FIRST AMEND. L. REV. 1, 15–23 (2009) (reviewing a variety of early state and federal stalking laws).

198. *See id*. at 15–23 (reviewing a variety of early state and federal stalking laws).

199. *See supra* Part III.A.1.

200. This assumption is implicit, for example, in some of the early books dealing with computer crime. *See, e.g.*, MCKNIGHT, *supra* note 152, at 98–113 (1973). It is also evidenced by the fact that "[i]t would have been technically possible to produce an affordable personal computer . . . anytime after the launch of the 4004 [microprocessor chip], in November 1971" but as we saw in the text, "it was not until nearly six years later that a . . . consumer product emerged." CAMPBELL-KELLY & ASPRAY, *supra* note 24, at 237. The influence of

are probably aware that it has for years been integrated into the manufacture of clothing and other consumer products,[201] but we tend to assume not only that it is a "laboratory" technology but that it will remain one. This may be true, or it may not. Speculating about nanotechnology's transition to a "democratic" technology at this point in time is as difficult and subject to the possibility of error as it would have been for someone accustomed to mainframe culture to speculate about a very different model of computing.

My point is that while I, personally, am confident that nanotechnology will evolve in a fashion analogous to computer technology and will eventually become an implement of criminal activity, I realize that the speculations I offer in the remainder of this section will no doubt prove inaccurate in varying respects. I am willing to assume that risk of error because, as I noted earlier,[202] I believe we have an advantage that those who experienced the rise and evolution of computer crime did not. We have seen how a "democratic" technology can be exploited for good and evil and are, therefore, on notice that nanotechnology may follow a similar course. It only seems prudent, then, to begin to consider how nanocrime might manifest itself and how the legal system should respond if and when it begins to emerge. In other words, I propose that we undertake efforts analogous to those outlined in Section II.C, i.e., I propose that we begin to analyze how criminal law can, and should, respond to the criminal exploitation of nanotechnology.

a. Target crimes

As we saw earlier, in target cybercrimes a perpetrator attacks a computer by (i) breaking into it, (ii) introducing code that damages it or (iii) bombarding it with data.[203] The strategy is to turn the technology on itself, i.e., use one computer to attack another. Logically, then, target nanocrimes should involve turning nanotechnology on itself. How might that manifest itself?

We will begin with break-ins—"hacks."[204] As I have explained elsewhere, hacking is conceptually analogous to trespass in that in both instances the perpetrator gains "entry" to a place to which he does not have lawful access.[205] All of the elements of trespass (the offender, the place being

an inclination not to move beyond mainframes is further supported by the fact that it was five years after the first personal computers appeared before IBM introduced its own version. *See supra* notes 171–173 and accompanying text. And then there is the apparently apocryphal statement attributed to IBM President Thomas Watson, for example, that there was "a world market for maybe five computers." *Thomas J. Watson*, WIKIPEDIA, http://en.wikipedia.org/wiki/Thomas_J._Watson (last visited Feb. 8, 2011). *See* Stephen J. Dubner, *Our Daily Bleg: Did I.B.M. Really See a World Market "For About Five Computers"?*, N.Y. TIMES FREAKONOMICS BLOG (Apr. 17, 2008, 10:33 AM), http://freakonomics.blogs.nytimes.com/2008/04/17/our-daily-bleg-did-ibm-really-see-a-world-market-for-about-five-computers/ (discussing the developments surrounding the authenticity of the quote).

201. *See, e.g.*, *Nanotech in Fashion: The Trend in New Fabrics*, NPR (Sept. 7, 2004), http://www.npr.org/templates/story/story.php?storyId=3892457 (describing how nanotechnology offers an alternative, revolutionizing way to process fabrics).

202. *See supra* Part I.

203. *See supra* Part III.

204. *See supra* note 180 (providing a definition of hackers and hacking).

205. *See* Brenner IV, *supra* note 124, at 81–82 (arguing that through simple modifications the four legal

trespassed upon and the means, if any, the trespasser uses to effect the unlawful entry) take place in the physical world.[206] Some of the elements of hacking (the offender, the computers involved) take place in the physical world but others arguably do not; the actual "entry" into the victimized computer does not occur in the physical world, at least not as literally as it does in a physical trespass.[207] The empirical differences between the two prompted most jurisdictions to create a new crime—"hacking"—that could be used to prosecute computer trespasses.[208]

That brings us to nanotech trespass.[209] While computer trespass deviates to some extent from physical trespass, computers are, ultimately, "places"—every computer is in effect a "box", an enclosed area. Trespassing consists of entering a "place" without authorization; while the mechanics of computer trespass deviate in certain respects from real-world trespass, the empirical analogies between the two endeavors are enough to support approaching hacking as a type of trespass.[210] Is that also likely to be true for nanotechnology?

How we answer that question probably depends on how we conceptualize nanotech hacks. I can see two options: In one, nanoparticles are the target of the attack, i.e., the trespass consists of gaining unauthorized access to one or more nanoparticles.[211] In the other option, the target is the construct of which nanoparticles are constituent entities.[212] The latter option approaches nanoparticles as the equivalent of the chips and other components that make up the computer that is hacked;[213] the first option approaches them as entities—"places" (or "computers")—in and of themselves.

I suspect these options (and, perhaps, any others that are subsequently identified) are not mutually exclusive. I suspect both may be relevant in

---

elements needed to prove trespass may also be utilized to prove hacking). If the perpetrator gains unlawful access to a place for the purpose of committing a crime once inside, then the "hack" becomes analogous to burglary. *Id.* at 84–85. The discussion in the text focuses on trespass, rather than burglary, because burglary subsumes trespass; therefore, if someone commits computer—or nanotechnology—burglary, they have also committed trespass. *See id.* at 81, 84 (defining criminal trespass and burglary).

206. *Id.* at 81.

207. *Id.* at 82.

208. *Id.* at 83.

209. Again, the discussion focuses on trespass, rather than burglary or burglary and trespass, because nanotech trespass would be subsumed by, and would be a necessary predicate for, nanotech burglary. *See id.* at 81, 84 (defining criminal trespass and burglary).

210. The trespass itself occurs in a "place," and since "places" exist in the physical world (because there is no other world), the trespass occurs in a physical "place." The conceptual differences between physical trespass and computer trespass lie in the fact that the "place" into which the hacker trespasses is not a tangible "place;" it is, instead, a digital "place" constructed from bits and bytes. No human could physically trespass in one of these digital places, which can make it difficult to determine when a computer trespass has, and has not, occurred. *See id.* at 81–82 (discussing the relationship between physical and virtual trespass).

211. *See supra* notes 51, 63 (discussing nanoparticles and nanoparticle materials); *see* discussion *supra* Part II.A (discussing target cybercrimes).

212. *See supra* notes 43–48 and accompanying text (discussing nanosystems and integrated nanosystems); *see also* discussion *supra* Part II.A (discussing target cybercrimes).

213. *See generally Computer*, WIKIPEDIA, http://en.wikipedia.org/wiki/Computer (last visited Feb. 8, 2011) (explaining the general definition, history, and functionality of computers); *see also generally "Computer"* ENCYC. BRITANNICA, http://www.britannica.com/EBchecked/topic/130429/computer (last visited Feb. 22, 2011) (discussing components of a computer).

different contexts. In some contexts, it may be reasonable to regard nanoparticles as the target(s). In others, it may be more logical to regard the construct of which they are a component as the target. To understand how the options might—or might not—apply in different contexts, we need to consider two examples.

Assume doctors inject "iron-bearing nanoparticles" into the arteries of a patient who has stents—"narrow metal scaffolds that widen a partly clogged blood vessel"—installed in certain of his blood vessels.[214] Stents are coated with a drug that prevent muscle cells from accumulating within a stent and clogging it; stents only contain one dose of the drug and its preventative effect begins to wane as time passes.[215] To address this, doctors inject nanoparticles that contain iron and a new dose of the anti-clogging drug into the patient's arteries and use magnets to drive the particles to the stents, where they recharge the anti-clogging drug.[216] After completing their mission, the biodegradable nanoparticles "break down safely" in the patient's body.[217]

Now assume that someone with the requisite expertise—Dr. X—is able to gain access to the patient after the nanoparticles have been injected but before they have been driven to the stents.[218] Dr. X injects the patient with nanoparticles that he created and that are designed to find and to infiltrate the drug-bearing nanoparticles. (In other words, each of his nanoparticles is designed to infiltrate one of the original nanoparticles.) Dr. X's motive is to establish that his nanoparticles can, in fact, invade the drug-bearing nanoparticles once they are in the patient's body; his nanoparticles are not designed to interfere with the functioning of the drug-bearing nanoparticles and/or gather information from them.[219]

This scenario is my attempt to outline a nanotechnology hack that conforms to the first option outlined above, i.e., someone trespasses on, or into, discrete nanoparticles.[220] To do that, I needed a scenario that is analogous to the scenario in which a physical trespasser walks onto someone's land or into someone's home without being authorized to do so. As I noted above, law approaches computer hacking as a derived type of physical criminal trespass; in both, the "entry" itself is the criminal act. The question is whether the scenario outlined above is sufficiently analogous either to criminal trespass or to computer hacking that it can be defined in a similar fashion, i.e., as nanotech

214. *Magnetic Fields Drive Drug-Loaded Nanoparticles to Reduce Blood Vessel Blockages in an Animal Study*, SCIENCEDAILY (May 8, 2010), http://www.sciencedaily.com/releases/2010/04/100419150821.htm.

215. *Id.*

216. *Id.*

217. *Id.*

218. I suspect this assumption is empirically incorrect, since I imagine the physicians who inject these nanoparticles would want to drive them to their intended destination stents as soon as possible. I employ this probably flawed assumption purely for the purposes of analysis.

219. I include this limitation to ensure that this scenario, and the one that follows, only involve simple hacking, i.e., only involve computer trespass. *See* Brenner IV, *supra* note124, at 84–85 (indicating that if by infiltrating the legitimate nanoparticles Dr. X's nanoparticles damaged the drug-bearing nanoparticles or extracted information from them and somehow sent the information to Dr. X, his conduct could constitute simple hacking (gaining access to a place without authorization) and aggravated hacking, or cracking (gaining access to a place without authorization to commit a crime once inside)).

220. *See supra* note 211 & accompanying text.

trespass.

I think it can: Dr. X did not himself physically enter into the drug-bearing nanoparticles (which is necessary for criminal trespass) but he gained "access" to them in a manner that is analogous to what a computer trespasser does when he hacks a computer. The computer hacker and Dr. X both use tools to penetrate a "place" that is not physically accessible to a human being.[221] Unlike a computer hacker, Dr. X has accessed a purely physical "place,"[222] albeit a minute one; like a computer hacker, Dr. X has used proxies to gain access to this otherwise inaccessible "place." Hackers use data to break into a system; Dr. X used other nanoparticles. Logically, then, Dr. X engaged in nanotechnology hacking (or trespass).[223]

Now we need an alternate scenario that exemplifies the second option outlined above.[224] Assume that doctors inject "self-assembling macromolecular particles" into someone who has cancer; after being injected, the molecules "self-assemble into complex structures" and "a new, supramolecular bomb is born."[225] Once the bomb is created, doctors irradiate it with a laser and heat it to the point at which "explosive bubbles" form; the bubbles then "burst and destroy cells in the area", including cancer cells.[226] Dr. X gains access to this patient after the bomb has been created but before it has been triggered; he injects the patient with other nanoparticles that are specifically designed to infiltrate the bomb. His goal is to establish that his nanoparticles can, in fact, invade the bomb once it has been created; and again, his nanoparticles are not designed to interfere with its functioning or gather information from it.[227]

If Dr. X commits nanotech hacking in the first scenario, it seems to follow that he also commits nanotech hacking in this second scenario. His conduct in the second scenario is empirically more analogous to that at issue in

---

221. *See* Brenner IV, *supra* note 124, at 81–82 (explaining that the "place" into which Dr. X would trespass (courtesy of his nanoparticles) is a physical "space," but its small size means that no human being could physically enter that "place.").

The fact that computer hackers and our fictional Dr. X use "tools" to gain access to a system without being authorized to do so does not transform the crime they commit from a target crime into a tool crime. The distinction between target and tool crimes is based, as I noted earlier, on the role a computer plays in a particular crime: In a target crime, the targeted computer's only role is as the "victim" of the crime, or perhaps as the scene of the crime; the hacker's goal is to gain entry to a computer, just as a trespasser's goal is to gain entry to real property. In a tool crime, the computer becomes the implement the criminal uses to commit a traditional crime, such as theft or vandalism; the focus here is on stealing or damaging property or on whatever other "harm" the tool crime encompasses.

222. *See id*. (drawing a similarity between a physical area and a virtual space).

223. *See id.* (presenting the elements that constitute computer hacking). We will assume for the purposes of analysis that the other elements of hacking are present, i.e., that Dr. X knew he was not authorized to access the drug-bearing nanoparticles and it was his purpose to do so. While Dr. X's accessing discrete nanoparticles apparently *could* be approached as a type of hacking, it might also, as I explain below, constitute another target crime—a malware crime.

224. *See supra* note 211–12 & accompanying text.

225. Levi Beckerson, *UCLA Gold Nanoparticle Structure Blows Away Cancer Cells*, DAILY TECH, (May 26, 2010), http://www.dailytech.com/UCLA+Gold+Nanoparticle+Superstructure+Blows+Away+Cancer+Cells/article18516.htm.

226. *Id*.

227. *See* Brenner IV, *supra* note 124, at 84–85 (indicating that if by infiltrating the legitimate nanoparticles Dr. X's conduct could constitute simple hacking (gaining access to a place without authorization)).

computer hacking than it was in the first scenario because here Dr. X gained access to a "structure" that was composed of discrete nanoparticles, rather than to individual nanoparticles.[228] Does that matter? If and when these issues actually arise, should law treat the two scenarios differently?

I chose the scenarios because each involves a relatively modest use of nanotechnology. The first involves what I assume is a threshold use of nanotechnology; the second involves a use that is only slightly more complex. I wanted to use scenarios that involve essentially *de minimis* uses of the technology because I believe the primary conceptual difficulty we will confront—if and when we consider criminalizing nanotech hacking—is the context in which the activity occurs. I suspect many will initially find it difficult to take the notion of sub-minuscule "trespassing" seriously; the scale on which the crime is committed may make it seem too insignificant to justify the imposition of criminal liability.[229]

To overcome that attitude, we would need to bring the "harm" nanotech hacking inflicts within the policy that justifies criminalizing trespasses in general. The "harm" criminal trespass traditionally addressed was violating someone's right to control access to and use of her real property.[230] Criminal trespass statutes continue to address that "harm", but in the latter part of the last century we extrapolated the "harm" so it also encompassed violating someone's right to control access to and use of their digital property.[231] In other words, we criminalized computer trespass.[232]

---

228. *See supra* note 213 and accompanying text (contemplating a view that considers nanoparticles as the equivalent of the chips and other components that make up the computer that is hacked).

229. *See, e.g.*, Nicholas R. Johnson, *"I Agree" to Criminal Liability: Lori Drew's Prosecution under §1030(A)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care*, 2009 U. ILL. J.L. TECH. & POL'Y 561, 587–88 (indicating that a similar attitude toward computer crime was one of the problems legislatures faced in trying to adopt computer crime legislation because "[m]ost people viewed hacking conduct as harmless" and not warranting criminal liability).

230. *See, e.g.*, WAYNE F. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 21.2 (2d ed. 2003) (discussing various aspects of criminal trespass). *See also* Commonwealth v. White, 492 A.2d 32, 36 (Pa. Super. Ct. 1985) (stating that the purpose of the trespass statute is to prevent intrusion on real property); State v. Pierce, 417 A.2d 1085, 1089 (N.J. Super. Ct. Law Div. 1980) (stating that the purpose of the trespass statute is to prevent intrusion on real property).

231. The realization that we needed to extrapolate the "harm" to the digital context evolved gradually. *See, e.g.*, William J. Broad, *Rising Use of Computer Networks Raises Issues of Security and Law*, N.Y. TIMES, Aug. 26, 1983, at A1, A15 (stating how a FBI agent noted that law needed to be updated because "under common law . . . going into someone else's home is trespass, but that's not the case with a computer"); Treaster, *supra* note 184, at A34 ("describing technological trespass by teens"). *See also* United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (stating that the witnesses' use "of the term 'intruder' to describe an unauthorized user of the computers" was appropriate in referring to the defendant "since by telephonic signal he . . . trespassed upon the physical property of OSI as effectively as if he had broken into the Rockville facility and instructed the computers from one of the terminals directly wired to the machines").

232. *See, e.g.*, *NYS Agrees on Penal Code that Makes Computer Tampering a Crime*, AM. BANKER, Apr. 16, 1984, at 23:

> Assemblyman Matthew Murphy . . . said, 'The growing presence of computers in the home and workplace has increased the possibilities for destruction of vital records, manipulation of finances, and exposure of confidential records by those who would exploit the potential for unwarranted access.
>
> 'Current law has not kept pace with technology,' he added, 'Ancient rules of criminal trespass simply do not work. . . . The new crime of computer trespass would occur when a person makes an unauthorized entry into a computer system. . . .

See also Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing*

If and when we decide it is necessary to criminalize nanotech hacking, we will need to do something similar. We will have to extrapolate the core "trespass" harm so it encompasses sub-minuscule intrusions into personal property as well as intrusions onto real property and into digital property. I suspect we will do this by extending the extrapolation we have already made, i.e., by analogizing intrusions into applications of nanotechnology to hacking. We may find this easier to do once the applications become more common, and more complex. I suspect that as nano-constructs become more complex and as we rely on them more, we will increasingly tend to regard them as analogues of the digital systems that are the targets of computer hackers.[233]

Even if we develop a law of nanotech trespass, that may not be enough. It is also quite possible that we will see nanotechnology analogues of the other target computer crimes: using malicious code (malware) to attack a computer[234] and taking a networked computer offline by bombarding it with Internet traffic (DDoS attack).[235] In analyzing the respective prospects for nano-malware and nano-DDoS attacks, I am going to use the scenarios outlined above, for two reasons. One reason is efficiency; since these scenarios provide the context and dynamics needed to analyze the remaining two target crimes, I see no reason to articulate new scenarios for the purpose of analyzing these target crimes. The other is the reason I chose the scenarios in the first place, i.e., they involve *de minimis* uses of nanotechnology. The scenarios are adequate for the purposes of analyzing the remaining target crimes; and the principles we extract in the course of that analysis can then be extrapolated to more complex uses of the technology.

We will begin with nano-malware. In both of the scenarios we examined above, Dr. X disseminated nanoparticles that infiltrated the legitimate nanoparticles that had already been injected into the patients. In both scenarios, then, Dr. X's nanoparticles had a relatively benign function; they were not designed to disable the legitimate nanoparticles or otherwise interfere with their operation in any way.[236] The only function of Dr. X's nanoparticles

---

Problem, 43 VAND. L. REV. 453, 468, 471, 476, 478–479 (1990) (explaining computer theft and distinguishing it from computer trespass).

233. Our appreciation of the extent to nanotechnology applications are analogous to digital systems may be accelerated by the anticipated intersection of computing and nanotechnology. *See, e.g.*, Jansen Ng, *Researchers Create Seven Atom Transistor, Working on Quantum Computer*, DAILY TECH (May 24, 2010), http://www.dailytech.com/Researchers+Create+Seven+Atom+Transistor+Working+on+Quantum+Computer/article18476.htm (noting that researchers are creating computer components as small as four nanometers across). *See also* James Mulroy, *Researchers Take Major Step Toward Quantum Computing*, NETWORK WORLD (May 26, 2010), http://www.networkworld.com/news/2010/052610-researchers-take-major-step-toward.html (stating researchers were able to use quantum dots to make a transistor).

234. *See supra* note 123 and accompanying text (explaining the term "malware").

235. *See supra* note 124 and accompanying text (explaining DDOS).

236. If our fictive Dr. X were later charged with nanotech hacking based on his conduct in either or both scenarios, he might argue that because his nanoparticles were designed to do no harm, he committed no crime. This was an argument early hackers (who tended to access a system out of intellectual curiosity rather than a desire to cause harm) made as to why the law should not criminalize merely accessing a computer system without being authorized to do so. *See, e.g.*, Charney & Alexander, *supra* note 120, at 954–957 (1996) (discussing the view that merely accessing a computer is still a crime). Others pointed out that even a non-malicious intruder could inadvertently damage a system while exploring it; they also noted that even if a hacker claimed to have done no harm, the owner of the system would need to take "expensive remedial

was to "access" the legitimate nanoparticles.

If we change that circumstance and assume Dr. X's nanoparticles *are* designed to have some negative effect on the legitimate nanoparticles they infiltrate,[237] then Dr. X has in effect disseminated nano-malware.[238] As noted above, statutes that criminalize malware define it in part as computer code that is designed to corrupt, destroy, or modify other computer code.[239] The cybercrime consists of knowingly disseminating or attempting to disseminate malware.[240] The nanotech version of the crime, if and when one is created, would presumably involve similar conduct and a similar mens rea. Dr. X's conduct in knowingly disseminating nanoparticles he knew would have a negative effect on the legitimate nanoparticles would therefore constitute commission of the nano-malware crime.[241]

That brings us to the third and final target crime: DDoS attacks (or nano-DDoS attacks). As noted earlier,[242] in a computer DDoS attack the attackers

---

measures" to ensure that was in fact the case. *See id.* at 954–955. The latter view ultimately prevailed, and resulted in the general criminalization of computer hacking. Johnson, *supra* note 229, at 586–588.

237. Perhaps Dr. X's nanoparticles carry the equivalent of a computer virus and release the virus once they successfully infiltrate one of the legitimate nanoparticles. Once triggered, the nano-virus prevents the legitimate nanoparticles from carrying out their intended task.

238. Depending on precisely how Dr. X's nanoparticles are intended to accomplish this, he might be held criminally liable both for gaining unauthorized access to the legitimate nanoparticles and for disseminating malware. Logically, when a cybercriminal disseminates malware and that malware infects someone's computer, the cybercriminal has both (i) "accessed" the computer without being authorized to do so and (ii) infected it with malware. *See, e.g.*, Robert J. Kroczynski, Note, *Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited?*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 817, 836 (2008) (discussing how placing malware on one's computer is enough to claim that one has affected changes on the computer).

239. *See supra* note 123 and accompanying text (defining "malware" and intrusive software).

240. *See, e.g.*, 18 U.S.C. § 1030(a)(5)(A) (2010); ARK. CODE ANN. § 5-41-202(a)(5) (West 2011); CAL. PENAL CODE § 502(c)(8) (West 2010); FLA. STAT. ANN. § 815.06(1)(e) (West 2010) (codifying the crime of knowingly disseminating malware).

241. *See supra* note 123 and accompanying text (defining "malware"). Instead of being designed to damage or destroy the legitimate nanoparticles. Dr. X's nanoparticles might be designed to extract information from them. Certain types of computer malware do precisely this. *Malware*, *supra* note 123. As noted earlier, some computer malware statutes include "recording" data in their list of negative effects associated with malware. *Id.* If Dr. X's nanoparticles were designed to record information rather than cause damage, and if the relevant nano-malware statute included recording information in its list of negative effects associated with nano-malware, then he could, again, be convicted of the crime of disseminating nano-malware.

If the jurisdiction in which this occurred defined the crime as disseminating nano-malware that actually causes harm or attempting to disseminate such malware, Dr. X would have committed the substantive nano-malware crime even if his nanoparticles did not have the desired negative effect on the legitimate nanoparticles (or if they did not succeed in infiltrating them). *See supra* note 240 and accompanying statutes. *See, e.g.*, ARK. CODE ANN. § 5-41-202(a)(5) (West 2011) (codifying that computer malware crime consists of knowingly introducing malware into a system or attempting to do so). If the jurisdiction defined the crime as only encompassing the dissemination of nano-malware that reached its target and actually caused damage, Dr. X could be charged with the completed substantive crime if his nanoparticles damaged the legitimate nanoparticles and could be charged with an attempt to commit the nano-malware crime if they for some reason failed to do so. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-2316(A)(3) (2011) (codifying that computer malware crime consists of knowingly introducing a computer contaminant into a computer or network); ARIZ. REV. STAT. ANN. § 13-1001 (2011) (defining "attempt" under Arizona law).

242. *See supra* note 124 and accompanying text (explaining a DDoS attack strategy in which the target is overwhelmed so as to render it ineffective). In an earlier article, I noted that we can analogize a DDoS "attack to using the telephone to shut down a pizza delivery business by calling the business' telephone number repeatedly, persistently and without remorse, thereby preventing any other callers from getting through to place their orders." Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J.L. & TECH. 3, 20 (2002).

bombard a networked computer with so many signals the computer is effectively taken offline.[243] The characteristic that primarily distinguishes a DDoS attack from the other target crimes is that a DDoS attack is an "outside" crime while hacking and the use of malware are both "inside" crimes.[244]

As we saw earlier,[245] the purpose of hacking is to trespass "in" someone's computer; like a physical trespasser, a hacker's goal is to gain access to a particular place, i.e., get "inside" it. The "harm" basic criminal hacking statutes target is gaining access without being authorized to do so.[246] As we also saw, malware is disseminated for various purposes, i.e., causing damage, stealing data, all of which require that the malware be inserted "into" a computer.[247] These two target crimes are therefore "insider" crimes, i.e., they involve *gaining* access to a computer.

DDoS attacks, on the other hand, are intended to *deny* access to a computer.[248] The crime requires an interactive environment composed of networked entities that communicate with the network via nodes or ports.[249] By bombarding a target's connections to the network with traffic, a DDoS attack effectively takes that system offline.

As I noted elsewhere, DDoS attacks are the one purely new crime to emerge from our use of computer technology.[250] They did not fit into any of our existing crime categories and therefore require the adoption of new, DDOS-specific criminal laws.[251] Since DDoS attacks are the unique product of a specific context, they *may* be limited to that context; in other words, it is possible that DDoS attacks cannot be predicated on the use of other technologies, such as nanotechnology.[252] While that is a reasonable

243. *See, e.g.*, T. Luis de Guzman, Comment, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 529 (2010) (explaining that a DDoS attack "overwhelms the target host, rendering it unable to respond to any other traffic."); *Denial-of-Service Attack*, *supra* note 124 (explaining a DDoS attack strategy in which the target is overwhelmed so as to render it ineffective).

244. *See infra* notes 245–49 and accompanying text (explaining how hacking and the use of malware are "inside" crimes and DDoS attacks are "outside" crimes).

245. *See supra* notes 204–08 and accompanying text (comparing and contrasting hacking with physical trespass).

246. *See* 18 U.S.C. § 1030 (2006) (stating that it is illegal to knowingly or intentionally access a computer without authorization). *See also supra* notes 204–08 and accompanying text (comparing and contrasting hacking with physical trespass). In Part III.A.2.B, *infra*, we will see that a more complex type of hacking (sometimes known as "cracking") involves not only gaining access to a system but committing some criminal act, such as destroying or copying data, once inside.

247. *See supra* note 123 and accompanying text (explaining what "malware" is and providing examples of it); *see also supra* note 241 (providing an example of the nano-malware crime).

248. *See supra* note 124 and accompanying text (stating that a DDoS attack "attempt[s] to make a computer resource unavailable to its intended users"). *See also* Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMP. & HIGH TECH. L.J. 177, 199 (2000) (explaining that DDoS attacks are meant to "deny access" to computers).

249. *See How a 'denial of service' attack woks*, *supra* note 124 (describing the many ways in which a DDoS attack may occur).

250. Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 385 (2007).

251. *See id*. (stating that it is necessary to create new criminal laws to cover DDoS attacks).

252. As noted above, telephones could be (and probably have been) used to launch an attack similar to a DDoS attack. *See* Goodman, *supra* note 242 (analogizing a DDoS attack to using the telephone to shut down a pizza delivery business); *see also Demon Dialer*, ANSWERS.COM, http://www.answers.com/ topic/demon-

hypothesis, I believe it is incorrect.

To understand why I believe the hypothesis is incorrect, we need to consider a variation on the Dr. X scenarios. In the original first scenario, Dr. X's innocuous nanoparticles merely infiltrate the nanoparticles that are delivering doses of the anti-clogging drug to stents installed in a patient's arteries; in the original second scenario, they infiltrate the nanotechnology bomb that is supposed to release bubbles that will destroy the cancer cells in another patient's body. In these scenarios, Dr. X can be held liable for the crime of hacking—gaining unauthorized access to—the legitimate nanoparticles.[253]

Now assume that in both scenarios, instead of simply having his nanoparticles infiltrate the legitimate ones, Dr. X uses his nanoparticles to prevent the legitimate nanoparticles from performing their intended functions. Assume Dr. X is somehow able to ensure that:

- his nanoparticles arrive at the stents before the nanoparticles carrying the anti-clogging drug do and block the stents so the legitimate nanoparticles are unable to deliver new doses of the drugs to the stents; and/or
- his nanoparticles arrive before the other legitimate nanoparticles can assemble into the "supramolecular bomb" that would have destroyed cancer cells.[254]

In these versions of the original scenarios, Dr. X cannot be held criminally liable for gaining unauthorized access because he (or, more precisely, the nanoparticles he used as tools) did not "access" the legitimate nanoparticles. Instead, his nanoparticle tools blocked their path and, in so doing, prevented them from performing their respective intended functions. Nor can Dr. X be held liable for disseminating nano-malware; his nanoparticles did not infect the legitimate nanoparticles with any analogue of a computer virus or worm. Again, they simply blocked their path and, in so doing, prevented them from performing their respective intended functions.

In these modified scenarios, Dr. X accomplishes something that looks very much like a DDoS attack—a physical, rather than digital, DDoS attack. As I noted above, DDoS attacks, as we know them, evolved in a digital context; that does not, though, mean they are exclusive to the digital context. I believe it means they are a phenomenon that has long been possible in the physical world but that we have not encountered due to the logistics involved in implementing such an attack. As I explained elsewhere:

---

dialer-computer-jargon (last visited Feb. 15, 2011) (noting that the term "demon dialer" dates from the 1970s and early 1980s and refers to calling the same telephone number repeatedly in, among other things, a denial-of-service attack). I don't address this possibility in the text for two reasons. One is that the use of telephones to launch denial-of-service attacks is an antiquated tactic; it has been replaced by the use of computers, which are far more effective. The other reason is that a telephone network is analogous to the computer network that is an integral component of computer DDoS attacks. Conceptually, they are functionally analogous.

253. *See supra* notes 214–228 and accompanying text (providing the original Dr. X scenarios and reasoning as to why Dr. X will be held liable for hacking).

254. *Id.*

> Denying access has been of little concern in the real-world because of the physical difficulties involved in inflicting the 'harm'; to deny others access to a facility in the real world, I need a group of individuals who are willing to physically block access to that facility for a period of time. It is possible to recruit such individuals when the denial of access supports a political or social issue they care about; it is unlikely, to say the least, that I could recruit such a group to block access to a facility for my own amusement or out of a vindictive desire to exact 'revenge' on the owner or operator of the facility. Computer technology eliminates those difficulties and makes it possible for me to launch a DDoS attack . . . because I am bored, because I am annoyed with a website, or because I want to experiment with the DDoS technology.[255]

The digital environment is not an integral component of a DDoS attack; it is an adventitious characteristic of the DDoS attacks with which we are familiar, a reflection of the pragmatic obstacles in attempting to predicate a real-world version of such an attack on collective human action.

This means that nano-DDoS attacks are possible whenever nanotechnology can play the same role bits and bytes play in a digital DDoS attack. In the modified scenario outlined above, nanoparticles swarm a physical target and achieve essentially the same effect a DDoS attacker achieves by bombarding a digital target with data. Since the effect is the same, as is the structure of the attack, it seems reasonable to approach this and analogous nanotechnology scenarios as the equivalent of a digital DDoS attack. In order to hold someone criminally liable for such an attack, we would either have to (i) modify our existing DDoS attack statutes so they encompass both digital and nanotech attacks or (ii) create new, distinct statutes that criminalize nano-DDoS attacks by including them in a generic crime that encompasses digital and physical DDoS in or by adopting a physical-DDoS attack-specific statute.

It seems, then, that we may well see nano-analogues of the three digital target crimes. If we do, I suspect they will be just that, i.e., I suspect they will be analogues, rather than clones, of the digital crimes. The fact that nano-crimes, including nano-target crimes, will be committed in a physical environment will no doubt mean they will differ in certain functional respects from their digital antecedents.

The extent to which that will require the adoption of new laws targeting the nano-analogues is a topic we take up in Part III.B, *infra*. Before we take up those issues, we need to consider the likelihood that nanotechnology can be used to facilitate the second category of computer crimes—tool crimes—and/or whether it can play an incidental role in the commission of crimes.

255. Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 WIDENER L.J. 667, 776–77 (2006) [hereinafter Brenner VII].

b. Tool crimes

As I noted earlier, it seems bigamy and rape are the only traditional crimes that cannot be carried out through the use of computer technology.[256] At this point in time, I do not know and cannot speculate as to whether the same will be true of nanotechnology, i.e., whether it will become as pervasive a criminal tool as computer technology.

My goal in this article is not to provide a comprehensive assessment of how nanotechnology can, and will, be used for criminal purposes. Aside from anything else, I do not believe such an assessment is possible given the nascent state of our use of nanotechnology. My goal is to examine the *possibility* that nanotechnology will evolve into a crime-facilitating implement analogous to computer technology. I believe I can achieve that goal by analyzing how nanotechnology could be used to facilitate some of the traditional crimes.

In this section, therefore, we will analyze how nanotechnology *might* be used to facilitate some representative crimes. Traditional crimes are often divided into categories based on the "harm" inflicted, e.g., crimes against persons, crimes against property, crimes against the state, etc.[257] In the sections below, we will consider how nanotechnology could be used to commit representative crimes that fall into each of these three categories.

i. Crimes against persons

We will begin with two of the crimes against persons: homicide and battery. Homicide, of course, is "the killing of a human being by another human being."[258] Homicide is divided into discrete offenses—e.g., murder, manslaughter and negligent homicide—based on the *mens rea* involved in the commission of the crime.[259] Battery is "the unlawful application of force to the person of another."[260] Traditionally, battery encompassed "any application of force even though it entails no pain or bodily harm."[261]

In analyzing whether nanotechnology could be used to commit homicide and/or battery, we will use the Dr. X scenarios we worked with earlier.[262] We will begin with homicide: in the original versions of both scenarios, Dr. X injected the patients with innocuous nanoparticles to determine if his nanoparticles could infiltrate the legitimate nanoparticles.[263] Now assume that

256. *See supra* notes 189–191 and accompanying text (discussing bigamy and rape in the context of the internet). For what I mean by "traditional crimes," *see supra* note 125.

257. Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 VA. J. L & TECH. 1, 18 (2004); Brenner VI, *supra* note 133, at 44.

258. PERKINS, *supra* note 125, at 46.

259. *See id*. at 46–119 (describing offenses included in homicide).

260. *Id.* at 152.

261. *Id.* The Model Penal Code and modern statutes limit battery to a use of force that inflicts physical injury and/or "unwanted sexual advances", but we utilize the older, broader standard in this analysis. LAFAVE, supra note 230, § 16.2(a).

262. *See supra* Part III.A.2.a. We will use these scenarios for the reasons noted above, i.e., efficiency and the *de minimis* nature of the conduct at issue in each essentially provides us with a baseline as to how nanotechnology can be exploited for criminal purposes.

263. *See supra* Part III.A.2.a.

in both scenarios,[264] Dr. X injects the respective patients with nanoparticles that are designed to take their lives directly (i.e., his nanoparticles contain poison which they release upon entering a patient's body) or are designed to do this indirectly (e.g., by rupturing one or more arteries and causing internal bleeding that leads to death).[265] Also assume that Dr. X intended to cause the patients' death in each of the four permutations of the two basic scenarios.[266]

If the patients die, then it should be possible to convict Dr. X of murder in each of these scenarios: in each he acted with the necessary *mens rea* and committed a voluntary act that was designed to, and did, result in the deaths of the respective patients. It should be a relatively simple matter to convict Dr. X of homicide in the two poison scenarios because the poison could no doubt be shown to have been the "but for" cause of the victims' deaths.[267] It might be more difficult to convict him of homicide in the ruptured artery scenarios because of the need to prove causation. Causation issues could prove problematic in the ruptured artery scenarios because each patient was suffering from a condition that could have—might inevitably have—led to their death at some point in time, perhaps relatively soon.[268] The defense might argue that it would be impossible for the prosecution to prove beyond a reasonable doubt that Dr. X's nanoparticles were the "but for" cause of the victims' respective deaths in the ruptured artery cases.[269]

---

264. I.e., the scenario in which the patient has arterial stents and the scenario in which the patient has cancer. *See supra* Part III.A.2.a.

265. *See, e.g.*, *Poison*, WIKIPEDIA, http://en.wikipedia.org/wiki/Poison (last visited Feb. 15, 2011) (explaining the use of poison to cause death); *see also WCCO-TV Reporter Darcy Pohland Dies At 48*, CBS MINNESOTA, http://minnesota.cbslocal.com/2010-most-watched-videos/ (last visited Feb. 8, 2011) (discussing ruptured artery caused fatal internal bleeding). The use of poison would probably be discovered and alert police to the fact that a murder had occurred; the ruptured artery would probably be discovered, but might be attributed to natural causes, meaning that Dr. X might escape prosecution.

266. The permutations are as follows: (i) poison nanoparticles injected into the patient with stents; (ii) poison nanoparticles injected into the patient with cancer; (iii) artery-rupturing nanoparticles injected into the patient with stents; and (iv) artery-rupturing nanoparticles injected into the patient with cancer. *See supra* Part III.A.2.a.

267. *See* LAFAVE, *supra* note 230, § 6.4(b) (stating the rule that in order for an act to constitute the actual cause of a particular result, it must be the "but for" cause of the result). *See, e.g.*, People v. Franszkiewicz, 4 N.W.2d 500, 502 (Mich. 1942) (citing the pathologist's and toxicologist's testimony that the breakdowns of vital organs were caused by a fatal dose of arsenic). Proximate cause does not seem to be an issue here, since we are assuming Dr. X intended to cause the patients' deaths and acted to carry out that intent. *See* LAFAVE *supra* note 230, § 6.4(c).

268. *See, e.g.*, People v. Tackett, 501 N.E.2d 891, 896 (Ill. App. 1986) ("Defendant contends that the record fails to establish that lesions found on Bailek's brain were caused by blunt trauma.").

269. *See id.* ("[T]he relevant question is whether, after viewing the evidence in the light most favorable to the prosecutor, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt."). *See also* LAFAVE, *supra* note 230, §§ 6.4(b), (c) (explaining actual cause and legal cause). If causation proved an insurmountable obstacle in these cases, the prosecution could charge Dr. X with attempting to cause the deaths of these patients. Under the Model Penal Code's approach to attempts, Dr. X can be held liable of attempting to cause their deaths if he acted with the necessary intent and took steps that were designed to achieve that result. *See id.* §§ 11.3, 11.4. The fact that he failed would not be a defense under the Model Penal Code's approach to impossible attempts; as long as Dr. X took the steps he believed would result in their deaths, he can be held liable for attempting to do so. *See id.* § 11.5(a).

The scenarios analyzed above are obviously not the only ways in which nanotechnology could be used to commit murder. Assume that instead of targeting patients Dr. X decides to do away with his rich uncle. Dr. X develops nanoparticles that carry poison and that are designed to self-destruct and deliver the poison within four hours after they are injected into a living being. Dr. X invites his uncle to his home to watch the Super Bowl, knowing his uncle will fall asleep before the game ends. While his uncle is asleep (and as the game is

Now assume yet another permutation on the Dr. X scenarios: In this version of the two basic scenarios we analyzed in the previous section,[270] Dr. X injects both of the patients with nanoparticles that are not designed to kill but that are designed to cause them to suffer some discomfort. If Dr. X's conduct is discovered and reported to the authorities, can he be charged with having committed a battery on each victim?

As noted above, to be guilty of battery Dr. X must have (i) intended to (ii) apply (iii) unlawful force to (iv) the person of another human being.[271] As noted above, we are assuming Dr. X intended to cause the patients discomfort because the nanoparticles were "designed" to do precisely that. We will also assume, for the purposes of analysis, that what he did could qualify as "applying" unlawful force[272] to the "person" of another human being; the crime of battery tends to assume, not unreasonably, that the unlawful force is applied to the exterior of the victim's body. We, though, will assume that injecting substances into someone's body can also qualify as battery.[273]

That leaves us with what *might* be the one problematic element in holding Dr. X. liable for battery in these revised versions of the two basic scenarios: the use of "unlawful force." The use of force on the person of another will not be held "unlawful" if it was (i) privileged or (ii) not excessive.[274] We will assume that if Dr. X's injecting the nanoparticles constituted a use of "force," the use of force was not privileged and was excessive.[275] That brings us to the

---

coming to a close), Dr. X injects his uncle with enough of his poison nanoparticles to cause his uncle to die once they release the poison they carry. When the game ends, Dr. X wakes his uncle, tells his uncle he enjoyed his company but that he, Dr. X, must leave for the hospital to do his rounds. Dr. X's uncle leaves, goes home, and dies roughly four hours later. The toxic nanoparticles self-destruct and dissipate into his bloodstream. The death looks like a heart attack. Since there are no signs of foul play, police do not investigate what was actually a murder; even if they investigated, they might never notice the remnants of the nanoparticles in the victim's bloodstream or realize the significance of the nanoparticles if they did notice them. It is possible that the coroner might discover the poison in the victim's system if an autopsy was done, but it would probably be difficult to link Dr. X to the poison and the resulting death since he made sure others saw his uncle leave his home alive and apparently well.

I am indebted to Burt Webb for this homicide scenario and use it with his permission. Burt Webb, *The Dark Side of Nanotechnology*, ESKIMO NORTH, (last visited Feb. 22, 2011), http://www.eskimo.com/~whitznd/nano_dark.htm. *See also* BOUCHER, *supra* note 1, at 219 (noting that nanotechnology could be used to deliver poison in committing murder).

270. *See supra* Part III.A.2.a.

271. *See* PERKINS, *supra* note 125, at 152–54. Battery charges can be predicated on lesser *mens rea*, including negligence, but we will assume intentionality. LAFAVE, *supra* note 230, at § 16.2(c). We assume intentionality both because it simplifies the analysis (i.e., one of the elements is clearly met) and because it seems likely, as a practical matter, that Dr. X acted with the purpose of causing discomfort. He might, of course, have injected the nanoparticles knowing they carried the substance that eventually caused the patients to suffer discomfort but not realizing it would do so. If that were the case, we would then have to determine whether his conduct rose to the level of criminal negligence.

272. We take up the issue of whether what Dr. X did qualifies as "unlawful force" in the next paragraph.

273. *See, e.g.*, Agripino v. State, 217 S.W.3d 707, 712 (Tex. App. 2007) (injecting mineral oil into a person's body could be prosecuted as aggravated assault). Battery is generally a lesser-included offense of aggravated assault. *See, e.g.*, Martinez v. State, 199 P.3d 526, 533 (Wyo. 2009) (battery was lesser-included offense of aggravated assault).

274. PERKINS, *supra* note 125, at 153.

275. The use of force is excessive when the actor used more force "than is necessary." 6 AM. JUR. 2D *Assault and Battery* § 132 (2010). Since we are implicitly assuming Dr. X was not the patient's physician (i.e., he covertly gained access to each patient), his use of force was not privileged. *See, e.g.*, Johnson v. St. Claire Medical Center, Inc., No. 2002-CA-001385-MR, 2003 WL 22149386, at *3 (Ky. Ct. App. 2003) (specifying

more difficult issue: was what Dr. X did a "use of force" sufficient to sustain a conviction for battery?

Under the traditional approach to battery, "force" encompasses any "touching" of the victim's body.[276] The final issue to be resolved in deciding whether Dr. X committed a battery by injecting nanoparticles into the patients' bodies is therefore whether the injections qualified as a "touching" under battery statutes. One state battery statute defines "touches" to mean "physical contact with another person."[277] Under that definition, Dr. X's conduct would presumably qualify as a "touching" of the patients: he must have touched them with his hands when he was preparing to inject the nanoparticles (e.g., using alcohol to ensure the area was sterile), and he definitely engaged in physical contact when he actually injected the nanoparticles. I cannot find any reported cases in which injecting a substance was held to constitute a use of force under a battery statute, but at least one case held that an injection could qualify as aggravated assault, and battery is generally a lesser-included offense of aggravated assault.[278]

If the prosecution were to proceed under this theory, it seems the only conduct that would be relevant in the battery prosecution is that involved in the injection. In other words, it seems this approach might focus on the acts leading to the penetration of the patients' skin and the injections themselves, but not on what happened after the injections, i.e., the dissemination of the nanoparticles throughout the patients' bodies.[279] I suppose that might not matter, since I assume the discomfort the patients endured is a circumstance that could be considered if and when Dr. X was sentenced for committing battery on both patients. Taking that into account at sentencing might ensure he was fairly punished for the "harms" he inflicted on the victims.[280]

Since simple battery is usually a misdemeanor,[281] focusing exclusively on the conduct leading to and resulting in the injection of the nanoparticles means that Dr. X would probably be charged with, and convicted of, two

limited circumstances when a doctor has the privilege to use force).

276. *See supra* note 261; *see also* LAFAVE, *supra* note 230, § 16.2(a).

277. CAL. PENAL CODE § 243.4(f) (2010).

278. *See Agripino*, 217 S.W.3d at 715 (suggesting that the injections received by the victims constituted aggravated assault).

279. If the prosecution were to focus only on the injections themselves as constituting the "harm" inflicted on the victims, it would be proceeding under the theory that battery can be predicated on an "offensive touching" that does not inflict bodily injury on the victim. *See generally* LAFAVE, *supra* note 230, at § 16.2(a) (stating that traditional view of battery encompassed both the infliction of bodily injury and an offensive touching).

The prosecution would also have to show that the injection constituted a "touching" that was "offensive." *See generally* May v. Mercy Memorial Nursing Center, No. 05-019213-NH, 2009 WL 131699, at *1 (Mich. Ct. App. 2009) (stating that for battery to occur, the touching must be offensive).

If the prosecution were to proceed under an "infliction of bodily injury" theory, it would then presumably focus on the consequences of the injection, not merely on the touching incidental to the injection. *See generally id.* In the discussion above, I focus on the first theory because it would presumably allow Dr. X to be prosecuted for battery even if the nanoparticles had not been intended to have any negative effect on the patients.

280. *See, e.g.*, Edwards v. United States, 523 U.S. 511, 514 (1998) (discussing the propriety of including conduct not encompassed in the offense of conviction in calculating the sentence).

281. PERKINS, *supra* note 125, at 152.

misdemeanors. States have also created the felony of "aggravated battery," which is variously defined as using a weapon, dangerous weapon or a dangerous instrumentality to commit battery.[282] Some states allow an aggravated battery charge to be predicated on the perpetrator's using "any poison or other noxious or destructive substance."[283] If Dr. X committed his crimes in a state with such a provision, the prosecution should be able to charge him with aggravated battery on the premise that his nanoparticles qualify at least as a "noxious substance."

It seems, then, that nanotechnology *could* be used to commit crimes against persons (with the exception of rape and bigamy).[284] In this regard, nanotechnology may provide more opportunities for criminal exploitation than computer technology. Crimes against persons generally involve inflicting a physical "harm" on the victim,[285] but computers are not a physical medium. While it may be possible to use computer technology to physically "harm" a human being, there are no reported cases in which that has occurred; the likelihood of computer technology being used to achieve such a result is probably low due to the difficulty involved in carrying out such an effort and the fact that there are so many easier ways to inflict physical "harm" on individuals.[286] Nanotechnology, on the other hand, is a physical medium; as we saw above, it is likely that nanotechnology can be manipulated so as to "harm" human beings.[287]

---

282. *See, e.g.*, LAFAVE, *supra* note 230, at § 16.2(d) (discussing the aggravated battery offense).

283. IDAHO CODE ANN. § 18-907(1)(c) (2010). *See also* ILL. COMP. STAT. ANN. Ch. 720 § 5/12-4 (West 2010); LA. REV. STAT. ANN. § 14:33 (2010) (showing other states' definitions of aggravated battery that include a similar poison-related provision as the Idaho statute). *See, e.g.*, LAFAVE, *supra* note 230, § 16.2(d) (discussing the aggravated battery offense).

284. Brenner IV, *supra* note 124, at ¶ 17, 110–14 (discussing how rape and bigamy cannot be committed via technological sources).

285. *See, e.g.*, PERKINS, *supra* note 125, at xvii–xx (e.g., homicide, assault, battery, rape, child abuse, child rape, false imprisonment, kidnapping). Assault is generally defined as either an attempt to commit a battery or "an intentional placing of another in apprehension of receiving an immediate battery." *Id.* at 159. It *might* be possible to use computer technology to place someone in fear of being the victim of battery, but the fear would presumably have to be predicated on conduct in the real, physical world. It seems, then, that computer technology could, at best, be used as a contributing factor in creating such an apprehension, i.e., play a role analogous to that of the telephone.

286. There is one reported instance of what might have been an attempt to use computer technology to commit murder and/or aggravated battery. *See* BRENNER I, *supra* note 7, at 100–02 (describing a case from 1994, in which a hospital employee in the United Kingdom used the hospital's computer to alter prescriptions in a way that could have resulted in injury or even death to the affected patients and the attempt, if such it was, failed). The fact that this is the only reported instance in which someone used computer technology in an effort to commit crimes against persons supports the premise outlined above, i.e., that computer technology is not well-suited for the commission of crimes in this category.

287. Although computer technology is ill-suited for committing physical crimes against persons, it has proved to be remarkably successful in implementing non-physical harms on individuals. *See, e.g.*, Brenner V, *supra* note 125, at 6–16 (explaining how our increasing use of computer technology resulted in a corresponding increase in the varieties and incidence of the crimes against persons that inflict "soft" harms, i.e., inflict emotional and/or reputational "harm" on individuals). Criminal law has expanded to recognize new offenses targeting "soft" harms and expand the scope of older offenses that targeted certain aspects of varying "soft" harms. *Id.* Computer technology may continue to dominate in this area, i.e., it may ultimately prove to be the most effective way to inflict "soft" harms on others. I suspect nanotechnology may have some capacity to be used as a vector for inflicting "soft" harms, but at this point in time I find it difficult to articulate nanotechnology-predicated stalking and/or harassment scenarios.

ii. Crimes against property

The crimes against property are more varied than the crimes against persons. They include theft, robbery, counterfeiting, fraud, forgery, vandalism, arson, receiving stolen property and extortion.[288] Since our purpose is to analyze the possibility that nanotechnology could be used to commit crimes in each of the three categories listed above, we will not consider how it could be used to commit all the crimes against property. We will, instead, proceed as we did with the crimes against persons, i.e., we will analyze how nanotechnology could be used to commit some representative crimes against persons.

We begin with two related crimes: counterfeiting and forgery. Historically, counterfeiting consisted of "making false money" and passing it off as genuine.[289] Forgery consisted of making "a false writing having apparent legal significance" with the "intent to defraud."[290] The distinction between counterfeiting and forgery was well established as long as "money" consisted of coins, but it began to erode with the use of paper currency.[291] As a result, the two terms often appear together in statutes that criminalize counterfeiting/forging money, property and other items, such as election returns.[292] Both crimes have also broadened in scope: goods bearing unauthorized trademarks are often referred to as "counterfeit goods" and forgery has expanded to encompass the falsification of items—e.g., art—as well as documents.[293] Logically, then, nanotechnology could perhaps be used to commit counterfeiting/forgery in either or both of two ways: falsifying documents (including money)[294] and/or counterfeiting goods.[295]

---

288. PERKINS, *supra* note 125, at xxi–xxiv. Trespass and burglary also constitute crimes against property, but since we examined them earlier they are not included here. *See supra* Part III.A.2.a.

289. *See, e.g.*, PERKINS, *supra* note 125, at 432; IV WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 80 (describing the crime of counterfeiting). As Perkins and Boyce note, counterfeiting "has usually been classified as an offense affecting the administration of governmental functions," but it is also a crime against property. PERKINS, *supra* note 125, at 432. We will analyze it as a crime against property.

290. *See, e.g.*, PERKINS, *supra* note 125, at 414; IV WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 290 (describing the crime of forgery).

291. PERKINS, *supra* note 125, at 432.

292. *See, e.g.*, 18 U.S.C § 471 (2006); 18 U.S.C § 485 (2006); ARIZ. REV. STAT, § 16-1011(A) (2007) (West); CAL. PENAL CODE § 470a (West 1977); FLA. STAT. § 831.01 (2010); N.D. CENTURY CODE ANN. § 12.1-24-01(1) (West 2006); 13 VT. STAT. ANN. § 1801 (West 2010) (using forgery and counterfeiting in the same offense). At least one state statute defines counterfeit as "to forge, counterfeit, materially alter, or falsely make." MD. CODE ANN., CRIM. LAW § 1-101(c) (West 2010).

293. Richard J. Pinto, Elliott J. Stein & Christine B. Savoca, *Recent Developments in Trademark and Copyright Law, in* UNDERSTANDING TRADEMARK AND COPYRIGHT DEVELOPMENTS FOR ONLINE CONTENT (2010), *available at* 2010 WL 1972540 *3 (2010); Joseph C. Gioconda, *Can Intellectual Property Laws Stem the Rising Tide of Art Forgeries?*, 31 HASTINGS COMM. & ENT. L.J. 47, 60–61 (2008).

294. *See* BLACK'S LAW DICTIONARY 1027 (8th ed. 2004) (defining "money" as consisting of "paper money," "e-money," i.e., data operating as "a money substitute," and "hard money", i.e., "coined money"). *See, e.g.*, People v. Harrison. 283 Mich. App. 374, 376–77 (Mich. App. 2009) (holding defendant liable for using a computer to counterfeit paper money). The dichotomy set out above does not explicitly encompass falsifying coins, but since "[t]oday counterfeit coins are made primarily to simulate rare coins which are [primarily] of value to collectors," the practice is implicitly included the in the "falsifying goods" category. *Know Your Money*, SECRETSERVICE.GOV, http://www.secretservice.gov/money_coins.shtml (last visited, Feb. 2, 2011). The dichotomy also does not explicitly include falsifying e-money, but since that is far more likely to be done with computer technology than with nanotechnology, the omission should not materially erode the

I use distinct terms to refer to what are versions of the same crime because I believe the "document" versus "goods" crimes inflict "harms" that are conceptually distinct, at least to some degree. The forgery "harm" consists of telling a lie; a forged document implicitly communicates a misstatement of fact that invalidates the document.[296] The counterfeiting "harm" is analogous to the "harm" encompassed by the common law crime of adulteration: passing debased goods—goods the quality of which was deliberately diminished in processing—off as legitimate.[297] Since the adulterated goods are not what they are represented to be, the adulteration "harm" includes a lie but the lie is not as all-encompassing as the forgery lie. The forgery lie is a zero-sum lie; the forged document is not at all what it is represented to be. The counterfeiting lie is a less than zero-sum lie; the counterfeited good is not entirely what it is represented to be. While this distinction has been neither particularly apparent nor particularly important in criminal law to this point in time, I suspect it may become significant if and when nanotechnology is used to create counterfeit goods. Before we consider counterfeiting, though, we need to consider the potential for nano-forgery.

Nanotechnology seems unlikely to play a significant role in falsifying documents, at least not for the foreseeable future. Today most documents—especially documents that have legal and/or financial significance—are computer-generated.[298] As long as that is true, computers will probably continue to be the preferred means for falsifying documents.[299]

---

dichotomy's efficacy in analyzing the use of nanotechnology to engage in counterfeiting and/or forgery. *See generally Electronic Money*, WIKIPEDIA, http://en.wikipedia.org/wiki/Electronic_money (providing an overview of electronic money); Joseph J. Sommer, *Where is a Bank Account?*, 57 MD. L. REV. 1, 94 (1998) (describing the current status and potential strengths of e-money).

295. BLACK'S LAW DICTIONARY 714 (8th ed. 2004) (defining "goods," in part, as "[t]angible or movable personal property other than money").

296. LAFAVE, *supra* note 230, § 19.7(j)(5); *see, e.g.*, Watts v. State, 158 S.W.2d 510, 514 (Tex. Crim. App. 1942) (giving examples of forgery); Merchs. Bank & Trust Co. v. People's Bank of Keyser, 130 S.E. 142, 150–51 (W. Va. 1925) (setting out principles of forgery). Since the forged document is invalid, the victim loses whatever money or property he parted with in relying on it. *See, e.g.*, Lowe v. Wright, 292 S.W.2d 413, 417 (Tenn. Ct. App. 1956) (describing the relationship between forgery and reliance).

297. *See* Pennsylvania v. Curry, 4 Pa. Super. 356, 360 (Pa. Super. Ct. 1897) ("The term adulteration is derived from the Latin adultero, which . . . signifies to defile, to debase, to corrupt, . . . to counterfeit, etc."). See *generally* 2 C.J.S. *Adulteration* § 1 (1972) (providing an overview of the topic).

298. *See, e.g.*, *Document*, WIKIPEDIA, http://en.wikipedia.org/wiki/Document (listing examples of electronic storing and displaying of documents) (last visited Feb. 23, 2011).

299. As one author notes, computer forgery can be committed by "1) altering data in documents stored in a computerized form; and, 2) using the computer as a tool to commit forgery through the creation of false documents indistinguishable from the authentic original." Miriam F. Miquelon-Weismann, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 329, 361 n.12 (2005).

Using a computer is clearly the preferred way to commit forgery today. *See, e.g.*, State v. Powell, 306 S.W.3d 761, 762–63 (Tex. Crim. App. 2010) (describing that the defendant used a computer to forge checks); *see also Lawyer Jailed for Inflating Pay When Changing Firms*, NAT'L L. J. 7, 7 (Mar. 29, 2010) (describing an attorney's forged claim about his salary); Nick Britten, *Benefit Cheat had Breast Surgery*, DAILY TELEGRAPH, Jan. 12, 2010, at 12 (describing how computer generated forged documents were used to claim false housing benefits). Indeed, the use of computers to generate documents is so common that using another means may increase a perpetrator's chances of being apprehended. *See, e.g.*, Nelson v. State, 32 So. 3d 534, 537 (Miss. Ct. App. 2009) (explaining that forged checks were identified because they were prepared using a typewriter instead of a computer).

If efforts to use nanotechnology to develop quantum computing prove successful, then nanotechnology

Nanotechnology might, though, still play some role in the computer-falsification of documents; nanotechnology-based inks could make it easier to generate documents that appear genuine[300] and/or to produce self-erasing forgeries that serve their purpose and then eliminate incriminating evidence.[301]

Falsifying documents may not be an area of criminal endeavor in which nanotechnology will play a significant role.[302] That in no way diminishes nanotechnology's potential as a vector for facilitating tool crimes; as we saw earlier, computer technology is a tool that can be used to facilitate a variety of crimes. But computer technology cannot be used to facilitate *all* crimes; it is, as noted earlier, particularly unsuited for facilitating the commission of crimes that involve inflicting physical "harm" on persons.[303]

Nanotechnology is likely to play a notable role in counterfeiting goods. As we saw in Part II.A, manufacturing goods of various types is expected to be one of the major applications of nanotechnology. The process of counterfeiting goods requires that counterfeiters have access to the technology needed to create the fake goods and an adequate supply of labor willing to produce the fakes. Counterfeiters use a production process that is analogous, but often inferior, to the process used by the legitimate manufacturers of the goods.[304] Goods counterfeiting has, as a result, tended to be product-specific,

---

may well come to play an important, though probably indirect, role in using computers to falsify documents. *See generally Nano Chat: It Seems Nanotechnology Might One Day Help Revolutionise Global Communications*, OURFUTUREPLANET.ORG (June 1, 2010), http://www.ourfutureplanet.org/news/390-nano-chat-it-seems-nanotechnology-might-one-day-help-revolutionise-global-communications- (describing the potential influence of quantum technology on communication).

300. *See generally* David Savastano, *NanoProducts Brings Nanotechnology to Ink Industry*, INK WORLD (Jan. 2004), http://findarticles.com/p/articles/mi_hb3143/is_1_10/ai_n29068170/ (describing nanotechnology's presence in producing ink).

On a different note, researchers recently announced the development of a new nanotechnology process that "could have important applications in the security printing industry" by making "bank notes and credit cards harder to forge." Press Release, Nanotechnology Now, How Butterflies' Wings Could Cut Bank Fraud (May 31, 2010), *available at* http://www.nanotech-now.com/news.cgi?story_id=38470. It might also provide forgers with a way to enhance the apparent authenticity of the documents they produce by utilizing this same technology.

301. *See, e.g.*, *Nanotechnology Inks for Self-Erasing Paper*, NANOWERK.COM (Aug. 26, 2009), http://www.nanowerk.com/news/newsid=12320.php (describing self-erasing technology).

This type of minimal facilitation of the commission of crime illustrated by the two examples given above probably would not rise to the level of involvement required to transform the crime into a nanotechnology-as-tool crime. *See supra* Part III. Minimal facilitation of this type is more likely to fall into the technology-as-playing-an-incidental-role in the commission of crime category that is discussed in the section immediately below.

302. That does not mean it cannot play an incidental role in the commission of crimes. *See infra* Part III.A.2.c.

303. *See* Brenner V, *supra* note 125, at 77 (differentiating virtual and real rape). *See also* BRENNER I, *supra* note 7, at 98–102 (discussing rape and murder as examples of physical harm crimes).

304. *See, e.g.*, Todd Datz, *Counterfeiting: Faked in China*, CSO SECURITY AND RISK (Jan. 1, 2006), http://www.csoonline.com/article/220737/counterfeiting-faked-in-china (identifying three types of counterfeit operations: legitimate factory also produces fakes; manufacturer hired to make a certain quantity of goods makes more and sells them on its own; and underground, usually low-technology, facilities).

One of the most common techniques in goods counterfeiting involves running "ghost" shifts, i.e., unauthorized third shifts, at legitimate factories; the goods from the ghost shifts, however, are sold on the side and their existence is never revealed to the rightful owner of the item being counterfeited. *See, e.g.*, Roger Parloff, *Not Exactly Counterfeit*, FORTUNE ON CNNMONEY.COM (Apr. 26, 2006, 4:34 PM), http://money.cnn.com/ magazines/fortune/fortune_archive/2006/05/01/8375455/index.htm. In a variation of this technique, overseas factories that were legitimately producing certain goods continue producing them

especially if the product is relatively complex, like an IPhone.[305]

Depending on its accessibility and complexity, nanotechnology manufacturing seems likely to be exploited by goods counterfeiters.[306] They would use the technology in the same way as, and for the same purposes as, those who employ it legitimately. The initial hurdle goods counterfeiters are likely to face is acquiring the technology itself; they might be able to accomplish this by compromising an employee of a company that is using nanotechnology in the manufacture of certain goods.[307] If the counterfeiters were able to acquire the technology, they might need individuals with expertise in how it should be utilized; they could address this issue by hiring ex-employees of a company utilizing the technology to work in their illegitimate goods factories (or to consult on the operation of such factories).[308]

Operationally, nano-goods counterfeiting would probably be very similar to conventional goods counterfeiting. The doctrinal issue is whether the use of nanotechnology to copy goods would make the application of current counterfeit goods law to nano-counterfeits problematic. Counterfeit goods law is based on copyright and trademark principles: basically, a counterfeit good is (i) an unauthorized copy of an item in which someone holds a valid copyright; or (ii) a copy that bears an unauthorized version of a valid trademark owned by someone else.[309] The "harm" inflicted by each alternative is the owner's loss of some quantum of the value of an intangible property right.

As noted earlier, counterfeiting originally encompassed the same "harm" as the common law crime of adulteration: the practice of diluting the value of a commodity (money) by passing a debased version of it.[310] Contemporary

---

illegitimately after their contract with the rightful owner ended. *Id.*

See also Richard Jones & Susie Boniface, *Fake Designer Boots Are Churned Out by Children in Chinese Sweatshops*, MIRROR (June 6, 2010), http://www.mirror.co.uk/news/top-stories/2010/06/06/fake-designer-boots-are-churned-out-by-children-in-chinese-sweatshops-115875-22313441/ (describing the use of child labor, being controlled by criminal gangs, to produce counterfeit goods); Patrick Mathangani, *Exposed: Secrets of Fake Goods Factory*, THE (KENYA) STANDARD (May 3, 2010), http://www.standardmedia.co.ke/InsidePage.php?id=2000004942&cid=4 (detailing counterfeit procedures in Kenya).

305. *See, e.g.*, John Liu & Chinmei Sung, *IPhone Knockoffs Steal Sales as Apple Delays in Asia*, BLOOMBERG (Sept. 11, 2007), http://www.bloomberg.com/apps/news?pid=20601109&sid=a7K_I.ifMcEA&refer=home.

306. Nanotechnology manufacturing involves self-assembly and/or molecular manufacturing. *See supra* Part II(A). *See, e.g.* Chris Phoenix, *Molecular Manufacturing vs. Self-Assembly*, RESPONSIBLE NANOTECHNOLOGY BLOG (Jan. 27, 2010), http://crnano.typepad.com/crnblog/2010/01/molecular-manufacturing-vs-selfassembly.html. In the discussion above, I assume the use of either process, even though molecular manufacturing is in a very early state of development.

307. *See, e.g.*, United States v. Chung, 633 F. Supp. 2d 1134, 1136–37 (C.D. Cal. 2009) (employee stole proprietary information concerning employer's technology). This assumes that the technology used to manufacture a particular product is not generally available. If it is, then the techniques referenced in *supra* note 304, would come into play, e.g., the counterfeiters might control or gain control of a legitimate factory that was making, or had been making, the product legitimately.

308. *See generally* United States v. Case, No. 3:06-cr-210-WHB-JCS, 2008 WL 1827429, at *3–5 (S.D. Miss. Apr. 23, 2008) (addressing an economic espionage scheme using current and ex-employees of targeted company).

309. *See, e.g.*, Adrian Otten & Hannu Wager, *Compliance with TRIPS: The Emerging World View*, 29 VAND. J. TRANSNAT'L L. 391, 404 n. 59 (1996) (under this treaty, "counterfeit goods are . . . defined as goods involving . . . copying of trademarks, and pirated goods as goods that violate a reproduction right under copyright or a related right").

310. *See supra* note 296 and accompanying text.

goods counterfeiting law implicitly encompasses that "harm" (since many counterfeit goods are of inferior quality) but it also encompasses another, newer "harm." Since counterfeit goods are often produced in the same factories that produce legitimate versions of a good, the "harm" resulting from their production and sale is not limited to the traditional adulteration "harm"; it includes that "harm" plus a similar "harm," i.e., the loss of value resulting from the production and sale of identical but unauthorized versions of a good.

We do not know what fully mature nanotechnology manufacturing will look like or will be capable of doing, but it seems reasonable to assume that it will involve fabricating items in a manner similar, but superior, to the manufacturing processes in use. It also seems reasonable to assume that to the extent evolved nanotechnology manufacturing is corrupted and used to make unauthorized copies of goods, the process will inflict one or both of the "harms" noted above. That is, it seems reasonable to assume that while a technologically superior process should produce superior (but counterfeit) products, it can also produce inferior (and counterfeit) products. Logically, then, it seems unlikely that existing counterfeit goods law will require major alteration as we move into eras of partial and then increasing nanomanufacture.[311]

There might, though, be a residual scenario: goods counterfeiters create unauthorized copies of consumer goods because they are relying on a mass market for their profits, which come from selling as many of the copies as possible, usually at reduced prices. Counterfeiting, as such, has not generally involved creating unauthorized versions of unique or extremely rare commodities, such as valuable jewels or works of art.[312] What if we assume,

311. There is another counterfeiting scenario that does not fit easily into either the crimes against persons or crimes against property category: counterfeiting drugs. Since this crime involves counterfeiting, it may seem a crime against property, but as noted below, the "harm" inflicted is physical "harm" to an individual victim, not a property "harm." The crime probably fits into the category into which other drug crimes fall, i.e., crimes against morality. *See, e.g.*, Brenner V, *supra* note 125, at 9–10.

Counterfeit drugs already exist and are already a matter of great concern. *See, e.g.*, *Counterfeit Medicine*, FDA (Jan. 28, 2011), http://www.fda.gov/Drugs/ResourcesForYou/Consumers/BuyingUsingMedicineSafely/CounterfeitMedicine/default.htm; Counterfeit Medications, WIKIPEDIA, http://en.wikipedia.org/wiki/ Counterfeit_medications (last visited Feb. 8, 2011). The drugs that are counterfeited can be legitimate prescription or over the counter drugs or they can be illegal controlled substances. *Id.* The primary "harm" currently associated with counterfeit drugs is safety: they can contain too much or too little of a particular medication or they can contain substances the inclusion of which is not identified on the package label (if there is one). *Id. See also* Adam Powell, *Benchmark Legislation: A Measured Approach in the Fight Against Counterfeit Pharmaceuticals*, 61 HASTINGS L.J. 749, 750–54 (2010) (detailing harms involved including death). Nanotechnology might become a tool used to create and/or deliver next-generation drug counterfeits. *See, e.g.*, *Nanomedicine*, WIKIPEDIA, http://en.wikipedia.org/wiki/Nanomedicine#Medical_use_of_nanomaterials (last visited Feb. 8, 2011) (describing the use of nanotechnology to deliver medicines). If nanotechnology is eventually used for this purpose, it is only reasonable to assume that eventually those with a criminal bent will find some way to use it to counterfeit and/or otherwise misrepresent the pharmaceutical substances they market.

312. *But see* JOHN E. CONKLIN, ART CRIME 80 (1994) (noting mass production and sale of counterfeit prints in the United States between 1980 and 1987). Art forgers probably avoid copying such high-profile targets for at least two reasons: One is the difficulty of convincing a prospective purchaser that the item you have for sale is, in fact, the "real" Mona Lisa when the original truly seems to be hanging in the Louvre Museum. The other is the relative small size and the relatively discerning eye of prospective purchasers. Neither factor comes into play in small scale counterfeiting operations like the one cited at the beginning of this note; the counterfeit print scam was really a consumer good counterfeiting scheme.

for the purposes of analysis, that nanomanufacturing reaches the point at which it can be used to make a copy of any item that is indistinguishable from the original?[313] It would, for example, be possible to make a perfect copy of the *Mona Lisa* or of the Hope Diamond.[314]

If someone used advanced nanomanufacturing to create an identical, indistinguishable, copy of the *Mona Lisa*, would that be a crime against property?[315] It would not constitute goods counterfeiting because the copy neither violates a copyright nor a trademark held by someone other than the copier. It *could* constitute fraud if the purchaser of the new *Mona Lisa* had been told she was buying the original, the only original, of the painting; but to make the analysis more interesting, we will assume she was told she was buying an identical copy and was quite happy to obtain such a copy of the *Mona Lisa* for what she considered to be a relatively small sum. Since she knows what she purchased and paid what she considers a fair price for the item, we do not have fraud.

Do we have theft? Can the Louvre Museum, which owns the original *Mona Lisa*, file a criminal complaint for theft against the creator of the new version of the painting in, say, New York City, where he lives and works? That, of course, depends on whether or not what he did constitutes theft, and to resolve that issue we need to briefly consider a computer crime case.

A computer specialist (Doe) worked as a contractor for the Intel Corporation in a division that created complex computer systems for the U.S. military.[316] After he had worked in that division for a while, Doe had a falling out with his supervisor and was transferred to another division; most of the passwords he used to access the computers in the original division were disabled, but for some reason one was not.[317] He continued to work at Intel and continued to use that password to access computers in the original division; Doe copied and downloaded the file that contained the passwords for all of the authorized users of the computers in the original division and stored it on a computer he controlled.[318] At that point, his activity was discovered and Intel went to the police.[319] Doe was charged with and convicted of computer theft, i.e., using a computer to commit theft, and appealed.[320] On appeal, Doe claimed he had not committed theft because Intel had not "lost"

313. *See, e.g.*, *What Is Nanotechnology?*, *supra* note 30 ("A computer can make copies of data files—essentially as many copies as you want at little or no cost. It may be only a matter of time until the building of products becomes as cheap as the copying of files. That's the real meaning of nanotechnology, and why it is sometimes seen as 'the next industrial revolution.")

314. *See, e.g.*, *Mona Lisa*, WIKIPEDIA, http://en.wikipedia.org/wiki/Mona_lisa (last visited Feb. 8, 2011); *Hope Diamond*, WIKIPEDIA, http://en.wikipedia.org/wiki/Hope_Diamond (last visited Feb. 8, 2011). The discussion in the text assumes, again for the purposes of analysis, that the creators of the copies were able to obtain whatever data they needed to be able to generate identical copies of both items.

315. I am indebted to Burt Webb for this scenario and use it with his permission. *See* Webb, *supra* 269 (posing similar hypothetical).

316. State v. Schwartz, 21 P.3d 1128, 1129–31 (Or. Ct. App. 2001). These and the remaining facts in this scenario are based on the facts in *Schwartz*.

317. *Id.*

318. *Id.*

319. *Id.*

320. *Id. at* 1131, 1135.

anything—it still had the original file containing all of the passwords and all of the passwords were still usable.[321]

Doe's argument was quite correct, as a matter of traditional law.[322] Theft has always been a zero-sum transaction: If a thief takes my bag, the possession of that bag shifts completely from me to him; he has it and I do not.[323] The thief cannot copy my bag, so that he has it and all its contents and I do, too. Doe's argument was therefore valid as far as traditional criminal law was concerned; had he been charged under a traditional theft statute, one that defined theft as taking property with the intent to permanently deprive the owner of its possession and use,[324] the appellate court would no doubt have had to reverse his conviction. But Doe was unlucky: he was charged under a new computer theft statute that defined the crime in part as taking "proprietary information."[325] The appellate court was therefore able to affirm the conviction because it found, essentially, that by taking a copy of the passwords the ex-employee deprived Intel of some portion of the value of the passwords: Intel had not lost the passwords, as such, and they still functioned as passwords but their value was significantly diminished once Intel lost exclusive possession and control of them.[326]

That brings us back to the new *Mona Lisa*. Something similar occurred in this scenario: the original version of the painting is still intact, still possesses all of the qualities that have made it admired and respected for centuries. Its tactile integrity has not been compromised. So the person who made the copy could, if he were to be charged with theft, make the same argument Doe made in the scenario analyzed above: He did not "take" anything from the Louvre Museum. They still have the original, the "real," *Mona Lisa.* All he did is to make a copy; he might even point out that the museum has allowed photographs of the painting to be taken and published,[327] and suggest that what he did was analogous to that. To sustain the theft charge, the prosecution (and the Louvre) would have to show how and why the museum "lost" something due to the fabrication of the copy.

In the Intel case, simply making the copy eroded the value of the passwords, just as making a copy of a key erodes its value. Once copies exist, the original key or password still functions as an access device, but it has lost

321. *Id. at* 1136.

322. *See, e.g.*, Brenner VII, *supra* 255, at 782 (discussing theft of tangible property as a zero-sum transaction).

323. *Id.*

324. *See, e.g.*, COLO. REV. STAT. ANN. § 18–4–401(1)(a)–(c) (2010) (indicating the a person commits theft when he obtains control over another's property with and "[i]nteds to deprive the other person permanently of the use or benefit of the thing of value."); MINN. STAT. ANN. § 609.52(2)(1) (2010) (indicating that a person commits theft when he "intentionally and without claim of right takes, uses, transfers, conceals or retains possession of movable property of another without the other's consent and with intent to deprive the owner permanently of possession of the property.").

325. *Schwartz*, 21 P.3d at 1135 (quoting OR. REV. STAT. § 164.377(2)(c)).

326. *Id. at* 1136.

327. *Paintings: Latest Acquisition*, LOUVRE MUSEUM, http://www.louvre.fr/llv/oeuvres/detail_actualite.jsp?CONTENT%3C%3Ecnt_id=10134198673403414&CURRENT_LLV_FICHE%3C%3Ecnt_id=10134198673403414&CURRENT_LLV_DEP%3C%3Efolder_id=1408474395181115&FOLDER%3C%3Efolder_id=9852723696500764&bmLocale=en (last visited Feb. 22, 2011).

all or much of its utility as a security device. The prosecution (and the Louvre) would have to show that the museum "lost" some quantum of the painting's intrinsic value once the copy was created. In other words, they would have to show that while they had not lost the *Mona Lisa* as such, they had lost a quantum of its . . . what? In the Intel case, the lost commodity—the lost quantum "value"—was a utilitarian function, i.e., the ability to keep certain systems secure from unauthorized users. If and when unauthorized nanotechnology copying of tangible (and perhaps unique) items becomes a reality, law will have to decide if it will pursue a similar approach to nanotechnology-copying and if so, how it will approach the issue of a "loss" of property.

If law decides to treat unauthorized nanotechnology-copying of tangible items as theft, then it will presumably have to utilize an approach analogous to that which the Oregon Court of Appeals employed in the case described above. The Oregon court implicitly acknowledged that theft can be zero-sum or less than zero-sum;[328] in other words, a thief can deprive me of all or only part of the "value" of my property. The focus shifts from the physical item, as such, to features of the item, such as its utility as a security device. When theft statutes refer to "value", they tend to define it in purely monetary terms,[329] but *Black's Law Dictionary* defines it more expansively, i.e., as the "significance, desirability, or utility of something."[330] The prosecutor who is pursuing the creator of the new *Mona Lisa* in the hypothetical outlined above might, with the assistance of Louvre Museum experts, argue that making the copy eroded some esthetic or cultural "value" associated with the original painting's status as the *only* version of that painting in existence. Or we could simply accept that nothing—at least nothing the existence and nature of which was known publicly—could ever be unique in a nanotechnology world.

As this discussion illustrates, if and when nanotechnology moves into general public use and becomes accessible to criminals and to those who are willing to facilitate criminal activity, criminal law will almost certainly have to confront new, nanotechnology-facilitated property crimes. Some of the crimes, such as forging documents and copying consumer goods, may not require significant changes in existing law and/or the adoption of new, nanotechnology-specific criminal laws. Others, such as the *Mona Lisa* scenario, may require a reassessment of existing law and policy to determine the extent to which the technology is being utilized in a manner that cannot satisfactorily be addressed by the civil justice system.

328. *See Schwartz*, 21 P.3d at 1137 (noting that the definition of taking could be "more than just the transfer of exclusive possession that defendant proposes").

329. *See, e.g.*, GA. CODE ANN. § 16–8–14(c) (2010) ("In all cases involving theft by shoplifting, the term "value" means the actual retail price of the property at the time and place of the offense."); WIS. STAT. ANN. § 943.20(2)(d) (2010) (noting that "value" "means the market value at the time of the theft or the cost to the victim of replacing the property within a reasonable time after the theft, whichever is less.").

330. BLACK'S LAW DICTIONARY 1690 (9th ed. 2009). It also includes the concept of "social value", which is the "significance, desirability, or utility of something to the general public." *Id.*

iii. Crimes against the state

Unlike other categories of crime, crimes against the state do not target the infliction of particular "harms" upon civilian victims, whether individuals or artificial entities. Crimes against the state target conduct that erodes or threatens to erode the state's ability to enforce its laws and thereby maintain social order. There are many different crimes against the state, such as treason, official bribery, escape, riot, perjury and obstructing justice.[331] While nanotechnology may some day be used to facilitate treason, bribery, escape or even riot, I cannot, at this point in time, begin to speculate on how that might come about.

I can, thanks to the unwitting assistance of some science fiction writers, speculate a bit about how nanotechnology could be used to obstruct justice, at least in the sense of tampering with evidence. Obstruction of justice statutes encompass a wide variety of conduct,[332] but our concern is limited to obstruction that consists of creating, altering and/or destroying evidence with the intent to obstruct a criminal investigation or prosecution.[333]

More precisely, our concern is with the development and use of canned obstruction of justice techniques, i.e., standardized techniques anyone who has access to them can use to destroy certain types of evidence. To understand what that could mean, we need to review a phenomenon that has emerged in the area of computer crime: anti-forensics. As one website explains:

> [A]nti-forensics in the realm of . . . computer forensics involves the hiding, destroying, and disguising of data . . . . One major goal of anti-forensics is to make analysis and examination of digital evidence as difficult and as confusing as possible. Today, thwarting an investigation has never been easier.[334]

Computer anti-forensics uses several general techniques, e.g., hiding data, securely destroying data or preventing data from being created, each of which involves the utilization of various tools.[335] Most anti-forensics software is available online for free on sites that often provide at least some instruction in

---

331. *See* PERKINS, *supra* note 125, at xxiv–xxvii (listing crimes).

332. *See id.* at 552–58 (discussing resisting or obstructing an officer, witness tampering, and destruction or suppression of evidence).

333. *See id*. at 558–59 (listing examples of obstruction crimes involving evidence tampering). *See also* 18 U.S.C. § 1512(c)(1) (2006) ("Whoever corruptly . . . alters, destroys, mutilates, or conceals a record, document, or other object . . . with the intent to impair the object's . . . availability for use in an official proceeding" commits a federal crime); MODEL PENAL CODE § 241.7 (person commits obstruction of justice if, believing an investigation is pending, he either "alters, destroys, conceals or removes" a document or "makes . . . any record, document or thing knowing it to be false and with purpose to mislead a public servant who is . . . engaged in such . . . investigation").

334. *About*, ANTI-FORENSICS, http://www.anti-forensics.com/introduction (last visited Feb. 22, 2011). The website's subtitle is "Rendering computer investigations irrelevant." *Id. See also* Darrin J. Behr, *Anti-Forensics: What It is, What It Does, and Why You Need to Know*, 255 N.J. LAW. 9, 10 (2008) (noting that anti-forensics is the term used to reference "developments dedicated to the idea of manipulating data to undermine the reliability of digital forensic investigations").

335. *See, e.g.*, Behr, *supra* note 334, at 10–13 (discussing the types of anti-forensic methods applied to undermine digital forensics"); *Anti-forensic techniques*, FORENSICS WIKI, http://www.forensicswiki.org/wiki/Anti-forensic_techniques (last visited Feb. 22, 2011) (describing various techniques designed to counter forensic investigation methods).

its use.[336]

Computer anti-forensics gives non-expert computer users the ability (i) to eliminate or obfuscate computer-generated evidence or (ii) to make the process of investigating a computer crime so complex, time-consuming and expensive that the inquiry may not proceed.[337] It essentially automates the process of obstructing justice by destroying, altering hiding and/or creating evidence.[338]

Anti-forensics automates the process of obstructing justice in the investigation of digital crimes. Might nanotechnology some day play a similar role with regard to the investigation of physical crimes?

As anyone who has watched *CSI* on TV, seen a movie involving the investigation of a crime, or read a murder mystery knows, investigations of physical crimes focus on the place—the scene—where the crime was committed. Modern crime scene investigation is based on a principle enunciated by Edmond Locard in 1920, which is that "the criminal leaves marks at the crime scene of his passage" and "takes with him, on his body or on his clothing, evidence of his stay or of his deed."[339] Modern technologies—including DNA—have reinforced the importance of Locard's principle: however clever a criminal is, however much she tries to conceal what she did, she inevitably leaves trace evidence establishing her presence at the scene of the crime and takes trace evidence from the scene with her.[340]

At least, that is where things stand today. I found an interesting nanotech-crime-scene scenario in a short story by science-fiction writer A.M. Dellamonica.[341] In the story, humans have fled Earth and are living as refugees on a planet inhabited by aliens who call themselves the Kabu but whom humans call "the Squids," given certain aspects of their physical appearance.[342] In the middle of the night, a woman arrives at a building in the

336. *See* Scott Berinato, *The Rise of Anti-Forensics*, CSO ONLINE (June 8, 2007), http://www.csoonline.com/article/221208/the-rise-of-anti-forensics?page=1 (discussing the growing problem of anti-forensic measures); *Directory: Anti Forensic Tools*, SECURITY WIZARDRY.COM, http://www.networkintrusion.co.uk/index.php/products/Forensic-Solutions/Anti-Forensic-Tools.html (last visited Mar. 9, 2011) (listing various sources of anti-forensic information and software).

337. *See, e.g.*, Behr, *supra* note 334 at 13 (providing a synopsis of the overall danger that is presented by anti-forensics).

338. *See also Antiorensic Overview*, COMPUTER FORENSICS AND ANTI-FORENSICS RESEARCH, http://www.forensics-research.com/index.php/anti-forensics/antiforensic-overview/(last visited Feb. 22, 2011) (defining anti-forensics as "[a]ttempts to negatively affect the existence, amount and/or quality of evidence from a crime scene") (quoting Marc Rogers). Many note that anti-forensic tools also have legitimate uses, such as protecting individual privacy. *See* Behr, *supra* note 334, at 11, (discussing the possible positive usages of digital anti-forensics).

339. John Horswell & Craig Fowler, *Associative Evidence – The Locard Exchange Principle*, *in* THE PRACTICE OF CRIME SCENE INVESTIGATION 47 (John Horswell ed. 2004) (translating Locard's statement from the original French). *See also id.* at 45–48 (discussing criminal forensics and Locard's contributions). John Fuller, *Who Was Edmond Locard?* HOWSTUFFWORKS, http://science.howstuffworks.com/locards-exchange-principle1.htm (last visited Feb. 22, 2011) (describing how Locard was known as the Sherlock Holmes of France).

340. *See, e.g.*, IAN K. PEPPER, CRIME SCENE INVESTIGATION: METHODS AND PROCEDURES 13–25 (Open U. Press ed. 2005) (discussing the packaging of trace evidence in criminal investigations).

341. A.M. Dellamonica, *The Town on Blighted Sea*, *in* THE YEAR'S BEST SCIENCE FICTION: TWENTY-FOURTH ANNUAL COLLECTION 589 (Gardner Dozois, ed., 2007).

342. *Id.* at 589–90 (introducing the story's setting and characters).

refugee area, having been called there by her nephew.[343] She knocks on the designated apartment door and when her nephew opens it, she sees a dead human female and a dead male Squid; her nephew says the Squid killed the woman and he killed the Squid.[344]

The first thing the woman—a police officer on Earth—does is to unpack "an assortment of sprays and other nanotech she'd" assembled before leaving Earth.[345] She sprays "nanosols onto a towel" and uses it to wipe several areas before laying it on the floor and having her nephew walk on it "a couple times" before he moves into the hallway.[346] She then uses another spray—one that "devours dead skin cells . . . , hairs, sweat, tears, blood—anything that might leave a trace" to remove other evidence that may have been left at the crime scene.[347]

There, then, is a fictional example of nano-anti-forensics. As we saw above, digital anti-forensics tools are usually employed *ex ante*, i.e., prior to the time a crime is committed or while the crime is being committed. In this fictional scenario, the aunt uses the nano-anti-forensics techniques *ex post* to clean up the crime scene after the crime has been committed; this might not have been necessary if the nephew had utilized the second anti-forensics spray before entering the apartment and committing the crime. If that tool prevented him from leaving trace evidence, he would not have to clean up afterward, though he might want to use this tool or a similar tool to remove any trace evidence he collected at the crime scene before he left it.

Tools such as this obviously do not exist, but the possibility that they may some day be developed does not seem outside the realm of possibility. The Environmental Protection Agency and other entities are studying how nanoparticles can be used to clean polluted sites by "absorbing contaminants and transforming them into nontoxic forms."[348] In the story, the "nanosols" seem to "eat" trace evidence; instead of consuming pollutants, the environmental clean up nanoparticles transform them into something else, which could presumably also work in the nano-anti-forensics context. The purpose is to defeat Locard's principle by ensuring that no identifiable trace evidence from the perpetrator is left at the crime scene, and that no identifiable trace evidence from the crime scene is found on the perpetrator. If the nano-anti-forensic tool transforms trace evidence of either type into something else, i.e., transforms skin cells into dust, that seems to serve the purpose.[349]

---

343. *Id.* at 590 (setting up the main plot of the story).

344. *Id.* at 590–91 (describing the scene of the crime).

345. *Id.* at 592.

346. *Id.*

347. *Id.* at 593 (utilizing tools "developed . . . to keep . . . investigators from contaminating crime scenes").

348. U.S. ENVIRONMENTAL PROTECTION AGENCY, USING NANOTECHNOLOGY TO DETECT, CLEAN UP AND PREVENT ENVIRONMENTAL POLLUTION, (2009), http://www.epa.gov/nanoscience/quickfinder/pollution.htm. *See also Chemical Engineers Call on Nanoparticles to Combat Polluted Groundwater*, SCIENCEDAILY (Apr. 1, 2008) http://www.sciencedaily.com/videos/2008/0404-nanotechnology__cleaning_up_our_water.htm, (discussing the efforts of a chemical engineer at Rice University in Houston to develop nanoparticles made out of gold and palladium to get rid of chemical pollutants).

349. *See* Behr, *supra* note 334 and accompanying text (discussing the deletion of data). As noted above,

My other fictional example of nano-anti-forensics involves an *ex ante* evidence destruction tactic. In Ian McDonald's book *Brasyl*, which is set partially in the Sao Paolo of 2032, a man uses a one-shot disposable handgun to kill a woman.[350] He takes the gun out, pulls "the strip" on it ("it began to decompose immediately"), points it at the woman, pulls the trigger and it fires.[351] He throws the gun into the gutter, where it dissolves into "black . . . liquid and drips from the rungs of the grating into the sewer."[352] McDonald does not specifically identify the dissolving gun as a nanotech-weapon, but I assume that is what he meant the reader to infer; nanotechnology, after all, seems the obvious technology for creating such a weapon.

This is another approach to destroying trace evidence or, perhaps in this instance, traceable evidence.[353] If the gun had not dissolved but was found in the gutter, ballistics experts would have been able to identify what kind (model and caliber) of gun it was. They might have been able to use its serial number to trace it to the store that sold it to someone, perhaps the shooter, perhaps someone else. They would certainly have been able to identify the striations the gun left on a bullet when it fired and match markings on the cartridge case to marks in the gun's chamber and breech.[354] They might also have been able to find fingerprints on the gun.

My point is that while investigators would not have known who the shooter was, they might have been able to find him by tracing evidence derived from the gun. Since the gun self-destructed, they were denied that opportunity. Even if a witness identified a man as the shooter, police would have no additional evidence they could use to prove his guilt. Whatever trace evidence he left on a busy street corner in Sao Paolo would have disappeared by the time they arrived at the crime scene, and they had no murder weapon. If we assume the bullet did not self-destruct after arriving at its destination, investigators could have analyzed the markings on it, which would have allowed them to link the bullet to the gun . . . if it still existed. If the bullet did self-destruct after inflicting the necessary damage on the victim, then that option disappears, as well.

The self-dissolving gun suggests another technique, another way to eliminate the murder weapon: assume John Doe wants to kill his elderly uncle so he can inherit the uncle's money. Doe wants to commit the murder without being caught; he decides the best way to do that is to invest in a sophisticated

---

computer anti-forensics do something very similar. *See also Field Practice of Anti-Forensics*, SLC SECURITY (Sept. 12, 2009), http://website.slcsecurity.com/index.php?option=com_content&view=article&id=124:field-practice-of-anti-forensics&catid=38:complap&Itemid=106 (describing trail obfuscation).

350. IAN MCDONALD, BRASYL 27–28 (2007).

351. *Id.* at 27.

352. *Id.* at 28.

353. Trace evidence tends to be associated with Locard's principle, which focuses on a crime scene. *See supra* note 339. We literally have a crime "scene" in this case, but it is not the kind of fixed, stable scene from which trace evidence could be collected. It seems, therefore, more precise to refer to "traceable evidence" in this context, i.e., to evidence that can be traced to a given source regardless of where it is found.

354. *See, e.g.*, *Ballistic Fingerprinting*, WIKIPEDIA, http://en.wikipedia.org/wiki/Ballistic_fingerprinting (last visited Feb. 22, 2011). *See also Bullet Identification*, FIREARMSID.COM, http://firearmsid.com/A_BulletID.htm (last visited Feb. 22, 2011).

murder weapon. He contacts a friend, who has contacts in the netherworld where technology and crime intersect. The friend obtains a nano-poison that is guaranteed to be lethal and to self-destruct at least within an hour of entering the victim's body. Doe drops by his uncle's house, where he shares a glass of wine with his uncle; Doe insists on opening the wine and pouring glasses for both of them, in the course of which he slips the nano-poison into the uncle's glass. After they have their wine, Doe leaves. The next day, he receives a call, telling him his uncle is dead, apparently of a heart attack.[355]

Here, Doe left trace evidence at the crime scene, but that does not matter because no one knows it is a crime scene. His presence at the crime scene on the day his uncle died is not suspicious because he often visited his uncle. Unless he admits to the crime, or his friend turns him in, Doe has committed the perfect crime.

Obviously, it will be a long time before lawyers and law enforcement officers actually have to deal with scenarios like these. And they may not ever come to pass. I, for one, would prefer to believe that those trained in nanotechnology will not be inclined to use their expertise to help facilitate crimes. Even if that turns out to be true, at least two of these fictional scenarios involve the criminal exploitation of techniques that were developed for legitimate purposes.

In the first scenario, the spray the aunt used to clean the crime scene of trace physical evidence was developed for a legitimate purpose, i.e. so investigators would not contaminate a crime scene.[356] It is far from inconceivable that a product developed for a legitimate use would find its way into criminal hands. In the nano-poison scenario, I described the nano-product Doe used to kill his uncle as a "poison;" it might be a poison or it might be a product with a legitimate medical use that could be employed for an illegitimate purpose. Assume the nano-product is supposed to be injected into the heart of patients who are suffering a specific defect in the way their heart functions; the nano-product remediates that defect. Doe's uncle's heart did not have that or any other defect. By having his uncle consume the nano-product in a glass of wine, Doe guaranteed that it would migrate to his uncle's heart and attempt to remediate a defect that did not exist. In so doing, it killed him and eliminated all traces of itself afterward.

Even the dissolving handgun might be an instance in which a legitimate product was exploited for illegitimate reasons. I have a difficult time coming up with a legitimate use for such a weapon, but it might be something a government's covert operatives would find useful. If so, it would probably not be surprising if the product found its way into civilian hands.

The availability of nano-anti-forensics might create legal questions beyond whether someone who used such a technique to destroy evidence could be prosecuted for obstructing justice. One issue that might arise is whether nano-anti-forensics devices should be illegal, i.e., whether creating, marketing

355. For a similar nano-poison scenario, *see* Boucher, *supra* note 1, at 219 (describing nano-poison that precisely targets a specific organ and therefore does not leave trace evidence throughout the victim's body).

356. *See* Dellamonica, *supra* note 341, at 593 and accompanying text.

and/or possessing nano-anti-forensics should be a crime.[357] This issue would arise only for the nano-anti-forensic devices that were deliberately created for the specific purpose of destroying evidence, and the permissibility of criminalizing such devices would depend, at least in part, on the extent to which their only use was for criminal activity, i.e., obstructing justice.[358] When a legitimate product was used as a nano-anti-forensics device, the issue might arise as to whether the person(s) who supplied the device to the criminal could be held liable for aiding and abetting the resultant crime(s).[359]

Before we leave this category, I want to note a particularly intriguing "tool" scenario outlined in a recent law review article. In *Nanotechnology and the Attribution of Responsibility*, Professor Katrina Sifferd discusses the possibility that nanotechnology could be used to implant "the mental states relevant to [criminal] responsibility."[360] She uses this example to illustrate how that might be done:

> Craig . . . had perfectly normal sexual desires until he . . . [met] a woman named Susan. They dated briefly before Craig decided to break up with her. To get her revenge, Susan abducted Craig and used nanotechnology to hyperstimulate his hypothalamus, and to connect the hypothalamus activity to a strong representation of young boys. As a result, Craig now has the desire to have sex with young boys.[361]

Here, the "tool" crime (if any) would presumably be Susan's manipulating Craig so he has sex with young boys in violation of the law. Susan could obviously be prosecuted for assault, but that would not address the consequential effects of her attack on Craig, i.e., the crimes against the children. Under Model Penal Code § 2.06(2)(a),[362] Susan could be held guilty of Craig's crimes under an accomplice theory, i.e., she caused an otherwise innocent person to commit them.[363]

---

357. At least one U.S. state takes this approach to malicious computer software, e.g., viruses, worms, Trojan horse programs. *See* 18 PA. CONS. STAT. ANN. § 7612 (LexisNexis 2010) ("A person commits an offense if he intentionally or knowingly engages in a scheme or artifice, including, but not limited to, a denial of service attack upon any computer, . . . or any part thereof that is designed to block, impede or deny the access of information . . . ."). For an analysis of this approach to computer malware, *see, e.g.*, Susan W. Brenner, *Burglar's Tools,* CYB3RCRIM3 (July 7, 2008), http://cyb3rcrim3.blogspot.com/2008/07/burglars-tools.html [hereinafter Brenner VIII] (stating that many U.S. states, including New York and Connecticut, outlaw the possession of burglary tools).

358. *See generally* State v. Bui, 92 P.3d 471, 475 n. 3 (Haw. 2004) (analyzing the constitutionality of criminalizing possession of burglar's tools). *See also* ALASKA STAT. § 11.46.315 (2010) (criminalizing the possession of burglary tools with intent to use); VT. STAT. ANN. tit. 13, § 1204 (1981) (criminalizing a person who possesses burglar's tools with intent to use such tools for the purpose of committing burglary).

359. *See, e.g.*, Brenner VIII, *supra* 357 (stating that statutes outlawing manufacture of burglar's tools are based on accomplice liability).

360. Katrina L. Sifferd, *Nanotechnology and the Attribution of Responsibility*, 5 NANOTECH. L. & BUS. 177, 188–89 (2008).

361. *Id.* at 186 (footnotes omitted).

362. "A person is legally accountable for the conduct of another person when . . . acting with the kind of culpability that is sufficient for the commission of the offense, he causes an innocent . . . person to engage in such conduct. . . ." MODEL PENAL CODE § 2.06(2)(a) *See also id.* § 2.06(1) ("A person is guilty of an offense if it is committed by his own conduct or by the conduct of another person for which he is legally accountable, or both.").

363. *See, e.g.*, Morrisey v. State, 620 A.2d 207, 209–11 (Del. 1993) (affirming the lower court's ruling that the defendant's criminal liability for unlawful sexual intercourse "could be predicated upon his actions

c. Technology incidental

As noted earlier, when computer technology plays an incidental role in the commission of an offense its involvement is so minimal it does not rise to the level of transforming the crime into a tool crime.[364] We could simply ignore the computer's involvement in the offense, just as we ignore the involvement of other, more routine technologies, e.g., electric light, telephones, even automobiles. The rationale for including the "incidental" category in the taxonomy used to classify computer-related crimes is that the computer can be an important source of evidence about the crime and the person(s) who committed it.[365] In other words, the assumption is that the computer plays a more active role in the commission of the crime than other, more passive technologies and consequently is more likely to be a source of useful evidence.

As others have noted, criminals could use nanotechnology to disguise their identities while committing crimes.[366] They might do this simply to avoid being caught and prosecuted; or they might use nanotechnology to create "biometric spoofs" that let them circumvent "biometric security detectors" and gain entry to the premises where they intend to commit a crime.[367] In other words, nanotechnology could in effect become a biometric lock pick.[368]

The production, sale and consumption of illegal drugs has for years been a major source of criminal activity. Nanotechnology might take that to the next level by facilitating the creation and marketing of new drugs and/or drug surrogates.[369] By "drug surrogates," I mean substances that are not chemically based but when ingested have effects similar to that of substances such as cocaine, heroin, LSD, etc. Nanotechnology might be used to create non-chemical surrogates that influence the human body in ways that differ from, but are analogous to, those associated with chemically based substances like cocaine. It might be possible to customize the user's experience in terms of factors such as the length, intensity and nature of the "high" that results from consuming a nano-surrogate.[370] And nano-drug surrogates would offer drug dealers an option they currently do not have: designer drugs, i.e., the ability to create new and newer surrogates to maintain or expand their customer base.[371] And since nano-drug surrogates would not be chemically based, it might be

through the instrumentality of an innocent intermediary"). Since Craig was innocent, he should not face any criminal liability. *See id.* at 211 (stating that innocent persons manipulated into committing crimes are not guilty).

364. *See supra* Part III.A.1.

365. *See supra* Part III.

366. *See, e.g.*, Frederick A. Fiedler & Glenn H. Reynolds, *Legal Problems of Nanotechnology: An Overview*, 3 S. CAL. INTERDISC. L.J. 593, 623 (1994) ("Imagine criminals disguising their . . . fingerprints, retinal patterns, blood types, or even genetic materials . . . ."). *See also* Webb, *supra* note 269 (stating that "falsification of identification is going to be simple with nanotechnology").

367. BOUCHER, *supra* note 1, at 219. *See* Brenner VIII, *supra* note 357 and accompanying text.

368. *See* BOUCHER, *supra* note 1, at 218–19 (explaining how "nanotechnology has the potential to provide new techniques" for attacking security systems employed with biometric security detectors).

369. *See* Webb, *supra* note 269.

370. *See id.* ("They can be made highly addictive and highly pleasurable without nasty side effects.").

371. *See id.* (stating that nanotechnology enables "the creation of a never-ending variety of new drugs").

easier for those engaged in their manufacture to conceal their operations from the authorities.[372]

It is difficult at this point in time to project all the ways in which nanotechnology might incidentally contribute to the commission of various crimes, just as it would have been difficult for someone writing in, say, 1977 to imagine the many and varied ways computer technology would contribute to criminal activity. These examples, I hope, illustrate how nanotechnology may be integrated into the commission of known crimes; it may also be that nanotechnology, like computer technology, gives rise to a class of previously unknown crimes, in which it plays a role of greater or lesser importance.[373]

B. Lessons Learned?

As I have noted elsewhere,[374] one lesson I believe we have learned from our experience with cybercrime is to be parsimonious in adopting new, technologically specific criminal laws. When cybercrime was still a very new phenomenon, some jurisdictions tended, at least in my opinion, to over-react by adopting laws that were specifically directed at computer-facilitated analogues of crimes they had already outlawed.[375]

Some U.S. states did this with harassment: U.S. states began criminalizing harassment about a century ago, as it became clear that telephones could be used for new and unintended purposes, i.e., to make obscene and otherwise harassing phone calls.[376] States responded to this new technological crime by adopting use-of-a-telephone-to-harass statutes.[377] About eighty years later, as computers began to be used for the same purpose, some states simply added a new crime, i.e., they adopted use-of-a-computer-to-harass-statutes.[378] Since criminal law is focused on the infliction of "harms" rather than on technology, as such, the better approach would have been to incorporate computer harassment into the telephone harassment statutes the states had adopted years earlier.[379] Aside from anything else, the unnecessary use of technologically specific laws has certain disadvantages:

---

372. *See id.* (stating that nanodrugs could be developed with "no obnoxious fumes to give away locations").

373. As is perhaps apparent from the discussion of nanotech-crimes in this section and the review of computer crimes in Part III.A.1, the distinction between crimes in which technology plays a "tool" role versus those in which it plays an "incidental" role is far from precise. Essentially, a crime will fall in the "tool" category if the technology plays an active role in committing the crime, such as the role computer technology plays in hacking or the dissemination of malware.

In the discussion above, nanotechnology obviously plays a pivotal role in creating and producing the new nano-drugs. That might lead some to put this alternative in the "tool" category. I assigned it to the "incidental" category because while nanotechnology's role is essential in this scenario, it is at once a passive and secondary role.

374. *See, e.g.*, Brenner VII, supra note 255, at 761–84 (arguing against the adoption of technology specific criminal laws).

375. *See, e.g.*, *id.* at 768–69 (discussing the laws enacted by legislators dealing with telephone harassment).

376. *Id.* at 768.

377. *Id.*

378. *Id.* at 768–69.

379. *Id.* at 769–70.

> It produces overlapping rules (e.g., rules outlawing theft, rules outlawing the use of computers to commit theft, and rules outlawing the theft of computers). The focus on method instead of result also produces rules that are transient. We began with use-of-a-telephone-to-harass rules and added use-of-a-computer-to-harass rules; this leaves us . . . with rules that may or may not overlap (for example, if one uses a computer to access a telephone line and uses that connection to harass another, is this use-of-a-telephone-to-harass, use-of-a-computer-to-harass, or both?). As technologies converge and the distinction between a 'telephone' and a "computer" erodes, this approach may take us back to where we began, with a "harm" (harassment by an as-yet unimplemented technology) that is not proscribed by existing law. And, finally, the focus on method becomes increasingly untenable as our "use" of technology ceases to be a segmented, compartmentalized part of our lives and becomes an integral, invisible part of our everyday lives.[380]

The adoption of technologically specific harassment legislation is but one example of how many jurisdictions responded to the rise of computer crime.[381] The question is, will we respond to nanocrime in a similar fashion?

Nanocrimes differ from real-world crimes and from cybercrimes in at least one respect: In real-world crimes, the perpetrator physically commits the crime himself (perhaps with the assistance of accomplices). In cybercrimes, the perpetrator also physically commits the crimes himself, using computer code as the intermediary device by which he acts "in" the virtual world of cyberspace.[382]

In nanocrimes, the perpetrator's role may be much more attenuated, more analogous to that of someone who sends malware out to wreak generalized havoc on computers than it is to the hands-on role of traditional criminals and most cybercriminals.[383] Nano-perpetrators will presumably operate in a fashion analogous to that of our fictional Dr. X., i.e., they will create[384] nanoparticles that are designed to implement their criminal schemes and send them out to do the dirty work. From what I know of the current state of nanotechnology, my sense is that nanoparticles will be created to perform particular functions (like finding a stent and offloading their drug cargo to it) autonomously. In that regard, they are again analogous to malware (though unlike malware it appears that they will be able to carry out tasks that could

380. *Id.* at 769 (footnotes omitted).

381. There were areas in which we needed to adopt new laws, i.e., DDoS attacks, but they were rare. Brenner IV, *supra* note 124, at 76.

382. This may be less true for certain types of malware, which can be programmed to take certain actions on its own or even operate autonomously. In that respect, malware may be more analogous to nanocrime than it is to real-world and cybercrime. *See, e.g.*, *MessageLabs '09 Report: Botnets Bounce Back with Sharpened Survival Skills*, DARK READING (Dec. 11, 2009), http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=222001767 ("It is predicted that in 2010 botnets will become autonomous[ly] intelligent, with each node containing an inbuilt self-sufficient coding in order to coordinate and extend its own survival.").

383. *See Id.* (describing how to create spams).

384. Or, perhaps, they will appropriate the nanotools they need from others and then either apply them or modify them for a particular criminal use.

directly inflict physical "harm" on human beings).[385]

If all of that is true, and if nanotechnology does not progress beyond the point at which nanoparticles are simply programmed to perform limited functions and then launched to do just that, it seems we could use malware laws as the basis for developing nano-crime laws. In other words, if nanotechnology does not evolve to the point at which nanoparticles are capable of independent (some level of artificial intelligence) or derivative (ability to extrapolate from basic functions to perform functions derived from that set of behaviors) action, it may simply become a tangible manifestation of malware.[386]

More difficult questions will arise if nanotechnology progresses beyond simple artificial intelligence and develops the capacity for truly intelligent, autonomous action. If that eventuates, and if the evolved nanotechnology engages in activity we define as criminal, we would have to decide how criminal law should address either or both of two scenarios.

The first scenario, the "Frankenstein scenario," focuses on how law should deal with a human being who intentionally creates nanoentities that have the capacity for independent action and releases them into a context in which they can function, knowing that their actions will be foreseeable for some period of time but may at some point evolve beyond what their creator intended or foresaw. If the nanoentities inflicted "harms" that come within the traditional scope of the criminal law,[387] we would have to decide whether to hold the creator liable (i) only for the "harms" he foresaw and/or intended or (ii) for both those "harms" and for the unintended and unanticipated "harms" the infliction of which was a proximate result of releasing the entities.

The second scenario takes us even further into a science fiction reality: if the scenario outlined above were to occur, we might also have to decide whether we would want to treat semi-intelligent, autonomous constructs as entities subject to the imposition of criminal liability. In other words, we might have to decide whether criminal law—or a type of criminal law—could apply to autonomous, intelligent nano-constructs.[388]

---

385. *See supra* Part III.A.1.

386. One possible problem with approaching nanotechnology as if it is an analogue of malware is that, as noted above, malware is evolving intelligence and the capacity for autonomous action. *See supra* note 382. If malware achieves intelligence and autonomy but nanotechnology does not, analogizing the two may become increasingly untenable. If malware and nanotechnology both achieve intelligence and autonomy, we might be able to use similar laws to address the criminal exploitation of each technology.

We would probably want to use similar laws rather than the same law because the "harms" each inflicts are likely to be focused on different venues, i.e., malware will presumably remain a creature of the digital world while nanotechnology will presumably remain a real-world phenomenon.

387. For a scenario in which this occurs inadvertently, *see* LERNER, *supra* note 54.

388. While we have not yet done so, the notion of holding a nonbiological entity criminally liable has arisen. On several occasions, robots have killed human beings. *See, e.g.*, Jennifer McLain, *La Puente Woman Crushed by Robot at McDonald's Supplier in Industry,* SAN GABRIEL VALLEY TRIB., July 22, 2009; *Robot Cited in Man's Death,* CHI, TRIB., Oct. 13, 1986, at C3; JAPAN ECONOMIC NEWSWIRE (Feb. 18, 1983) (explaining that two workers were fatally crushed between manipulating arms of robots and machine tools). There was no attempt to prosecute the robots in question because none of them was intelligent and autonomous.

If we ultimately decide to prosecute non-biological entities, the deodand might serve as something of a precedent. *See, e.g.*, Anna Pervukhin, *Deodands: A Study in the Creation of Common Law Rules*, 47 AM. J.

IV. CONCLUSION

It is not surprising that it took years before American lawmakers realized the need to take computer crime seriously by adopting legislation that criminalized certain kinds of computer-facilitated activity. When personal computers were introduced, coincidentally with the Internet, no one had any reason to anticipate that the interaction of the two would create new and unprecedented opportunities for criminal activity.

Personal computers were only the latest in a series of communications technologies—telephones, radio, television, motion pictures—that appeared between 1880 and 1980.[389] Three of the technologies—radio, television and motion pictures—had essentially no capacity to be exploited for criminal purposes because each was a passive communications technology, i.e., each content was broadcast to an audience whose only options were to accept or reject it.[390] Telephones had some capacity to facilitate criminal activity; phones could be used to facilitate fraud and to harass others anonymously.[391] It was a relatively simple matter for legislators to adopt statutes criminalizing the use of telephones (or "the wires") to commit fraud and other crimes, including harassment.[392]

Given our history with technology to that point, it is not surprising that no one anticipated the extraordinary opportunities networked computers would create for enterprising criminals. Nor is it particularly surprising that it took years for legislators to adopt laws that adequately addressed computer-facilitated criminality. Neither the legislators nor law enforcement nor the general public had a model of technologically facilitated crime they could use as a guide in understanding what needed to be done to respond to the new wave of computer crimes.

We *might* be approaching a new era of technologically facilitated crime—the nanocrime examined in this article. Whether nanocrime emerges and whether it becomes a matter of serious concern depend, as noted earlier, on the extent to which nanotechnology evolves from a "laboratory" technology to a "democratic" technology. If nanotechnology remains a "laboratory" technology, its potential for criminal exploitation will be essentially non-existent; if, on the other hand, nanotechnology becomes a "democratic" technology, its potential for criminal exploitation rises, perhaps equaling or exceeding that of computer technology.

I, obviously, have no way of knowing whether nanotechnology will make the transition to "democratic" technology or not, and neither I nor anyone else at this point has any way of knowing the extent to which nanotechnology will

---

LEGAL HIST., 237, 256 (2005) (summarizing the effects of the evolution of deodand law as it encountered novel problems).

389. *See, e.g.*, Brenner VII, *supra* note 255, at 708–43 (illustrating the development of personal computers and communication technology).

390. *Id.* at 725–29.

391. *See, e.g.*, Brenner IV, *supra* note 124, at 12 (stating that the rise of the telephone produced anti-social behaviors). *See also supra* notes 376–71 and accompanying text.

392. *See supra* notes 376–71 and accompanying text.

be used for criminal purposes if and when it makes this transition. As I noted earlier, my purpose in writing this article is not to answer these questions. It is to raise them and, in so doing, encourage those of us who have expertise in crime and criminal law to do what our counterparts could not do thirty-odd years ago: (i) educate ourselves about this emerging technology's capacity to facilitate the commission of crimes and (ii) monitor the development (if any) of such a capacity and anticipate how criminal law should respond if and when it appears. In other words, my goal is to encourage an effort that is the criminal counterpart of the efforts that are underway to develop civil regulatory systems that can respond to the inadvertent hazards associated with nanotechnology.