Taming the Internet Wild:
Punishing and Deterring Virus-Creators and Script Kiddies Through Victim-Offender Mediation*

Ian Best

I. INTRODUCTION

When a teenager creates a computer virus, he does not always have the desire to send it out himself.[1] The creation of the virus is often sufficient to give him pleasure.[2] But once he posts his new virus on the Internet he has no control over the "script kiddies," the less experienced members of the virus underground who download and tinker with other people's viruses and then send them out "into the wild."[3] The actual creator of the virus is thus detached from the harm done by its use.[4] As one virus-creator, Dark Avenger, said, "I wrote the virus so it would be killed…. It was not supposed to do all this."[5] How are such crimes to be punished, when the initiators of the computer viruses can truthfully say that they had no intention of causing the harm that ultimately resulted from their creation?[6] And how does one penalize the script kiddies

---

* By Ian Best, graduate of the Michael E. Moritz College of Law, The Ohio State University, class of 2006. This unpublished student note was written as a required assignment for the *Ohio State Journal on Dispute Resolution*. It is available at http://3lepiphany.typepad.com/3l_epiphany/2006/10/taming_the_inte.html.

[1] Clive Thompson, *The Virus Underground*, N.Y. TIMES MAGAZINE, Feb. 8, 2004 at 28, available on Lexis.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Sarah Gordon, *Inside the Mind of Dark Avenger*, 1993, *available at* www.research.ibm.com/antivirus/SciPapers/Gordon/Avenger.html

[6] Thompson, *supra* note 1.

who often have no realization that the viruses they send out can be catastrophic in their consequences? [7]

Creators and distributors of computer viruses, who are often juveniles, may cause substantial damage far beyond what they envisioned. [8] As a computer security officer has said, "There are people who would never toss a Molotov cocktail into a warehouse, but they wouldn't think for a second about launching a virus."[9] To properly punish a young offender who creates or sends out a virus is inherently problematic, because the harm can be so far out of proportion to the criminal act. [10] Just as it has been recognized that cybercrimes in general necessitate new legal considerations, punishment for computer virus crimes requires a new approach.

One possibility is victim-offender mediation (VOM), which has been used to punish juvenile offenders for crimes similar to virus-creation like vandalism. VOM would force the virus-creator or script kiddie to lose his anonymity and confront first-hand the consequences of his actions. This would be a fitting punishment for young people who are oblivious to the damage resulting from their activity. Furthermore, the victims of computer viruses would be enabled to confront the source. Computer users who are frustrated with the onslaught of virus infections would have an opportunity to be part of the system that remedies the harm. Future virus-creators and script kiddies would be deterred, knowing that if they are caught they will have to face their victims. And the state's interest in punishing and deterring crime would be fulfilled.

---

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

This note examines the problem of computer viruses and offers victim-offender mediation as a solution. Computer viruses are defined and explained in Part II. The general scope of the virus problem is described in Part III. Then Part IV examines the virus-creators and script kiddies who are responsible for this new crime. Part V elaborates upon why virus-creation is such a difficult crime to prosecute and punish. And Part VI puts forward victim offender mediation as an effective means of punishment for virus-creators and script kiddies.

II. THE DEFINITION, NATURE AND PROBLEM OF COMPUTER VIRUSES

A. *What is a Computer Virus?*

A virus is a piece of computer code that attaches itself to a program or file so it can spread from computer to computer, infecting as it travels. [11] The first computer viruses were benign and were limited to laboratory computers where they could be contained.[12] But because

---

[11] Microsoft, *What are viruses, worms, and Trojans*, March 9, 2004, *available at* http://www.microsoft.com/athome/security/viruses/virus101.mspx?pf=true [hereinafter Microsoft]. See also Eugene H. Spafford, *Cyber-Terrorism: The New Asymmetric Threat*, Prepared Testimony Before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threat and Capabilities, July 24, 2003, available on Lexis. Spafford gives the history of the term 'computer virus':

> The first use of the term virus to refer to unwanted computer code was by Gregory Benford. As related by Dr. Benford in correspondence with me, he published the idea of a virus in 1970 in the May issue of Venture Magazine. His article specifically termed the idea "computer virus" and described a program named Virus — and tied this to the sale of a program named Vaccine to defeat it. All this came from his experience as a programmer and research physicist at the (then) Lawrence Radiation Lab in Livermore. He and the other scientists noticed that "bad code" could self-reproduce among lab computers, and eventually get onto the ARPANet [the predecessor of the Internet].
>
> …

viruses can take on a 'life' of their own, they are able to spread beyond any artificial limitation designed by the virus's creator. [13] The computer code in the virus is written with the express intention of replicating itself. [14]

Computer viruses are "extremely small, hard to locate, and dangerous."[15] Like an organic virus infecting a person, a computer virus disguises itself as a harmless "cell" (program), and hides within the computer. [16] It then attaches itself to other programs and clones itself, seeking to continually infect its host, thus potentially causing substantial damage.[17] Unlike an accidental flaw – a 'bug' – in a computer, a virus is intentionally created with the possibility of causing harm,[18] although the harm itself may be intentional or inadvertent.[19]

Fred Cohen more formally defined the term computer virus in 1983. At that time, Dr. Cohen was a graduate student at the University of Southern California attending a security seminar. Something discussed in class inspired him to think about self-reproducing code. He put together a simple example that he demonstrated to the class. His advisor, Professor Len Adleman, suggested that he call his creation a computer virus.

[13] See e.g. Thompson, *supra* note 1 (describing a young man who got in trouble with Spanish authorities because a virus he designed escaped into the wild when it behaved unpredictably).

[14] See Microsoft, *supra* note 11.

[15] Mark Colombell, *The Legislative Response to the Evolution of Computer Viruses*, 8 RICH. J. L. & TECH. 18 (Spring 2002).

[16] *Id.*

[17] *Id.*

[18] Spafford, *supra* note 11. (noting difference between a common 'bug,' in which the computer code causes damage by accident, and 'malware' or 'vandalware' such as computer viruses, in which the computer code is intentionally and maliciously designed to cause harm).

[19] *Id.*

B. *How a Computer Virus Spreads.*

A virus does not spread without human action to move it along, such as sharing a file or sending an e-mail.[20] Most viruses are spread through email attachments. The virus is sent as a file attached to an email message, and is launched when the attachment is opened.[21] Many viruses are able to spread further by collecting information from personal email programs and sending themselves to everyone listed in the address book.[22] Viruses can also spread through observing the in-box of the infected computer and sending automatic replies in response with the same email subject.[23] Victims of viruses can get also them from Internet downloads and borrowed computer disks, but by far the most frequent way is through opening an email attachment.[24]

C. *How a Computer Virus is Like a Biological Virus.*

The term 'computer virus' is derived from the fact that it is analogous to a biological virus invading the human immune system.[25] A virus is simply "a computer program file capable

---

[20] *Id.*

[21] *Id.*

[22] The "Love Bug is one such example of a virus which sent itself to every email address in the user's computer. *See* Mark Landler, *A Filipino Linked to 'Love Bug' Talks About His License to Hack,* October 21, 2000, at C1. *See also* Frank Thorsberg, *The World's Worst Viruses*, August 23, 2002, *available at* http://www.pcworld.com/resource/printable/article/0,aid,103992,00.asp (entry on 'Melissa') ("The e-mail fooled many recipients because it bore the name of someone the recipient knew and referred to a document they had allegedly requested. So much e-mail traffic was generated so quickly that companies like Intel and Microsoft had to turn off their e-mail servers.")

[23] Thorsberg, *supra* note 22 (entry on 'Exporer.zip Worm').

[24] See Microsoft, *supra* note 11.

[25] Spafford, *supra* note 11. Spafford elaborates:

of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission."[26] Viruses can cause damage by attaching to files so that when the infected file executes, the virus also is activated.[27] They can also wait in a computer's memory and infect files as the computer opens, modifies or creates the files. A virus does not need to express symptoms or cause damage to be labeled a virus.[28]

Computer viruses bear enough similarities to biological ones that models of 'computer virus epidemiology' have been constructed.[29] Epidemiological terms related to biological viruses have been borrowed from medicine and utilized for analyzing computer virus outbreaks and

---

> The word virus itself is Latin for poison. Biological viral infections are spread by the virus (a small shell containing genetic material) inserting its contents into a far larger host cell. The cell then is infected and converted into a biological factory producing replicants of the virus. Similarly, a computer virus is typically a segment of computer code or a macro that will copy itself (or a modified version of itself) into one or more larger "host" programs when it is activated. When these infected programs are run, the viral code is executed and the virus spreads further.

[26] *Id.*

[27] *Id.*

[28] McAfee Virus Glossary, *available at* http://us.mcafee.com/virusInfo/default.asp?id=glossary [hereinafter McAfee].

[29] Steve R. White, *Open Problems in Computer Virus Research*, October 1998, *available at* www.research.ibm.com/antivirus/SciPapers/White/Problems/Problems.html:

> [One such model] characterizes virus spread in terms of three things: [1.] The birth rate of the virus – the rate at which one infected system can spread the infection to other systems. [2.] The death rate of the virus – the rate at which an infection is found on a system and eliminated. [3.] The pattern (topology) of connections between systems along which viruses spread, whether by program sharing via diskettes, sending infected attachments via email, or other connections yet to come.

strategies to confront them.[30] Although computer viruses are obviously not organic, they are similar to biological viruses in that they "spread from program to program and computer to computer, much as biological viruses spread within individuals and among individual members of a society."[31] The use of medical analogies has created a specific terminology for computer viruses.[32] Computer viruses are also similar to biological ones in their dependence on environmental factors,[33] and in their varying degrees of harm.[34]

---

[30] See Jeffrey O. Kephart et al., *Computers and Epidemiology*, *available at* www.research.ibm.com/antivirus/SciPapers/Kephart/Spectrum/Spectrum.html. Such terms include:

> Birth rate: the rate at which a virus attempts to replicate from one machine to another
>
> Death rate: the rate at which a virus is eliminated from infected machines, usually when the user discovers it and cleans it up
>
> Epidemic: the widespread occurrence of a disease. A disease need not overwhelm a population to be epidemic; it must simply spread through some fraction of it.
>
> Epidemic threshold: the relationship between the viral birth and death rates at which a disease will take off and become widespread. Above this threshold, the disease becomes a persistent, recurring infection in the population. Below it, the disease dies out.
>
> Incident rate: the rate at which virus incidents occur in a given population per unit time, normalized to the number of machines (computers) in the population.
>
> Infected machine: a computer that contains a virus, and can spread that virus to diskettes or other computers.
>
> Prevalence: the degree to which a virus is widespread in a population.
>
> Virus Incident: the infection of a number of machines within an organization by a particular virus, due to a single initial infection from outside the organization.

[31] Jeffrey O. Kephart et al., *Fighting Computer Viruses*, 88 SCIENTIFIC AMERICAN, November 1997.

[32] *Id.* These terms are used to make predictions concerning virus activity. Kephart et al describe one such epidemiological model, but also suggest that this model is inadequate:

D. *Other Computer Virus Attributes and Definitions.*

Viruses can generally be divided into three categories: file infectors, boot-sector viruses, and macro viruses.[35] The computer file to which the virus attaches itself is called a 'host,' and

---

> The simplest models predict the behavior of a disease from a few parameters— most significantly, the "birth rate" at which sick individuals infect others and the "death rate" at which the sick either die or are cured. If the ratio between these two rates is less than a critical value, any infection will quickly die out. The larger the ratio, the more likely an epidemic, and (if there is no immunity) the greater the fraction of the population that will be infected at any one time….
>
> Unless the ratio of the birth and death rates just happens to be close to the critical value, a virus should either die out completely or spread exponentially and become almost universal. Instead many viruses persist steadily at levels that are a small fraction of the overall population. One crucial error in this simple model appears to be in assuming uniform chances of contact among everyone in the population at risk. More sophisticated models take into account the extraordinary cliquishness of typical patterns of software exchange.

[33] *Id.* "Just as external factors such as drought, sanitation and migration have a strong influence on biological epidemics, changes in the computing environment are responsible for the presence of several distinct epochs in viral infection." The article names several changes in the mainstream use of computer software that has impacted the nature and prevalence of different categories of computer viruses.

[34] See Thompson, *supra* note 1.

> "It's like comparing Ebola to AIDS," says Joe Wells, an antivirus researcher and founder of WildList, a long-established virus-tracking group. "They both do the same thing. Except one does it in three days, and the other lingers and lingers and lingers. But which is worse? The ones that linger are the ones that spread the most."

[35] Kephart, *supra* note 31. This article describes how viruses can generally be divided into three technical categories: file infectors, boot-sector viruses, and macro viruses.

> [1. File infectors:] When a user runs an infected application, the virus code executes first and installs itself independently in the computer's memory so that it can copy itself into subsequent

most viruses are programmed to run once an attempt is made to execute the host file.[36] When a virus enters a computer system or storage device, it causes an 'infection.'[37] Once a virus has

---

> applications that the user runs. Once in place, the virus returns control to the infected application; the user remains unaware of its existence. Eventually a tainted program will make its way to another computer via a shared diskette or network, and the infection cycle will begin anew.
>
> [2. Boot-sector viruses:] [These viruses] reside in a special part of a diskette or hard disk that is read into memory and executed when a computer first starts. The boot sector normally contains the program code for loading the rest of a computer's operating system (hence the name, a reference to lifting oneself up by one's own bootstraps). Once loaded, a boot-sector virus can infect any diskette that is placed in the drive. It also infects the hard disk, so that the virus will be loaded into memory whenever the system is restarted. Boot viruses are highly effective: even though there are fewer strains, they were for a time much more prevalent than file infectors were.
>
> [3. Macro viruses:] The third category, macro viruses, are independent of operating systems and infect files that are usually regarded as data rather than as programs. Many spreadsheet, database and word-processing programs can execute scripts—prescribed sequences of actions—embedded in a document. Such scripts, or macros, are used to automate actions ranging from typing long words to carrying out complicated sequences of calculations. And virus writers have created scripts that insert copies of themselves in other documents. Macro viruses can spread much more rapidly than other kinds of viruses because many people share "data" files freely …

Concerning macro viruses, see also Spafford, *supra* note 11.

> Eight years ago we saw the emergence of the macro virus. This is a virus written in a high-level macro language and attached to word-processing documents or spreadsheets. When an infected document is opened on any computer platform supporting the software the macro is activated and spreads itself to other, similar documents on the system. As these documents are shared across networks, the macro viruses spread widely.

[36] McAfee, *supra* note 28.

[37] *Id.*

infected a computer, it engages in 'replication,' in which the virus makes copies of itself in order to carry out subsequent infections. The replication process is one major distinction between viruses and other rogue computer programs.[38] Frequently the original virus is modified, producing a 'variant.' This variant may be designed by the original virus-creator or by another person.[39]

Most viruses, including the ones that draw the most attention and cause the most damage, are said to be 'in the wild,' meaning that they have caused a verified infection outside a laboratory situation.[40] This is in contrast to 'zoo viruses' (which exit in the collections of researchers and have never infected a real world computer) and viruses 'not in the wild' (which are in the real world but fail to spread successfully).[41] Some viruses include a 'triggered event,' in which the virus sets off a particular action after a specific condition is met.[42] Some viruses are created specifically to look for and remove other viruses. However, these viruses can still be destructive.[43]

E. *Viruses which Don't Replicate: Worms*

---

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] McAfee, *supra* note 28 ("Examples include a message displayed on a specific date or reformatting a hard drive after the 10th execution of a program.").

[43] For example, the 'good' virus 'Necchia' attempted to destroy the 'bad' virus 'MSBlast,' but ended up causing almost as many problems by producing an overload of Internet traffic. See Matt Bean, *Prosecuting Internet virus creators is a challenge as big as the Web*, Court TV, Aug. 25, 2003, *available at* http://news.findlaw.com/court_tv/s/20030825/25aug2003123034.html.

One form or subclass of computer virus is a 'worm,' [44] although some researchers put worms in a separate category from viruses. [45] Worms are capable of spreading on their own without inadvertent human assistance, as compared to more typical viruses require human action to spread (such as transferring a file or using an infected computer disk).[46] Therefore it is more difficult to inoculate a computer against a worm than a virus.[47] Worms take their name from the

[44] See Robert M. Slade, *History of Computer Viruses*, *available at* www.cknow.com/vtutor/vtsladecontents.htm. See also Microsoft, *supra* note 11.

[45] Spafford, *supra* note 11. Spafford differentiates worms from viruses:

> Unlike viruses, worms are programs that can run independently and travel from machine to machine across network connections; worms may have portions of themselves running on many different machines. Worms do not necessarily change other programs, although they may carry other code that does, such as a true virus. It is this replication behavior that leads some people to believe that worms are a form of virus…

[46] See Tim Lemke, *Virus creators share code online to create copycats*, THE WASHINGTON TIMES, March 17, 2004, *available at* http://washingtontimes.com/business/20040316-093754-4080r.htm.

[47] *See* White, *supra* note 29.

> A given worm is created and unleashed. It spreads very quickly through its target systems, in many cases creating a much more substantial problem than a run-of-the-mill PC virus. Eventually, it is discovered and eliminated, and steps are taken to help ensure that that particular worm cannot recur. Unlike today's PC viruses, which often constitute a low-level, ongoing infection of the world's systems, worms tend to come and go and not come back. By itself, this is good. But it also means that every worm we see will be a new worm. Unlike PC viruses, from which you can be protected because I happened to find the virus months ago and create a cure, the anti-virus industry will not have time to craft a cure for a worm before you get it.

patterns on printouts that appeared 'worm-eaten.'[48] The destructive power of worms comes from their speed – when they multiply they may generate enough traffic to overwhelm network servers.[49] For example, the sixth version of the SoBig worm, 'SoBig.F,' spread more than 1 billion unwanted e-mail messages in August, 2003, and spread to more computers than any of its predecessors.[50]

F. *Gifts with Malicious Content: Trojan Horses*

One form of malicious software, the Trojan Horse (or Trojan for short), is created with the specific intent to do harm.[51] Trojans are not actually viruses since they do not replicate.[52] Trojans are named for the Trojan horse from Greek mythology which had the appearance of a gift, but contained soldiers who overthrew the city of Troy.[53] A Trojan horse program pretends to be a benign and innocuous application, but when activated does something unexpected and malicious.[54] A Trojan appears to be useful software, but is actually a pernicious program that

---

[48] Slade, *supra* note 44. Attempts to trace the "path" of damage or operation would show "random" patterns of memory locations. Plotting these on a printout map of the memory looks very much like the design of holes in "worm-eaten" wood: irregular curving traces which begin and end suddenly. The model became known as a "wormhole" pattern, and the rogue programs became known as "worms." But see Spafford, *supra* note 11 (describing a science fiction novel, The Shockwave Rider by John Brunner, as the source for the name 'worm,' since programs that traversed networks and carryied information with them were called 'tapeworms' in the novel).

[49] Thompson, *supra* note 1.

[50] *See* Lemke, *supra* note 46.

[51] "The Trojan Horse was the gift with betrayal inside; so a trojan horse program is an apparently valuable package with a hidden, and negative, agenda." Slade, *supra* note 44.

[52] McAfee, *supra* note 28.

[53] See Microsoft, *supra* note 11.

[54] *Id.*

invades and damages the computer. [55] Thus Trojans are designed to attract people into opening a computer program they think is legitimate.[56] For example, one Trojan was attached to an email claiming to bring security updates from Microsoft. [57] If the attachment was opened the Trojan disabled existing antivirus software and firewalls on the computer.[58] Some Trojans are 'logic bombs' that execute when a specific condition occurs.[59] Trojan programs are usually spread via public access electronic bulletin boards so that the creator of the virus cannot be identified.[60]

G. *The Potential Interactions between Viruses, Worms, and Trojans*

---

[55] *Id.*

[56] *Id.* See also Spafford, *supra* note 11. Spafford gives a hypothetical example of a Trojan horse program designed to resemble a game:

> While the program appears to be doing what the user wants, it actually is doing something else entirely. For instance, the user may think that the program is a game. While it is printing messages about initializing databases and asking questions about "What do you want to name your player?" and "What level of difficulty do you want to play?" the program can actually be deleting files, reformatting a disk, or otherwise altering information. All the user sees, until it's too late, is the interface of a program that the user thinks he wants to run.

[57] Microsoft, *supra* note 11.

[58] *Id.*

[59] Spafford, *supra* note 11 (defining a logic bomb as "code that checks for a certain set of conditions to be present on the system," and if "those conditions are met, executes some special function that is not an intended function of the code in which the logic bomb is embedded, and is not desired by the operator of the code.") McAfee, *supra* note 28. (" Triggers for logic bombs can include a change in a file, by a particular series of keystrokes, or at a specific time or date." The latter are also called 'time bombs.')

[60] Slade, *supra* note 44.

Viruses, worms, and Trojan horses are usually linked (and often fall under the general term 'viruses') because of their similarities.[61] The distinction between viruses and worms is becoming less obvious,[62] and some programs can be both a virus and a worm.[63] Sometimes these three different forms of malicious software can work in conjunction. [64] For example, some viruses and worms are able to install a separate Trojan function that records the subsequent keystrokes from users on their infected personal computers, and sends their data to someone else. [65] This data may include computer passwords and financial information.[66] Such a program is called a 'backdoor.' Backdoors are applications of computer code within a virus that causes the computer to give special access to someone other than the user.[67] Even a seemingly innocuous

---

[61] McAfee, *supra* note 28. (" Examples include a message displayed on a specific date or reformatting a hard drive after the 10th execution of a program.")

[62] Thompson, *supra* note 1. "These days, the distinction between worm and virus is breaking down. A worm will carry a virus with it, dropping it onto the victim's hard drive to do its work, then e-mailing itself off to a new target."

[63] This was the case with the 'Love Bug.' "It's a virus because it breeds on a host computer's hard drive and a worm because it also reproduces over a network." Lev Grossman, *Attack of the Love Bug*, TIME EUROPE, May 15, 2000, *available at* www.time.com/time/europe/magazine/2000/0515/cover.html.

[64] See Erika Morphy, *Virus Writers Co-opt CNN Headlines*, ENTERPRISE SECURITY TODAY, January 21, 2005, *available at* www.newsfactor.com/story.xhtml?story_id=29909.

[65] *Id.*

[66] *Id.*

[67] Spafford, *supra* note 11.

> Back doors, often called trapdoors, consist of code written into applications to grant special access by circumventing the normal methods of access authentication. … The back door is code that either recognizes some special sequence of input, or is triggered by being run from a certain user ID. It then grants special access.
>
> Back doors become threats when they are used by unscrupulous programmers to gain

virus can leave a computer vulnerable to another attack by installing a backdoor,[68] which can allow data to be stolen, more viruses to be installed, or a remote user to exercise control over the computer externally.[69]

H. *Denial of Service Attacks*

Viruses can also cause 'denial of service attacks.' This occurs when a virus launches an attack (sometimes merely email messages) at a particular system or website.[70] When multiplied by the thousands of personal computers infected, a denial of service attack prevents the system from functioning properly and prevents authorized users from accessing the system.[71] The Morris worm was an inadvertent denial of service attack, causing unintended damage by flooding networks with traffic.[72]

I. *Virus Hoaxes and Their Consequences*

---

unauthorized access, or when the initial application developer forgets to remove the back door after the system has been debugged, and some other individual discovers its existence.

[68] See also J. D. Biersdorfer, *Arming a Computer Against Trojan Horses*, N.Y. TIMES, October 5, 2000, at G4 ("Once an electronic Trojan horse is in place on your computer, it can do things like giving hackers access to your machine or dumping viruses all over your hard drive.").

[69] Erika Morphy, *Bagle Virus Sweeps Networks*, ENTERPRISE SECURITY TODAY, January 20, 2004, *available at* www.newsfactor.com/ story.xhtml?story_id=23028.

[70] McAfee, *supra* note 28. See also Spafford, *supra* note 11 (defining 'denial of service attacks' as "systems that are designed to flood sites with more network traffic than they can handle," and noting that "the resulting network traffic can flood (or crash) multiple systems for hours or days at a time").

[71] McAfee, *supra* note 28.

[72] *Id.*

There also exist 'virus hoaxes,' which are not actually viruses but are email messages warning people about an upcoming virus.[73] Some hoaxes cause as much trouble as viruses by causing massive amounts of unnecessary e-mail. [74] Virus hoaxes can sometimes be as damaging as an actual computer virus. After damaging outbreaks of the Blaster and SoBig viruses at the Baylor College of Medicine, a virus hoax ('jdbgmgr.exe') circulated, causing further productivity loss just as the college was recovering from the original outbreaks.[75] Sometimes the fear and hysteria over an expected virus outweigh the actual virus.[76]

---

[73] *Id.*

[74] *Id.* According to McAfee,

> Most hoaxes contain one or more of the following characteristics:
>
> Warnings about alleged new viruses and its damaging consequences,
>
> Demands the reader forward the warning to as many people as possible,
>
> Pseudo-technical "information" describing the virus,
>
> Bogus comments from officials: FBI, software companies, news agencies, etc.

[75] Deborah Ausman, *Computer Viruses Afflict Hospitals, Which Learn to Cope*, September 18, 2003, Health-IT World, *available at* www.imakenews.com/eletra/mod_print_view.cfm?this_id=183662&u=health-itworld&issue_id=000038747 (quoting one Baylor employee: "I'd estimate we lose the same amount of time, productivity-wise, to a virus hoax as we do to a virus").

[76] *See* White, *supra* note 29.

> Similarly, we have become used to periodic virus "scares," in which stories of a newer virus make their way into the popular media, accompanied by warnings of certain and sudden doom. These warnings occur whether or not the virus has ever been seen, or will ever be seen, in the wild. You may remember Michelangelo Madness in 1992, one of the first such scares. In such a scare, millions of people want to make sure that their anti-virus software can protect them from this allegedly deadly threat. This gives rise to "download storms," in which millions of requests for updated virus definitions must be handled in a very short time.

J. *Targeted Viruses*

Computer viruses are usually random, but can also be targeted at specific entities.[77] For example, the Blaster worm spread through computer networks belonging to large corporations, while the SoBig.F virus focused primarily on personal computers used in homes and small businesses.[78] Recent viruses have targeted banks and financial institutions.[79] These are different than the more typical viruses which cause random chaos.[80] Some viruses are programmed to attack the websites of anti-virus companies such as McAfee and Symantec (the maker of Norton software).[81] On occasion, a virus-creator will target a specific company, as when a disgruntled ex-employee takes revenge on the company that fired him.[82]

---

[77] Sarah Kershaw and Laurie J. Flynn, *Arrest Made In Attacks On Computers*, N.Y. TIMES, August 30, 2003, at C1,

[78] *Id.*

[79] See e.g. Thompson, *supra* note 1. According to Thompson:

> A variant of the Mimail worm, which appeared last spring, would install a fake pop-up screen on a computer pretending to be from PayPal, an online e-commerce firm. It would claim that PayPal had lost the victim's credit-card or banking details and ask him to type it in again. When he did, the worm would forward the information to the worm's still-unknown author. Another worm, called Bugbear.B, was programmed to employ sophisticated password-guessing strategies at banks and brokerages to steal personal information. "It was specifically designed to target financial institutions," said Vincent Weafer, senior director of Symantec.

[80] *Id.*

[81] *See* Lemke, *supra* note 46. The seventh version of MyDoom was "programmed to flood Symantec's Web site with information in an attempt to shut it down."

[82] See Steve Strunsky, *Prison Sentence In Computer Case*, N.Y. TIMES, February 27, 2002, at B8. The virus-creator was a 39 year-old man. Three weeks after being dismissed from Omega Engineering, he created a virus which targeted the company and wiped out millions of dollars worth of software. According to an assistant U.S. attorney,

K. *Is Microsoft to Blame?*

Many viruses are written in a Microsoft computer language, Visual Basic, that is used for all programs on Microsoft Windows.[83] Once one Microsoft program is infected, it is easy for the others to be as well.[84] Microsoft appears especially vulnerable when compared to Apple's Macintosh computers which are rarely threatened by viruses.[85] Virus-writers have even successfully prepared viruses for Microsoft software prior to the software being released into the market.[86] Problems resulting from viruses have also caused Microsoft to be criticized for failing to do more to prevent it.[87] Some are even advocating legislation to penalize Microsoft and other

---

Omega spent $2 million to recreate the computerized manufacturing programs and lost an estimated $10 million in anticipated sales.

[83] See Chris Taylor, *Bug Analysis: Why PCs are easy targets*, TIME EUROPE, May 15, 2000, *available at* www.time.com/time/europe/magazine/2000/0515/pcs.html (naming several of the worst 1999 viruses and pointing out which specific Microsoft program they were written for).

[84] *Id.* (noting that Microsoft software "so genetically interconnected that it qualifies as a monoculture," meaning that it is a "homogeneous ecosystem").

> Using Word, Excel and Outlook exclusively on Windows machines in a company network 'is like planting Kansas with the same grain of wheat,' says Bill Cheswick, a senior researcher at Lucent. When a virus preys on the crop, nothing is left standing. The companies hit hardest by the Love Bug were closed Microsoft shops. Users who had planted their PCs with a slightly more colorful selection of seeds — even just substituting Eudora for Outlook — suffered not at all.

[85] See Spafford, *supra* note 11 (noting that while the number of known viruses affecting Intel/Microsoft platforms has grown to around 90,000 since 1986, less than only 60 viruses have been found utilizing the Macintosh platform).

[86] Thompson, *supra* note 1 (citing Windows 2000 as an example; the virus was designed to humiliate Microsoft).

[87] Paul Kaliciak, *available at* http://www.exn.ca/nerds/Virus.cfm. ("…Microsoft is going to face some heat for not putting more safety checks and restrictions in its Outlook mail clients. Some critics have even gone as far as to point to this incident as an example of the dangers of Microsoft's monopoly power. Because of its tight integration

companies for damage caused due to weakness in the software which are taken advantage of by virus-creators.[88]

Virus-writers in particular view Microsoft as the culprit because of the flaws in their software that are so easily taken advantage of. Onel de Guzman, the alleged creator of the "Love Bug," said he had no moral qualms about the damage caused by viruses, and blamed software makers like Microsoft for creating and licensing products vulnerable to sabotage.[89] Ironically, these virus-writers agree with computer experts that part of the problem is Microsoft's virtual monopoly on computer products, a 'digital monoculture' that allows viruses to spread more easily.[90]

L. *Duping People to Click.*

Because a virus (unlike a worm) cannot start itself without the computer user activating it, virus writers engage in tricks to fool the user into triggering the virus.[91] In order to spread their product, virus creators have to use attractive ways to trick users into opening infected files. Some

---

between Windows, Exchange, Internet Explorer and Outlook, tools created for one program can easily interact with the others, creating unpredictable — and sometimes chaotic — results.")

[88] Amy Harmon, *As Digital Vandals Disrupt the Internet, A Call for Oversight*, N.Y. TIMES, September 1, 2003, at A6. ("'There's a reason this kind of thing doesn't happen with automobiles,' says Bruce Schneier, chief technical officer at Counterpane Internet Security in Cupertino, Calif. 'When Firestone produces a tire with a systemic flaw, they're liable. When Microsoft produces an operating system with two systemic flaws per week, they're not liable.'")

[89] See Landler, *supra* note 22.

[90] Thompson, *supra* note 1.

[91] *Id.* "A virus cannot kick-start itself; a human needs to be fooled into clicking on it. This turns virus writers into armchair psychologists, always hunting for new tricks to dupe someone into activating a virus. ("All virus-spreading," one virus writer said caustically, "is based on the idiotic behavior of the users.")"

virus-creators use the term "social engineering" to describe manipulating people into opening the malicious computer file. [92] Some viruses are able to forge email addresses, thus giving receivers of a virus a false identity for the source.[93] One virus took the form of an electronic greeting card, although the creator called it an 'art project' and not a true virus.[94] Fake holiday greetings carrying viruses have become more frequent.[95] Emails with viruses may claim to carry a celebrity picture, such as the tennis player Anna Kournikova,[96] or a news update, such as a

---

[92] Grossman, *supra* note 63.

[93] Microsoft, *supra* note 11. ("Beware of messages warning you that you sent e-mail that contained a virus. This may mean that the virus has listed your e-mail address as the sender of tainted e-mail. This does not necessarily mean you have a virus. Some viruses have the ability to forge e-mail addresses.")

[94] Matthew Mirapaul, *A Greeting Steals Its Way Into Your Hard Drive*, N.Y. TIMES, April 11, 2002, at G3. ("When the card is opened, the virus spreads by randomly picking three images from the recipient's hard drive and sending them in a flickering message to everyone in the victim's Outlook address book.")

[95] See also Elizabeth Millard, *Holiday Viruses Make Merry on the Web*, ENTERPRISE SECURITY TODAY, December 15, 2004, *available at* http://www.newsfactor.com/story.xhtml?story_id=29070. Virus posing as holiday cards such as Christmas greetings are specifically timed to lure users into opening infected files. For example:

> The Zafi.D contains a simple Christmas wish, with a subject line of "Merry Christmas! Happy Hollydays!" It spoofs the sender address, so a recipient might believe it is from a friend, family member or colleague. When run, the virus displays a decoy error message of "Error in packed file!" although it is actually spreading into a user's system and creating a backdoor that can be used to control the computer remotely. Even more unusual, the virus spreads in e-mails that are written in several different languages, based on the recipient. This multilingual approach is highly unusual, said F-Secure researcher Mikko Hypponen, and could cause the virus to spread more than it would have normally.

[96] Thorsberg, *supra* note 12 (entry on 'AK Worm').

headline newsletter claiming to be from CNN.[97] Virus-creators have even taken advantage of humanitarian impulses by sending emails claiming to be appeals for charitable contributions (such as for the victims of the 2004 tsunami), but with a worm attached.[98] Sometimes viruses are loaded onto banner advertising.[99] Viruses have also been spread through emails purporting to be from the FBI or other government agencies.[100]

M. *Anti-Virus Measures*

Anti-virus software companies have responded to computer virus outbreaks by creating 'firewalls' and 'vaccinations.'[101] A 'firewall' prevents computers on a network from communicating directly with external computer systems, and acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software rejects any information that does not conform to pre-configured rules.[102] A

---

[97] *See* Morphy, *supra* note 64. ("The virus takes its subject lines, message content and attachment names from headlines gathered from the CNN Web site. It then e-mails itself to addresses found on infected computers.")

[98] Tsunami disaster donation plea is really a virus, Sophos reports (no author given), *available at* www.sophos.com/virusinfo/articles/vbsuna.html. A worm was discovered that pretended to request donations for the victims of the recent tsunami disaster. The worm was attached to an email, and when the attachment was clicked on it would launch a denial-of-service attack against a German website and would forward the virus to other users.

[99] Ed Raymond, *Hacker Exploit Spreads Virus Through Banner Ads*, ENTERPRISE SECURITY TODAY, November 22, 2004, *available at* www.newsfactor.com/story.xhtml?story_id=28597.

[100] See http://www.snopes.com/computer/virus/fbi.asp (discussing the Sober K. virus) ("These scam e-mails tell the recipients that their Internet use has been monitored by the FBI's Internet Fraud Complaint Center and that they have accessed illegal web sites. The e-mails then direct recipients to open an attachment and answer questions. The attachments contain a computer virus.").

[101] McAfee, *supra* note 28.

[102] *Id.*

'vaccination' stores information about files within the computer in order to notify the user about file changes. [103] Anti-virus measures are designed to restore damaged or infected files without destroying the data if possible.[104] In response, some viruses are created to be 'self-encrypting' so that their text strings are different with each infection and no signature remains.[105] Some viruses ('mutating viruses') change their form as they work their way through computer files, and others ('polymorphic viruses') create varied copies of themselves. Both of these types of viruses are thus difficult to detect and disinfect.[106]

---

[103] *Id.*

[104] Kephart, *supra* note 31. Kephart et al elaborate on the necessity of attempting to restore the original host file:

> Once a virus has been detected, it must be removed. One brutal but effective technique is simply to erase the infected program, much as certain types of immune cells destroy an infected cell. Body cells are generally easy to replace, but computer programs and documents are not so expendable. As a result, antivirus programs do their best to repair infected files rather than destroy them. (They are aided in this endeavor by the fact that computer viruses must preserve their host program essentially intact to remain undetected and multiply.) If a virus-specific scanning program detects an infected file, it can usually follow a detailed prescription, supplied by its programmers, for deleting viral code and reassembling a working copy of the original.

[105] McAfee, *supra* note 28.

[106] *Id.*. Polymorphic viruses are particularly problematic:

> Some polymorphic virus use different encryption schemes and requires different decryption routines. Thus, the same virus may look completely different on different systems or even within different files. Other polymorphic viruses vary instruction sequences and use false commands in the attempt to thwart anti-virus software. One of the most advanced polymorphic viruses uses a mutation-engine and random-number generators to change the virus code and its decryption routine.

III. THE SCOPE OF THE COMPUTER VIRUS PROBLEM

A. *The Number of Computer Viruses*

It is estimated that at any one time there are approximately 500-1000 viruses which are in the wild and which pose a threat.[107] Each one alone can cause tremendous damage. One virus, Sobig.F[108], "propagated so rapidly that at one point, one out of every 17 e-mail messages traveling through the Internet was a copy of Sobig.F."[109] Virus-creating activity occurs in cycles in which younger virus writers 'age out' and are replaced by new virus-writers.[110] Although the number of computer viruses was declining in the first three years of the new millennium, 2004

---

[107] *See* Spafford, *supra* note 11. For a year-by-year timeline describing specific computer viruses and their outbreaks, see *The History of Computer Viruses - A Timeline*, Discovery Channel, *available at* www.exn.ca/nerds/20000504-55.cfm.

[108] For a description of how viruses and worms are named, *see* Jay Lyman, *Name That Worm - How Computer Viruses Get Their Names*, NewsFactor Network, January 8, 2002, *available at* http://www.newsfactor.com/perl/story/15662.html. Virus names usually come from the first researcher who finds and names them. The names given by the virus-creators are almost always rejected. Sometimes the names given by researches derive from the content of the virus, and other times the name is whimsical, such as "Code Red" being named after the researcher's favorite beverage. Id. See also Mike Musgrove, *Who Names Computer Viruses? Everybody*, WASHINGTON POST.COM, Feb. 26, 2004, *available at* www.msnbc.msn.com/id/4376005 (describing complications when different people name the same virus different names). One virus creator, a college student in Indonesia, was annoyed that his virus was named 'Ohio' by the McAfee company, which was in reference to Ohio State University being the place of first identification of the virus. Slade, *supra* note 44.

[109] Thompson, *supra* note 1.

[110] Sarah Gordon, *Virus Writers: The End of The Innocence?*, *available at* www.research.ibm.com/antivirus/SciPapers/VB2000SG.htm

showed an increase in number.[111] According the anti-virus company McAfee, approximately 50 new viruses were discovered every day during the first half of 2004.[112] The risk threshold of the viruses also was higher in 2004.[113] Because of the prevalence of viruses today, there would still be a problem even if no more viruses were written from now on.[114]

B. *The Potential for Future Harm*

Researchers who study computer viruses believe that the problem will become worse as the Internet becomes a more dominant part of life.[115] Viruses are likely to have even greater consequences as wireless networks become more prevalent.[116] The frustration resulting from the

---

[111] See Robin Arnfield, *McAfee Warns on Top Viruses*, ENTERPRISE SECURITY TODAY, January 4, 2005, *available at* www.newsfactor.com/story.xhtml?story_id=29450.

[112] *Id.*

[113] *Id.* ("Virus attacks reaching a "medium" or higher risk assessment dramatically increased in 2004 compared to 2003, Avert [an anti-virus company] said. Avert has assessed 46 threats as a "medium" or higher risk compared to 2003's total of 20 threats reaching that same risk level.")

[114] See Spafford, *supra* note 11. "If no more computer viruses were written from now on, there would still be a computer virus problem for many years to come. Of the thousands of reported computer viruses, several hundred are well- established on various types of computers around the world. The population of machines and archived media is such that these viruses would continue to propagate from a rather large population of contaminated machines."

[115] *See* White, *supra* note 29.

> As the Internet becomes the common vehicle for communication in the world, and as more and more people use it, digital communication will increase vastly in scope and speed. As this happens, new kinds of viruses will take advantage of this increase to spread much more broadly, and much more quickly, than present-day viruses. These viruses will spread to thousands of systems in a matter of minutes, and around the world in a matter of hours.

[116] See Grossman, *supra* note 63. (quoting Symantec vice president Steve Cullen: "We're only fractionally connected right now. The possibility for virus attacks will become exponentially greater in the wireless future.")

prevalence of computer viruses, and the recognition that the problem will grow worse, have given rise to new demands for governmental regulation of the Internet, despite the benefits derived from its free and unregulated use.[117] The newest virus-threat, the one that most concerns Internet security experts, are worms created specifically for criminal purposes.[118]

C. *The Damage from Computer Viruses on an Individual Level*

Computer viruses are a difficult crime to quantify because there are diverging perspectives on both the scope of the problem and the criteria for ascertaining how 'bad' the problem really is.[119] On the level of an individual's personal computer, the consequences of

---

[117] *See* Harmon, *supra* note 88.

[118] *See e.g*. Thompson, *supra* note 1. 'Sobig' is the epitome of this recent phenomenon. According to Thompson, "['Sobig'] was released six separate times throughout 2003, and each time the worm was programmed to shut itself off permanently after a few days or weeks. Every time the worm appeared anew, it had been altered in a way that suggested a single author had been tinkering with it, observing its behavior in the wild, then killing off his creation to prepare a new and more insidious version." Eventually 'Sobig.F' appeared in August, by which time the worm was programmed to install a back door that would allow the author to assume control of the victim's computer. "Experts say its author has used the captured machines to send spam and might also be stealing financial information from the victims' computers."

[119] Gordon, *supra* note 110 (differentiating between the perspectives of the anti-virus researcher, the legislator, and the individual computer user). Gordon details the difference in perspective:

> For example, from the perspective of the anti-virus researcher working in a non-automated environment, the scope of the problem is probably based upon the sheer number of viruses, as he must deal daily with all incoming virus, analyzing, meticulously naming and prioritizing them, creating cures, etc. For the researcher in an automated environment, the measurement is likely to be those viruses which cannot be handled automatically and which she must deal with manually. For the end user, the infection rate per 1000 PCs in environments which are representative of his or her own is a vital statistic. However, from the perspective of the legislator, the scope of the

running a virus range from the annoying to the destructive.[120] A virus may cause the computer screen to show a funny slogan, may merely slow down the computer's functioning, or it may attack and destroy the files stored on the computer's hard drive.[121] Computer viruses have been programmed to grab random documents from a computer and send them out to e-mail addresses captured from the address book.[122] A virus can alter Microsoft Office files and then show a fake error message to the user,[123] or it can simply overwrite the entire hard drive and prevent the computer's systems from booting. [124] The result for an individual computer user can be devastating.[125]

> problem is probably related to the sheer number of problematic viruses - viruses which are highly publicized and brought to his attention - as this is a direct measure of the number of "illegal" or "undesirable" acts occurring (not allowing for natural corruption of existing viruses, etc).

Id. (internal citations omitted)

[120] See e.g. Gil L. Solomon, MD, *There's a virus going around . . .*, MEDICAL ECONOMICS [no date given], *available at* www.memag.com/memag/article/articleDetail.jsp?id=121146. ("A physician I work with lost everything on her home computer to the Chernobyl virus, and another doctor's daughter lost two college term papers for which she didn't have a backup or hard copy."); Steve Dimeck, *The Computer Virus That Could Take Advantage of You*, Ezine Articles, [no date given], (detailing the experience of the author battling a trojan on his computer and losing over 90% of his files).

[121] Microsoft, *supra* note 11.

[122] Thorsberg, *supra* note 12 (entry on 'Sircam').

[123] *Id.* (entry on 'Exporer.zip Worm').

[124] *Id.* (entry on 'Magistr').

[125] See David Narkiewicz, *Legal Tech: How to Avoid Catching a VIRUS*, 24 PENNSYLVANIA LAWYER 55 (giving personal testimony of receiving virus, and advice for preventing them). See Thompson, *supra* note 1, for an excellent description of a virus's effect:

D. *An Example of a Damaging Virus: The Love Bug*

One virus, the Love Bug, spread around the world in an astonishing two hours,[126] and caused unprecedented damage.[127] In the United States, the Love Bug infected 80% of all federal agencies, including the Defense and State departments. At least four classified, internal Defense Department e-mail systems were affected.[128] The Love Bug was also able to reset a person's own home page to a website in the Philippines so that a second virus would automatically be downloaded. This virus was designed to collect all the user's passwords stored on the computer's hard drive and email them to a particular email address. This website was shut down after being

---

> [If a person received an email with a virus,] and if he clicked on it — and didn't have up-to-date antivirus software, which many people don't — then disaster would strike his computer. The virus would activate. It would quietly reach into the victim's Microsoft Windows operating system and insert new commands telling the computer to erase its own hard drive. The next time the victim started up his computer, the machine would find those new commands, assume they were part of the normal Windows operating system and guilelessly follow them. Poof: everything on his hard drive would vanish — e-mail, pictures, documents, games.

[126] Grossman, *supra* note 63.

[127] *Id.*

> [I]n the offices of the German newspaper Abendblatt in Hamburg, system administrators watched in horror as the virus gobbled up 2,000 digital photographs in their picture archive. In Belgium atms were disabled, leaving citizens cashless. In Paris cosmetics maker L'Oréal shut down its e-mail servers, as did businesses throughout the Continent. As much as 70% of the computers in Germany, the Netherlands and Sweden were laid low. The companies affected made up a Who's Who of industry and finance, including Ford, Siemens, Silicon Graphics and Fidelity Investments. Even Microsoft, whose software was the Love Bug's special target, got so badly battered that it finally severed outside e-mail links at its Redmond, Wash., headquarters.

[128] *Id.*

discovered by officials once the first virus struck. [129] The LoveBug demonstrated the incredible world-wide damage that can result from one malicious virus-creator.[130]

E. *General Large-Scale Harm from Viruses*

Viruses can force business and governmental entities to revert to paper. The Sasser worm caused the branches of one major Australian bank to abandon their PC's and use pen and paper to complete their transactions. [131] In Taiwan, the nation's post office had to move entirely to paper in about a third of its branches after approximately 1,600 computers were infected by Sasser.[132] Viruses also have impact outside the Internet. One virus ('Slammer') shut down cell-

---

[129] *Id.*

[130] See also Thomas L. Friedman, *Space Rangers*, N.Y. TIMES, June 11, 2001, at C7 ("The Cuban missile crisis was to the cold-war system what the "Love Bug" virus is to today's globalization system — it was the event that illustrated our most dangerous vulnerability.") See also Shannon Sprinkel, *Note: Global Internet Regulation: The Residual Effects of the "I Love You" Computer Virus and the Draft Convention on Cyber-Crime*, 25 SUFFOLK TRANSNAT'L L. REV. 491. *Id.* at 493. Sprinkel described the LoveBug:

> "The virus cloaked itself with an e-mail message entitled "ILOVEYOU" and spread rapidly worldwide once opened, causing billions of dollars in damage and halting corporate networks worldwide. The virus operated in a series of stages within each victim's computer. First, the virus searched the hard drive of the personal computer (PC) for MP3 music files and pictures carrying the ".jpg" suffix. Once found, the virus destroyed each file and replaced it with a copy of itself. Second, the virus redirected Microsoft Internet Explorer surfers to a predetermined website where a separate program scanned the victim's PC for passwords and log-in names. Finally, the virus sent a copy of itself to every name in the user's address book if the computer ran Microsoft's Outlook program, overloading computer systems worldwide."

[131] Gregg Keizer, *Sasser Worm Impacted Businesses Around the World*, TechWeb.com, May 07, 2004, *available at* http://www.techweb.com/wire/26804909.

[132] *Id.*

phone use for 27 million people in South Korea.[133] Viruses have also been responsible for airline cancellations and delays.[134]

F. *The Damage to Companies and Businesses*

The introduction of computer viruses into company networks has become a prevailing problem.[135] Sometimes small businesses with limited resources suffer more damage than large corporations which can afford to pay for the necessary preventions.[136] The damage to a companies internal computers may often come from the feature of a virus emailing itself to every email address on each computer. Since computers within a company are likely to contain numerous email addresses of other company workers, this can translate into tens of thousands of emails which then cripple the Internet server. [137] The amount of damage has varied according to the behavior of the virus.[138] Furthermore, damage to businesses from computer viruses is rarely insured.[139]

---

[133] James Maguire, *The Folly of Publishing the Slammer Code*, NewsFactor Network, June 23, 2003, *available at* www.newsfactor.com/story.xhtml?story_id=21780.

[134] See e.g. Keizer, *supra* note 131 (noting problems at Delta Airlines concurrent with world-wide difficulties resulting from the Sasser worm); Maguire, *supra* note 133, *The Folly of Publishing the Slammer Code*, NewsFactor Network, June 23, 2003, *available at* www.newsfactor.com/story.xhtml?story_id=21780 (another virus caused Continental Airlines to cancel all its flights from its Newark hub).

[135] See e.g. Michael Schrage, *Should Virus Carriers Wear a Scarlet V?*, ComputerWorld, Jan 27, 1997, at B37, *available at* www.computerworld.com/news/1997/story/0,11280,12501,00.html (advocating that the names of employees who negligently allow viruses to infect a company's computers be published as a shaming technique).

[136] Morphy, *supra* note 69 (giving 'Bagle' as an example of a virus that "appear[ed] to be aimed at people who are not savvy about viruses and smaller businesses that are not up-to-date on the latest spam and virus developments").

[137] Paul Kaliciak, at www.exn.ca/nerds/Virus.cfm.

[138] See Spafford, *supra* note 11. Spafford gives several examples of viruses and their official damage estimates:

G. *The Dangerous Harm to Hospitals*

Perhaps the place where viruses can cause the most danger is a hospital. In October, 2003, the outbreak of two viruses (Blaster and SoBig) affected several thousand computers used by hospitals and emergency services in Glasgow, Scotland.[140] There is at least one instance, in

---

- The Brain virus, introduced in 1986, required 5 years to reach its maximum level of spread. This was to approximately 50,000 machines, and resulted in perhaps $5 million in damages according to some estimates.

- The Melissa macro worm, released 13 years later, spread to approximately 150,000 systems over a period of four days. Damage was estimated to be in the vicinity of $300 million.

- The ILOVEYOU macro worm [the 'LoveBug'], released in May 2000, spread to as many as 500,000 systems in a little over 24 hours. Damage was estimated to be as much as $10 billion.

- The Code Red and Nimda worms in October/November 2001 exploited flaws with published fixes but still managed to compromise 500,000 systems in 14-16 hours. Several billion dollars in damages were estimated.

- The Sapphire/Slammer worm at the beginning of this year [2003], also exploiting flaws with known patches, reached its maximum spread of 75,000 systems in 10 minutes. It was doubling every 8 seconds. It caused over a billion dollars in damages (approximately $13,000 per machine; $1.7 million per second).

[139] Alison Langley, *Computer Viruses Are Frustrating Insurers, Too*, N.Y. TIMES, October 12, 2003, at 4. ("Those who try to get insurance find that there are no policies being written against viruses, although they can buy limited coverage against hackers whose attacks are more local. The lack of insurance exists because insurers do not know how to provide adequately for possible losses. … A nascent virus could strike globally, bringing claims on many more policies simultaneously.") An amended correction to this article, dated November 9, 2003, noted that one insurance company, AIG eBusiness Risk Solutions, does provide policies which cover damage resulting from computer viruses under certain conditions.

[140] Ausman, *supra* note 75.

Russia, of a computer virus being implicated in hospital deaths.[141] One medical center in the U.S. was so affected by an Internet worm that hospital officials declared it an internal disaster and placed the hospital in full diversion mode.[142] Computer viruses hinder hospitals' ability to care for patients by making it more difficult for doctors to communicate, and by forcing hospitals to devote resources to fighting computer viruses which could be used for diagnosing and treating illnesses.[143] The danger to hospitals also has more subtle consequences. Unlike companies or other institutions which can lockdown all their computers in the event of a computer virus attack, hospitals require an open system for optimized patient care.[144] Viruses are a particular concern for medical specialties which require the use of medical devices that often run on Windows operating systems.[145] Viruses may also effect medical care in less obvious ways, such as

---

[141] See Andrey Rumyantsev, *Death from a Computer Virus*, IZVESTIA, January 23, 1996 (translated by T.M. Weber). A virus creator posted his infected program on the city's electronic bulletin board. The virus infected two hospital pediatric wards, and their computerized diagnostic systems crashed as a result. Two children are known to have died. It is not entirely certain that the children's deaths were the direct result of the computer virus, but specialists believe that to be the case. The article indicates that the virus-creator was not prosecuted, despite being identified.

[142] Jerry Jones, *Computer virus affects VUMC system*, January 31, 2003, *available at* www.mc.vanderbilt.edu/reporter/?ID=2499 (describing the affect a worm had on Vanderbilt University Medical Center: "Clinical workstations throughout the Medical Center were unable to communicate with each other or other services, slowing the admission process, lab results, pharmacy orders and radiology results.")

[143] Ausman, *supra* note 75. See also Keizer, *supra* note 131 (briefly describing the Sasser worm caused one of Korea's largest hospitals to stop using its computer system and switch to paper, causing delays in treating patients).

[144] Ausman, *supra* note 75. ("Patients will keep being sick even if a computer virus freezes systems. Hence hospitals, unlike other institutions, need to maintain some connection to critical data, both across departments and outside the institution's walls.")

[145] *Virus concern for radiology*, Oct. 7, 2004 (no author given), *available at* www.e-health-insider.com/comment_and_analysis/index.cfm?ID=30. This article notes:

delaying an airline flight carrying an organ for a transplant .[146] One other potentially deadly consequence of viruses was seen in Bellevue, Washington, in which the 911 emergency system was slowed down to the point where operators had to track their calls manually.[147]

IV. THE CREATORS AND DISTRIBUTORS OF COMPUTER VIRUSES

A. *The Hierarchy of Computer Delinquents*

Creators of computer viruses are to be distinguished from computer hackers, in that viruses have widespread but unpredictable effects, while the targets of hackers are usually specific.[148] In the computer underground, virus creators are at the lower end of the hierarchy, while hackers are at the top because of their superior skill. [149] Virus-creators are not considered to have as much originality or ingenuity. [150] This is especially true of the 'script kiddies' who

---

> Time lags involved in fixing viruses and other computer infections have caused delays and disruption in radiology departments already under pressure to cut waiting times and meet high demand for their services. The problem is compounded by the fact that many medical scanners now run on Windows operating systems and are connected to hospital computer networks to enable images to be stored and shared. This means that, unless patches are promptly applied, a scanner running on Windows and connected to such a network can be infected by viruses and worms designed to attack Microsoft software.

[146] See also Jill D. Jacobson, M.D., letter to the editor [in reponse to Clive Thompson's *The Virus Underground*, *supra* note 1], N.Y. TIMES MAGAZINE, February 22, 2004, at 6. ("A major worm that leads to the loss of scientific grants, scientific manuscripts or patient data could result in increased human suffering and even death. Flight delays caused by these worms could cause a delay in an organ transplant.")

[147] Thompson, *supra* note 1.

[148] See John Schwartz, *Decoding Computer Intruders*, N.Y. TIMES, April 24, 2003, at G1.

[149] Kim Zetter, *What Makes Johnny (and Jane) Write Viruses?*, PC WORLD, November 15, 2000, *available at* www.pcworld.com/news/article/0,aid,34405,pg,3,00.asp.

[150] *Id.*

cobble a virus out of someone else's original work.[151] Virus-creators definitely see themselves as distinct from hackers.[152]One distinction is that hacking targets a specific computer system while virus-creators send their creation 'into the wild' where the results are unpredictable and uncontrollable.[153]

B. *The Divergent Motivations of Virus-Creators*

Motivations for creating computer viruses range from an innocuous desire for developing and refining computer skills, to seeking acceptance among their peers in the 'virus underground,' to genuinely malicious intent to cause tremendous harm.[154] Some virus-creators see themselves as artists,[155] and consider viruses to be a form of artistic expression.[156] They enjoy being original

---

[151] *Id.*

[152] See Schwartz, *supra* note 148. "A recent virus detected by Sophos, a security firm, seems to embody the tension between hackers and virus coders: the virus, which originated in India, contains text with insults directed at Pakistani hackers. The conflict "took it away from the geopolitical stage and put it into a geek-to-geek stage," said Chris Wraight, a technology consultant with Sophos."

[153] Zetter, *supra* note 149. "Hacking is really about control," [researcher Susan] Gordon says, "and virus writing is about ... uncontrolled mayhem."

[154] *Id.*

[155] See Schwartz, *supra* note 148. ("Some of those who pursue the craft say they are blending computer science and art. A Spanish programmer who goes by the online name Jtag said in an e-mail exchange that he found in viruses "some kind of 'artistic' beauty." "It's like to give 'life' to one creation and this 'life-form' takes control of things, replicating, transforming and giving his own 'touch' to another programs (infecting them)," he wrote.")

[156] Thompson, *supra* note 1. Thompson depicts one virus creator, 'Philet0ast3r', describing his rationale for engaging in the activity: "A truly innovative worm, Philet0ast3r said, "is like art." To allow his malware to travel swiftly online, the virus writer must keep its code short and efficient, like a poet elegantly packing as much creativity as possible into the tight format of a sonnet. "One condition of art," he noted, "is doing good things with less."" This perspective of being an artist has been sharply criticized. *Id.* Sarah Gordon of Symantec also says the

and pioneering,[157] and the sense of accomplishment is greater because viruses are comparable to living organisms.[158] Virus-creators may simply desire to create a virus that can survive 'in the wild' and escape detection and destruction.[159] Thus viruses in general are not always as destructive as before, because one goal of virus-creators is to keep the host alive so that the virus can spread.[160]

Other virus-creators focus on the consequences of the virus outbreak rather than the design of the virus itself. They "thrive on the thrill of shutting down a company or government e-mail system," and "enjoy the notoriety and pride of seeing their virus listed in antivirus software

---

authors are ethically naive. "If you're going to say it's an artistic statement, there are more responsible ways to be artistic than to create code that costs people millions," she says. Critics like Reitinger, the Microsoft security chief, are even harsher. "To me, it's online arson," he says. "Launching a virus is no different from burning down a building. There are people who would never toss a Molotov cocktail into a warehouse, but they wouldn't think for a second about launching a virus."

[157] Thompson, *supra* note 1. One virus-writer from the Czech Republic, a 21-year old nicknamed 'Benny,' put it this way: "The main thing that I'm most proud of, and that no one else can say, is that I always come up with a new idea. … Each worm shows something different, something new that hadn't been done before by anyone."

[158] *Id.* "Writing malware, as one author e-mailed me, is like creating artificial life. A virus, he wrote, is "a humble little creature with only the intention to avoid extinction and survive.""

[159] Zetter, *supra* note 149. "[Virus-creator] Doctor Owl's … scorns most viruses today as "worthless" because they're easily detected and destroyed. He really wants to create a long-lasting virus that will survive transparently in the wild for months, he says. Then he'll sell the technology and retire a happy man, content in knowing he created such a great program."

[160] See e.g. Thompson, *supra* note 1. "Five years ago, the biggest danger was the "Chernobyl" virus, which deleted your hard drive. But the prevalence of hard-drive-destroying viruses has steadily declined to almost zero. Malware authors have learned a lesson that biologists have long known: the best way for a virus to spread is to ensure its host remains alive."

programs."[161] Some analysts believe that virus-authors simply enjoy the notoriety.[162] An 'alert' from an anti-virus company thus becomes a badge of honor.[163]

Occasionally virus-creators believe their motives are benevolent. Some virus-writers sincerely believe they are providing a service by openly exposing weaknesses in computer systems and software. In keeping with their philosophy, they will send their viruses to anti-virus companies so that an outbreak can be prevented if a script kiddie gets hold of it and sends it out into the wild.[164] They might create viruses to combat existing ones and remove them from infected computers, without any desire to cause harm. Or they may have political motivations,[165]

---

[161] Zetter, *supra* note 149. One example, a virus-creator named 'Evul,' is instructive:

> Evul falls into this category. He says he never releases his programs, but often sends a finished virus to antivirus vendors such as AVP and McAfee so they can add a definition to their scanning software. (Most antivirus vendors accept "submissions.") He also distributes to virus "collectors." But he's reconsidering that action after his program called Angela was unleashed by a collector.

[162] Sarah Fraser, *What Makes Virus Writers Tick?*, NewsFactor Network, July 1, 2003, *available at* www.newsfactor.com/story.xhtml?story_id=21837.

> Gartner Group analyst John Pescatore told NewsFactor that "seeing your creation spread across the Internet and talked about on the 6 p.m. news is sort of like putting cherry bombs in toilet bowls in the high-school restroom and getting written about in the school paper — but on a much larger, more brag-inducing scale."

[163] Thompson, *supra* note 1. Thompson likens it to an author getting a great book review.

[164] See e.g. Thompson, *supra* note 1. Virus writers believe that their activity "strengthens the 'immune system' of the Internet."

[165] Zetter, *supra* note 149. One example is the Bulgarian virus-creator Dark Avenger. "Writing viruses lent him a sense of political power and freedom he was denied in Bulgaria. 'I think the idea of making a program that would travel on its own, and go to places its creator could never go, was most interesting for me,' he wrote."

and create viruses related to social activism.[166] Creating viruses for the sake of political activism has been likened to sending a message through graffiti, except the virus can reach millions of people.[167]

C. *The Profile of a Virus-Creator*

According to one researcher who has had numerous interviews with virus creators, the people who do this have an attitude "typical of youths in crisis." Their private mail generally embodied "frustration, anger and general dissatisfaction followed by small glimpses of conscience - often resulting in a decision to at least consider the consequences of their actions."[168] Virus-creators may believe that they are "simply lashing out at what they often perceive as the big, greedy, distant, corporatized world," without realizing the actual human consequences. [169] "They don't quite grasp that the entities on the other end are human beings whose feelings can be hurt and whose personal and work lives can be disrupted."[170]

---

[166] See Schwartz, *supra* note 148.

> There was, to be sure, the explicitly political Code Red, a self-reproducing program known as a worm that was unleashed in 2001 to take control of thousands of computers and force them to block access to the White House Web site by flooding government servers with data. Many security experts believe that the program was developed in China in retaliation for the loss of a Chinese jet and its pilot after a collision with an American spy plane. Once the worm was detected, a tweak to the numeric online address for the White House Web site prevented disruption.

[167] *Id.* (predicting that viruses and computer hacking for political goals is going to become more frequent).

[168] Gordon, *supra* note 5.

[169] Jon Katz, *Script Kiddies: Who are these guys?*, TIME EUROPE, May 15, 2000, *available at* www.time.com/time/europe/magazine/2000/0515/hackers.html.

[170] *Id.*

Many virus-writers do actually fit the caricature of intelligent young men who are alienated social misfits.[171] But they do not always fit that profile.[172] "Most virus coders are well-adjusted youths who have normal relationships with their family and friends and intend no real harm with the viruses they write," according to Susan Gordon, an expert on virus-creators who has interviewed more than a hundred of them.[173] Most virus-creators are young, but the average age has risen over the years, changing from teenagers to an average in the mid- to late-20's.[174]

---

[171] Thompson, *supra* note 1. One virus-writer, 'Vorgon,' admitted he was a "social reject." He was suicidal until he began to write computer viruses and became accepted into the community of virus-writers. When one of his worms was posted on an antivirus website, he described the feeling as, "I was god for a couple days."

[172] Zetter, *supra* note 149.

> The image of the virus writer as an angry social malcontent bent on destruction is generally wrong, Gordon says. Most—especially the teenagers—code for thrills and are often disconnected from the reality of what their creations can do, she says.
>
> "They don't believe that their code can actually hurt anyone," Gordon says. It's actually a normal level of ethical development for their age group, she adds. "Most teenagers don't really think about the effect their actions will have on other people."
>
> The community harbors a few malcontents, but virus writers come from all ages, backgrounds, countries, and skill levels, with varying motivations and intents. They are teenagers and college students and middle-aged professionals, Gordon says. Some are female.

[173] *Id.*

[174] *Id.*

> Usually, older virus writers work as engineers or system administrators in the computing industry…. It's not simply that teen virus writers are aging. In the past, most lost interest in viruses when they began a profession around age 22. Today, they may still code viruses after entering the workforce. Some don't even start until their mid- to late 20s.

Furthermore, although most virus-creators are male, there are a number of females who also participate.[175]

Virus-creators are often romanticized and regarded with begrudging respect by the public. The suspected creator of the LoveBug was even offered a job by several computer companies.[176] This romanticism can include concepts of remedying social injustice.[177] Some virus-writers prefer to create viruses that are not destructive.[178] Virus-writers seem to crave anonymity, as seen by the newspaper reports and research surveys in which they go by their 'handles' or nicknames.[179] Many virus-writers first become interested in the activity by being the victim of a computer virus themselves.[180]

D. *Groups of Virus-Creators*

---

[175] *Id.* "…[Researcher Susan] Gordon is in touch with some of the few female writers, such as a 16-year-old European girl who goes by "Gigabyte." Female virus writers like her are generally motivated by an urge to impress boyfriends or male peers, to be accepted in a predominantly male club. But Gordon knows at least one female virus writer in her early 50s. Another, in her 40s, works at a government agency, Gordon says."

[176] *Id.*

[177] *Id.*

> [Suspected LoveBug creator] de Guzman was viewed as a hero by fellow students at the AMA Computer College in the Philippines because the Trojan horse he allegedly created was designed to steal Internet passwords. Internet access in the Philippines costs about $90 monthly, a price prohibitive to students in de Guzman's lower-class neighborhood. He was viewed as a hero for robbing from rich ISPs to give to the Internet poor.

[178] Thompson, *supra* note 1. ("Mario says he prefers to create viruses that don't intentionally wreck data, because simple destruction is too easy. "Anyone can rewrite a hard drive with one or two lines of code," he says. "It makes no sense. It's really lame." Besides which, it's mean, he says, and he likes to be friendly.")

[179] *Id.*

[180] Thompson, *supra* note 1.

Although computer programming is by nature an individual activity, virus-creators have their own elite clubs, such as the "super-elite cadre within the virus underground" known as '29A.'[181] Sometimes virus-creators communicate to each other through their creations using 'greetz,' which are encoded greetings to their friends in the virus underground.[182] On occasion they may even go to battle with each other.[183] The most famous example is the Netsky/Bagle war, which directly led to a higher quantity of viruses on the Internet.[184]

E. *The Distinction between Creating the Viruses and Sending Them into the Wild*

Many of the most skilled virus-writers may spend hours creating their viruses, but have no desire to set them free into the wild.[185] Virus-creators are often dismissive of the people who

---

[181] *Id.*

[182] *Id.*.

[183] See e.g. Erika Morphy, *Despite German Teen Arrest, Sons of Sasser Live On*, ENTERPRISE SECURITY TODAY, May 10, 2004, *available at* http://www.newsfactor.com/story.xhtml?story_id=23981.

> The development of yet another Sasser offshoot is confirmation that the German teenager is not the only individual programming these worms, according to Luis Corrons, head of PandaLabs. "Rather, it is an organized group of delinquents," he said. "This seems to indicate that there is a kind of cyber war being waged among the creators of the Bagle, MyDoom, Netsky and Sasser worms, and it will continue to cause many more variants of the virus.

[184] For example, a war erupted between the creators of the Netsky and Bagle worms. Later versions of each worm tried to undo and remove the other worm. The code used in the worms contained taunts, insults and expletives against the creator of the other worm. The Netsky/Bagle war was partially responsible for an increase in the rate of virus production. See Robin Arnfield, *McAfee Warns on Top Viruses*, Enterprise Security Today, January 4, 2005, *available at* www.newsfactor.com/story.xhtml?story_id=29450. ("Vincent Gullotto, vice president of Avert, says in a statement. "Although we saw a steady 5 percent year-over-year decrease in the rate of virus production from 2000 to 2003, we have seen an increase in 2004, which can be partly attributed to the Bagle and Netsky authors feuding.")

[185] Thompson, *supra* note 1.

take their viruses and send them out.[186] Many virus-creators do not send out their creations but treat it as an experimental hobby.[187] But even virus-creators who don't agree with sending out viruses to cause damage may still provide a forum for others to do so.[188] Virus-creators justify

---

[186] See Gordon, *supra* note 5 (an interview with a virus-creator named 'Dark Avenger'). One excerpt details the Dark Avenger's reaction to those who distribute his viruses:

> SG (interviewer)- …By writing and distributing the viruses, making them available, you do provide people with the idea and the means, in the same way you were initially provided. By doing this, your actions affect innocent users.
>
> DA- The innocent users would be much less affected if they bought all the software they used (and from an authorised dealer) and if they used it ion [sic] the way they are allowed to by the license agreement. If somebody instead of working plays pirated computer games all day long, then it's quite likely that at some point they will get a virus. Besides, there's no such thing as an innocent user, but that's another subject.
>
> SG- What about the fact that you're giving people the idea, by creating such clever viruses?
>
> DA- Ideas are not responsible for people who believe in them. Or use them. Or abuse them. Also, I didn't write them to "provide" anybody with anything. The weasel is the one who "provides". I just wrote them for fun. I couldn't care less for all the suckers who see/use them. They were not supposed to make such a big mess.

[187] Zetter, *supra* note 149.

[188] *Id.*

> …Evul runs a well-known virus exchange site where writers can post source code. The site clearly states he won't allow posting of executable code; he says he can't stop anyone from stringing together a program from source code from his site—including his own code—and then sending it off. …
>
> "I can't control what someone else does with [my code]," Evul says. "The simple fact that one other person is going to do something criminal with my code doesn't mean I am not going to enjoy

this seeming contradiction by saying they are not responsible for the consequences of someone else sending out their virus. They even liken their justification for disclaiming responsibility to the NRA's famous slogan, "Guns don't kill people, people do."[189] Virus-creators can nevertheless be charged with inciting other people to spread their viruses.[190]

Virus-creators often share their code online, which allows others to create 'copycat' viruses which are similarly destructive.[191] For example, one teenager who created a variant of the Blaster worm which spread to millions of computers admitted that he found code from the original Blaster worm online and simply made minor changes.[192] Multiple versions of some of the worst computer viruses, such as MyDoom, Beagle, and Netsky, circulated long after the original was detected.[193] The antivirus company Symantec has reported finding found more than 38,000 Web sites containing source code for viruses and worms (most of which are shut down by authorities).[194] According to Symantec, the amount of malicious code publicly available rose 5 percent in 2003.[195] Besides posting their viruses on websites, virus-creators can use other methods of distributing source code for their programs that are more difficult to trace, including

---

my hobby. Had I known someone else would [spread my virus], I would have made a better choice of who received it."

[189] *Id.*

[190] *See* Gordon, *supra* note 110 (citing the example of Christopher Pile (the "Black Baron") who pled guilty to five charges of gaining unauthorized access to computers, five charges of making unauthorized modifications, and one charge of inciting others to spread his viruses.)

[191] *See* Lemke, *supra* note 46.

[192] *Id.*

[193] *Id.*

[194] *Id.*

[195] *Id.*

mailing lists, chat rooms, instant-messaging programs, and file-sharing networks (such as Kazaa).[196]

F. *Less Skill, More Harm: Script Kiddies*

The individuals who take the viruses from the Web and release them into the wild are nicknamed 'script kiddies.'[197] It is usually the script-kiddies, and not the original virus-writers, who are the most destructive and the most naïve.[198] The term 'script kiddies' refers to untrained individuals who are able to create viruses because of the availability of tools written in simple computer language. [199] Whenever new software is mass-distributed, script kiddies are already waiting to exploit their flaws.[200]

---

[196] *Id.*

[197] Thompson, *supra* note 1. Thompson described the script kiddies as unskilled in virus-writing and ignorant of the potential consequences:

> The people who release the viruses are often anonymous mischief-makers, or "script kiddies." That's a derisive term for aspiring young hackers, usually teenagers or curious college students, who don't yet have the skill to program computers but like to pretend they do. They download the viruses, claim to have written them themselves and then set them free in an attempt to assume the role of a fearsome digital menace. Script kiddies often have only a dim idea of how the code works and little concern for how a digital plague can rage out of control.

[198] Thompson, *supra* note 1. Thompson quotes David Perry, global director of education for Trend Micro, an antivirus company. "If you're writing important virus code, you're probably well trained. You know a number of tricks to write good code, but you don't want to go to prison. You have an income and stuff. It takes someone unaware of the consequences to release a virus."

[199] See Spafford, *supra* note 11. Spafford describes the reactions of script kiddies to flaws in newly developed software, and their motivations:

> When new faults ("bugs") are discovered in widely-deployed software, some individuals race to develop tools to exploit those flaws. These tools often contain sophisticated interfaces and

Some virus-writers become annoyed by the script-kiddies who take their work and send it out.[201] But without the virus-writers creating and posting their work in the first place, the script kiddies would not be able to do it on their own.[202] Thus a large number of computer viruses are

---

> documentation so as to enable unsophisticated users to employ them. These tools are then posted on newsgroups and WWW sites for open download. What results are widespread break-ins to sites where the patches for the affected flaws have not yet been applied…. As some of these tools are written in simple scripting languages, the untrained people who employ them are known as script kiddies.
>
> These kits and scripts are written by a variety of individuals. Some are well-meaning individuals who believe they are producing tools to help others determine vulnerabilities in their own systems. Some are simply antisocial individuals with ill-specified agendas, such as to cause embarrassment to particular software vendors. Often these exploits are an attempt to gain some form of notoriety in the marketplace.

[200] *Id.*

[201] Thompson, *supra* note 1. Thompson gives the example of a 16-year-old boy in Detroit, Stephen Mathieson.

> A year ago, Mathieson became annoyed when he found members of another virus-writers group called Catfish—VX plagiarizing his code. So he wrote Evion, a worm specifically designed to taunt the Catfish guys. He put it up on his Web site for everyone to see. Like most of Mathieson's work, the worm had no destructive intent. It merely popped up a few cocky messages, including: Catfish—VX are lamers. This virus was constructed for them to steal.
>
> Someone did in fact steal it, because pretty soon Mathieson heard reports of it being spotted in the wild. To this day, he does not know who circulated Evion. But he suspects it was probably a random troublemaker, a script kiddie who swiped it from his site. "The kids," he said, shaking his head, "just cut and paste."

[202] *Id*.

> By putting their code freely on the Web, virus writers essentially dangle temptation in front of every disgruntled teenager who goes online looking for a way to rebel. A cynic might say that

the result of a "symbiotic relationship between the people smart enough to write a virus and the people dumb enough — or malicious enough — to spread it."[203]

Sometimes the new deviant variants of the virus sent out by the script kiddies are just as damaging as the original.[204] For example, the Sasser worm was actually a new modified version of the Netsky virus.[205] The original Blaster worm was written by an unknown, skilled programmer, but subsequent versions of Blaster were slightly altered versions of the original written by at least two teenage 'script kiddies,' one in Romania and the other in the U.S.[206] One Minnesota teenager who was eventually arrested created 'Blaster.B' by modifying the original

---

malware authors rely on clueless script kiddies the same way that a drug dealer uses 13-year-olds to carry illegal goods — passing the liability off to a hapless mule.

"You've got several levels here," says Marc Rogers, a former police officer who now researches computer forensics at Purdue University. "You've got the guys who write it, and they know they shouldn't release it because it's illegal. So they put it out there knowing that some script kiddie who wants to feel like a big shot in the virus underground will put it out. They know these neophytes will jump on it. So they're grinning ear to ear, because their baby, their creation, is out there. But they didn't officially release it, so they don't get in trouble." He says he thinks that the original authors are just as blameworthy as the spreaders.

[203] Thompson, *supra* note 1.

[204] *See e.g.* Morphy, *supra* note 183 ("For example, 'new and potentially dangerous variants of the Sasser worm continue to rip through computer networks, presumably dispatched by copycat virus authors.'").

[205] Alastair Dalton and Allan Hall, Teenage hacker faces jail for global net virus *available at* http://news.scotsman.com/topics.cfm?tid=45&id=531332004. The Sasser worm had global consequences. According to Dalton, "British Airways flight computers were affected, the UK Coastguard had to draw maps usually printed by computer, German civil servants were reduced to writing reports in pen and ink, and hospitals in the Far East had their drug inventories and emergency admission schedules thrown into disarray."

[206] Thompson, *supra* note 1.

Blaster worm, but he was entirely unconnected with the creators of the original Blaster worm. Blaster and its derivatives have cost North American companies $1.3 billion.[207]

G. *The Dwindling Skill Level Necessary for Virus-Creation*

Originally virus-creation was limited to an elite cadre of computer researchers engaging in benign experimentation.[208] While in earlier days virus-creators needed a minimal level of expertise, now it has become exceptionally easy.[209] A virus-creator does not have to be exceptionally bright to design a pernicious virus.[210] Script-kiddies are able to take advantage of information which is easily accessed on how to write virus coding.[211]

---

[207] *See* Kershaw, *supra* note 77.

[208] See Schwartz, *supra* note 148. "Many of the early virus writers were computer researchers testing the limits of machines in the days before the Internet allowed rogue programs to spread around the world in minutes. But as the information on virus coding moved from the elite to the merely adept, there emerged a generation of "script kiddies" who could cobble together malicious programs from online tips."

[209] Zetter, *supra* note 149.

> The Internet makes it easy to share source code. In the early days of boot sector viruses, writers needed a certain level of programming skills. But the 1995 release of Microsoft WordBasic, a simple, text-based programming language, opened the market to nearly any amateur. What's more, virus writers show off their source code at Web sites and distribute virus "starter kits" of tools. Any mischievous 13-year-old or curious 45-year-old can cobble together a virus and send it into the wild. "It's like this huge candy shop has opened up on the World Wide Web," Gordon says.

[210] See Grossman, *supra* note 63. (noting that the creator of the Love Bug was likely to be someone who "took pieces from three or four viruses that came out this year and glommed them together").

[211] See Schwartz, *supra* note 148. "Many of the early virus writers were computer researchers testing the limits of machines in the days before the Internet allowed rogue programs to spread around the world in minutes. But as the information on virus coding moved from the elite to the merely adept, there emerged a generation of "script kiddies" who could cobble together malicious programs from online tips."

Often the original virus is superior in skill, while the work of the script kiddie – the 'copycat' variant – requires little originality.[212] To create a variant of an existing worm or virus is comparatively easy and requires only minimal changes.[213] Virtually anyone with minimal computer skill can download a virus, play with it, and send it on its way to cause random and unpredictable damage.[214] Thus virus-writing has become an easy skill to master.[215]

V. THE DIFFICULTIES INHERENT IN PUNISHING THE CRIME OF COMPUTER VIRUS-CREATION AND DISTRIBUTION

A. *The General Problem of Cybercrimes*

Viruses are a class of cybercrimes, and such crimes are difficult to prosecute in general. The Internet is increasingly becoming a new vehicle for criminals to damage people and

---

[212] *See* Lemke, *supra* note 46.

[213] Kershaw, *supra* note 77.

[214] Thompson, *supra* note 1 (describing the process of using a downloadable 'how-to' program which asks questions of the user and designs a virus according to preference, and which takes less than a minute to complete).

[215] *Id.*

> This development worries security experts, because it means that virus-writing is no longer exclusively a high-skill profession. By so freely sharing their work, the elite virus writers have made it easy for almost anyone to wreak havoc online. When the damage occurs, as it inevitably does, the original authors just shrug. We may have created the monster, they'll say, but we didn't set it loose. This dodge infuriates security professionals and the police, who say it is legally precise but morally corrupt. "When they publish a virus online, they know someone's going to release it," says Eugene Spafford, a computer-science professor and security expert at Purdue University. Like a collection of young Dr. Frankensteins, the virus writers are increasingly creating forces they cannot control — and for which they explicitly refuse to take responsibility.

society.[216] One reason is that a criminal's presence at the scene of a crime is no longer necessary to commit the crime.[217] Experts debate whether cybercrimes necessitate the invention of new laws, or the application of traditional ones in a new context.[218] Cybercrimes are multi-jurisdictional and thus present unique procedural problems.[219] The Internet presents a unique forum allowing anonymity, both for law-abiding users and for cybercriminals, with both positive and negative benefits. Confronting cybercrime requires the reducing of anonymity.[220] A

---

[216] Catherine Clarke. *From CrimNet to Cyber-Prep: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191 (noting that most lawyers view computer crime as a form of traditional crime occurring in a new environment, i.e. computer hacking being considered as theft or trespass). *See also* Susan Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 J. TECH. L. & POL'Y 123, 124 (2002) ("Cyberspace creates new potentials for good and evil, for creative expression and criminal exploitation.").

[217] See Michael A. Sussman, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millenium*, 9 DUKE J. COMP. & INT'L L. 451 ("As we begin a new millennium, governments must work together to stay ahead of this next generation of criminal activity. They cannot allow cyberspace to become the new Wild West - a frontier bereft of the rule of law, where criminals prey on citizens with impunity." *Id* at 486).

[218] Eric Sinrod and William Reilly. *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws.* 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 180-81 (2000) (describing various 'cyberattacks,' and discussing how the federal government has treated computer crimes both as traditional crimes occurring in a new situation, and as a brand new set of crimes).

[219] Neal Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001) ("Computer crime forces us to confront the role and limitations of criminal law, just as criminal law forces us to reconceptualize the role and limitations of technology.").

[220] Albert Aldesco, *The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime.* Anonymity is especially relevant in dealing with cybercrimes:

cybercrime can create damage to society far beyond the initial scope and intention of the criminal.[221] But the crime of computer virus-creation is often not seen as a high priority in comparison to computer crimes involving fraud and embezzlement in which the harm is quantifiably more harmful.[222]

Scholars are now continuously debating whether cybercrimes fit with modern criminal law.[223] The debate basically comes down to two possibilities: either cybercrimes are traditional

---

> The technology underpinning online anonymity, however, has come under increasing scrutiny from law enforcement investigators who face unique technical and legal challenges from criminals operating online. Principally, the same technology that allows individuals to communicate anonymously also enables criminals to hide their identities and evade detection in cyberspace. Not surprisingly, investigators have been searching for a technical solution that would enable them to trace the perpetrators of computer crimes and expose their identities.
>
> *Id.* at 82

[221] Susan Brenner, *Toward a Criminal Law for Cyberspace: A New Model for Law Enforcement.* 30 RUTGERS COMPUTER & TECH. L.J. 1, 39 (noting the potential emergence of "collective crime," meaning "automated mass victimization," and describing the confusing effect this will have if traditional perspectives on crime are maintained; for example: "Is the automated victimization of 5,000 victims by one human offender using technology the commission of one "crime" or 5,000 "crimes"?")

[222] Russell Shaw, *Why Are Virus Writers So Tough To Catch?,* ENTERPRISE SECURITY TODAY, May 12, 2004, *available at* http://www.newsfactor.com/story.xhtml?story_id=24020.

[223] Kelly Cesare, *Prosecuting Computer Virus Authors: The Need for an Adquate and International Solution* , 14 TRANSNAT'L LAW 135, 142 (2001). Cesare describes the two sides of the debate as follows: 1) "computer crimes, including the mischievous use of viruses, are simply traditional crimes committed with advanced technology, and current criminal laws suffice to punish computer crimes"; and 2) "cyber crimes are a new category of crime requiring a comprehensive, separate legal framework to address the unique nature of the emerging technologies and

crimes committed with advanced technology,[224] or they are a new category of crime requiring a new legal framework to address challenges not fitting with traditional criminal law.[225] Because of the peculiarities and frustrations in dealing with cybercrime, some are suggesting alternative means of handling these new types of offenses.[226]

B. *Determining the* Mens Rea *of Computer Virus-Creation*

---

the unique set of challenges that traditional crimes do not address." Cesare points to differing federal statutes to illustrate this debate:

> In the United States, there are many statutes from which a federal prosecutor can choose when prosecuting a computer criminal. Sometimes, a prosecutor uses a traditional statute to prosecute a computer-related offense. For example, the federal Copyright Infringement Act, 17 U.S.C. 506 can be used to prosecute a copyright violation, despite the fact that a person used a computer to facilitate the crime. Other times, a prosecutor may utilize a new computer crime statute, tailor-made for crimes that cannot be committed absent the aid of a computer. An example of such a statute is the National Information Infrastructure Protection Act. The prosecutor's choice depends on the circumstances surrounding the crime and which statute is most likely to lead to a successful prosecution.

[224] See generally Tomas A. Lipinski, *The Devloping Legal Infrastructure and the Globalization of Information – Character, Content and Confusion*, 6 RICHMOND J. L. & TECH. 19 (1999-2000).

[225] See Laura J. Nicholson et al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207, 258 (2000) (noting that "law enforcement was initially hampered by the difficulty of trying to shoehorn computer crimes into traditional criminal offenses").

[226] *See e.g.* David L. Gripman, *The Doors are Locked but the Thieves and Vandals are Still Getting In: A Proposal in Torts to Alleviate Corporate America's Cyber-crime Problem,* 16 J. MARSHALL J. COMPUTER & INFO. L. 167 (suggesting torts law as a way to penalize and deter cybercrimes, and as an alternative to both criminal law and contract law).

One difficulty of virus-creation is defining the *mens rea* element of the crime.[227] Federal laws differentiate between offenders who send out a virus with the intent to cause damage, and offenders who act in reckless disregard for damage that might be caused. The first group acts out of malice, while the second group acts out of naivete.[228] The distinction between these two intentions is problematic for prosecutors, including in other countries.[229]

---

[227] See e.g. Catherine Clarke, *From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191, 206 (1996) (discussing *mens rea* in regard to cybercrimes).

[228] *See* Gordon, *supra* note 110.

> The 1994 Computer Abuse Act tries to deal differently with those who foolheartedly launch viral attacks and those who do so intending to wreak havoc. To do this, the Act defines two levels of prosecution for those who create viruses. For those who intentionally cause damage by transmitting a virus, the punishment can amount to ten years in federal prison, plus a fine. For those who transmit a virus with only "reckless disregard" to the damage it will cause, the maximum punishment stops at a fine and a year in prison.

[229] *Id.* In Taiwan, a young man serving in the country's military confessed to writing a virus, but claimed his intention was for research purposes only and that he did not spread the virus. Because of this he was not charged with a crime. As the article (quoting a report from Taiwan) explains:

> [I]f it were determined that Chen Ying-hao had maliciously disseminated the virus, he could be sentenced to time in jail. However, many creators of computer viruses are computer jocks, most of whom write viruses to show off their computer acumen. As Chen Ying-hao likely belongs to this ilk, and since under the article in question a prosecution can only be brought if a complaint is made, it has thus far not been possible to charge Chen, for lack of sufficient evidence. Prosecutors are currently reviewing the case.

For example, in United States v. Morris,[230] the crime was defined as "intentionally access[ing] a Federal computer without authorization" involving conduct which "alters, damages, or destroys information."[231] The issue in the case was to what degree "intentionally" applies to the statute.[232] The defendant Morris intentionally accessed a Fed computer without authorization, but damage that he caused happened unintentionally. The Court decided this was a strict liability crime, and that the *mens rea* "intentionally" only applied to the initial access to the computer.[233] In denying Morris's motion for acquittal, the District Court noted, "Although the evidence may have shown that defendant's initial insertion of the worm [virus] simply exceeded his authorized access, the evidence also demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program."[234]

C. *Determining who is to Blame*

Viruses and worms are frustrating to track down at the source, because they do not leave the equivalent of fingerprints, unless the creator leaves a message in the code. Furthermore, the 'crime scene' is one that transcends time and place, because the viruses can reach practically

---

[230] United States v. Morris, 928 F.2d 504 (Second Circuit, 1991).

[231] Morris, 928 F.2d at 505.

[232] *Id.*

[233] *Id.* at 509.

[234] *See* KU, FARBER, AND COCKFIELD, CYBERSPACE LAW: CASES AND MATERIALS 585 (2002). See also United States v. Sablar, 92 F.3d 865, 868 (Ninth Cir., 1996) (ruling government needs only prove intentional access without authorization, not intentional damage to computer file); Bradley Davis, *Note: It's Virus Season Again, Has Your Computer Been Vaccinated? A Survey of Computer Crime Legislation as a Response to Malevolent Software*, 72 WASH. U.L.Q. 411 (1994) (noting that "[t]he Supreme Court's refusal to review the conviction of [Morris] sent a message of deterrence to would-be authors of malevolent software).

anywhere and they can remain for a long time undetected.[235] Dealing with computer viruses is further complicated by the fact that creating a virus without spreading it is probably not a crime.[236] Criminality is determined by the sending of the virus and the intention behind it.[237]

The distribution of blame is a problem for criminal prosecution, because often the virus-writer does not send out the virus, but rather publishes the virus's computer code on the Internet, allowing others to use it.[238] Even after the virus-creator is arrested and jailed, his virus may remain active and continue to cause more damage.[239]

D. *When Writing Malicious Computer Code is Not Illegal*

---

[235] See Bean, *supra* note 43 (quoting a federal prosecutor that the crime-scene "is really four dimensional because it's distributed over time as well.")

[236] *Id.* "The vagaries of computer-virus case law are such that free-speech issues arise in attempts to prosecute virus writers who have not yet spread their creations across the Internet. "It's not illegal to write a computer virus," said Gullotto. Unless it is spread, a virus "is just a piece of computer code." *Id.*

[237] See Spafford, *supra* note 11. "It is the use of the item, and the state of mind of the user that determine the criminality. As such, it is probably the case that the deliberate release of a computer virus should be considered criminal and not simply the writing of the virus. Laws should reflect that difference."

[238] Thompson, *supra* note 1. "These days, many elite writers do not spread their works at all. Instead, they "publish" them, posting their code on Web sites, often with detailed descriptions of how the program works. Essentially, they leave their viruses lying around for anyone to use."

[239] Erika Morphy, *2004 Virus Activity Collaborative and More Clever, Says Security Firm*, ENTERPRISE SECURITY TODAY, December 8, 2004, *available at* http://www.newsfactor.com/story.xhtml?story_id=28938. ("German teenager Sven Jaschan, who wrote both the Netsky and Sasser worms, was responsible for more than 55 percent of all virus reports in 2004. Although Jaschan was apprehended in May 2004, his worms continue to spread. Eight months later, Sophos says, Jaschan's Netsky-P worm is still the most widely reported virus.")

Writing computer viruses has been likened to vandalism[240] and graffiti.[241] In most countries simply writing viruses is not illegal, and in the US it is often protected as free speech under the First Amendment.[242] A malicious computer code only becomes illegal when it is sent out and causes damage.[243] But computer code is distinguishable from other 'language' protected by the First Amendment.[244] Some have considered using conspiracy laws to charge virus-

---

[240] See Fraser, *supra* note 162 (using the terms 'vandalism phenomenon' and 'the art of online vandalism' to refer to the evolution of computer viruses). See also Harmon, *supra* note 88. ("The Internet has become a vital part of commerce and culture, but it is still a free-for-all when it comes to facing computer meltdowns. As America's 156 million Internet users brace for the next round of digital vandalism, some experts say that it is time for the government to bolster a basic sense of stability in cyberspace that societies expect from their critical public resources.")

[241] Thompson, *supra* note 1. "For a virus author, a successful worm brings the sort of fame that a particularly daring piece of graffiti used to produce: the author's name, automatically replicating itself in cyberspace."

[242] *Id.*

[243] *Id.*

> Software is a type of language, and writing a program is akin to writing a recipe for beef stew. It is merely a bunch of instructions for the computer to follow, in the same way that a recipe is a set of instructions for a cook to follow. A virus or worm becomes illegal only when it is activated — when someone sends it to a victim and starts it spreading in the wild, and it does measurable damage to computer systems. The top malware authors are acutely aware of this distinction. Most every virus-writer Web site includes a disclaimer stating that it exists purely for educational purposes, and that if a visitor downloads a virus to spread, the responsibility is entirely the visitor's.

[244] See e.g. Thompson, *supra* note 1.

> "The code for a virus is itself the weapon. You could read it in the same way you read a book, to help educate yourself about malware. Or you could set it running, turning it instantly into an active

writers, with creating a virus being a form of abetting a crime by providing materials.[245] Viruses and other malware are now considered to be a major threat to national security.[246] An exception may exist for the recent trend of viruses becoming a tool for spammers and thus being designed for a 'nefarious commercial purpose.'[247] The SoBig virus, for example, was atypical in that it was designed to make a profit.[248]

E. *The Attempt to Federalize the Illegality of Computer Virus-Creation*

For its part, the United States government has created federal law to apply to computer viruses. In 1996, Congress passed the National Information Infrastructure Protection Act (NIIPA), 18 U.S.C. 1030. This statute modifies existing computer law, namely the Counterfeit Access Device and Computer Fraud and Abuse Law.[249] This federal criminal statute previously was limited to crimes involving computers in more than one state.[250] With the passage of NIIPA,

---

agent. Computer code blurs the line between speech and act. "It's like taking a gun and sticking bullets in it and sitting it on the counter and saying, 'Hey, free gun!"' Rogers says.

[245] *Id.*

[246] Spafford, *supra* note 11 (elaborating on how malicious computer code including viruses, worms, and Trojans, present a new danger to security).

[247] Bean, *supra* note 43. Experts believe that derivative variants of the Sobig worm were created for the sake of making computers more vulnerable to spammers. If this were the case, it is possible the spammer paid a virus-creator to design the worm, which would give him deeper pockets to target in a civil suit.

[248] See Suzanne Goldenberg, *$700,000 bounty put on heads of virus creators*, THE GUARDIAN, November 7, 2003, *available at* www.smh.com.au/articles/2003/11/06/1068013326679.html?from=storyrhs&oneclick=true.

[249] *Id.*

[250] *Id.*

the statute covers any computer with Internet access (even if located within one state).[251] One particular section of NIIPA applies to virus creators. Section 1030 (a)(5) makes it a federal offense to knowingly cause the transmission of a program, code, or command with the intent to cause damage.[252] Furthermore, sections 1030 (a)(5)(B) and (C) make it a federal offense to access intentionally a computer in excess of one's authority, and cause damage as a result regardless of intent.[253]

F. *Finding and Prosecuting Virus-Creators*

It is often difficult to locate the source of a computer virus.[254] Virus-creators have developed sophisticated techniques for escaping detection.[255] It has been alleged that some virus-creators deliberately include 'clues' to their identity within the computer code that are actually

---

[251] Kelly Cesare, *Prosecuting Computer Virus Authors: The Need for an Adquate and International Solution* , 14 TRANSNAT'L LAW 135, 147 (2001).

[252] *Id.*

[253] *Id.*

[254] Shaw, *supra* note 222.

> "It is awfully hard to track down the source of a virus, because [virus writers] usually connect to the Internet through a sequence of other peoples' machines," Dave Kotz, director of research and development at Dartmouth College's Institute for Security Technology Studies.' Once the computer virus propagation process is underway, the untold number of hops the malicious code takes makes tracing it back to the source exponentially more difficult, Kotz added. "By the time anyone notices a new worm or virus, it has already propagated anonymously and quietly, far from its first location."

[255] These techniques include "linking multiple computers to upload the initial seed, faking IP addresses (a computer's unique numerical gateway to the internet) and even encrypting the worm code itself." Bean, *supra* note 43.

designed as a smokescreen.[256] Virus-creators can also use false or stolen email addresses.[257] However, viruses still arguably have 'digital fingerprints,' a unique pattern which identifies the virus.[258] One virus creator (Jeff Parson, the creator of 'Blaster.B') was apprehended when investigators intentionally infected a computer with the specific virus and observed it connect to a Website linked to the source.[259] Virus creators can also be found if they deliberately plant clues in their creations, or boast on Internet chatrooms of their accomplishments.[260]

Federal agencies and corporations have joined forces to find and apprehend the creators of specific damaging viruses.[261] Because of the difficulty in locating the original source, the use of reward money has the potential to be an effective means of discovering virus-creators, who

---

[256] Grossman, *supra* note 63.

[257] The perpetrator of the Love Bug, for example, used a series of false and stolen email addresses and anonymous Internet-access cards. *Id.*

[258] *Id.*

[259] *See* Kershaw, *supra* note 77.

[260] *See* Bean, *supra* note 43 ("Waiting for the worm's author to slip up isn't the most aggressive approach, but sometimes it's the only one.")

[261] The FBI has teamed up with Microsoft in offering several hundred thousand dollars bounty for information on the creators of the viruses MSBlast and SoBig. These viruses targeted Microsoft's operating system and caused millions of dollars damage in the early part of 2003. Among the systems they shut down were hospitals and airlines, as well as thousands of personal computers. See also Goldenberg, *supra* note 248; Elizabeth Millard, *BlasterMaster Gets 18 Months*, ENTERPRISE SECURITY TODAY, January 28, 2005, *available at* www.newsfactor.com/entsec/story.xhtml?story_title=BlasterMaster-Sentenced-to----Months&story_id=30093&category=entsec. The investigation into the Blaster variant investigation involved the U.S. Secret Service, the FBI, the U.S. Attorney's Office, and the Microsoft corporation.

often brag about their creations.[262] After Microsoft promised a reward for one virus-creator, informants contacted the corporation and offered information about where he could be found. The informants proved their tip was genuine by providing part of the worm's computer code.[263]

G. *Punishing and Sentencing Virus-Creators*

In most cases where a computer virus creator is prosecuted, a conviction results only in a fine and a suspended sentence.[264] Robert Morris, whose worm escaped 'into the wild' and caused unintended damage was sentenced to three years of probation, four-hundred hours of community service, and more than $10,000 in fines.[265] The creator of the AK Worm (which was attached to an email claiming to hold a picture of the tennis player Anna Kournikova) was a 21-year-old Dutchman.[266] He was sentenced to one-hundred and fifty hours of community service. [267] However, the 19-year old creator of a Blaster worm variant was only sentenced to 10 months of community service and 18 months in prison, the minimum time allowed under the sentencing guidelines. [268] His sentence will first be served at a minimum security prison, and will then include three years of supervised release during which he can use computers only for business or

---

[262] *See e.g.* Morphy, *supra* note 183. ("This past November [2003], Microsoft began offering a $US250,000 bounty for the heads of worm writers. If the two individuals just arrested are convicted, theirs will be the first successful prosecutions stemming from the program. Microsoft reportedly got a tip from five Germans who approached the company with information about the Sasser virus.")

[263] See Dalton, *supra* note 205.

[264] Spafford, *supra* note 11. "The little experience we have had with these cases also suggests that the convictions did little to dissuade others from writing viruses."

[265] Bean, *supra* note 43.

[266] Thorsberg, *supra* note 12 (entry on 'AK Worm').

[267] *Id.*

[268] See Millard, *supra* note 261.

education.[269] One reason the District Judge gave for a minimum sentence was that the virus-creator's parents were partially to blame.[270]

In some instances, criminal sentences for virus-creators have become more severe. [271] The writer of the Mesissa worm, for example, received 20 months in prison.[272] Because criminal sanctions do not always lead to a heavy penalty, some have advocated civil suits as a means of confronting virus-creators. But civil suits have failed to be effective because usually virus-creators are not 'deep-pocketed' and thus lack the assets to make it worthwhile.[273] And although arrests of virus-creators have become frequent and higher profile,[274] the deterrent effect on other virus creators in general seems limited.[275] Even for adult virus-creators, research indicates that new laws and penalties are not an effective deterrent unless there is a perceived likelihood of being prosecuted.[276]

---

[269] *Id.*

[270] *Id.*

[271] Bean, *supra* note 43.

[272] *Id.*

[273] *Id.* ("'They're not going to have assets to satisfy a judgment,' said Christopher Wolf, a partner in the partner in the I-practice group of the New York-based intellectual property firm, Proskauer Rose. 'The company would probably get nothing more than the satisfaction of winning a judgment.'")

[274] Gordon, *supra* note 110.

[275] *Id.* (citing author's own survey of a 'hacker's convention' in Las Vegas, in which most of those surveyed did not believe new laws or high-profile arrests had deterrent effect on them or other virus-creators).

[276] *Id.*

VI. APPLYING VICTIM-OFFENDER MEDIATION TO THE COMPUTER VIRUS PROBLEM

A. *Definition and Philosophical Origins of Victim-Offender Mediation*

Victim-offender mediation (VOM) involves a face to face meeting conducted by a trained mediator between a person who has been victimized by a crime and the perpetrator of that crime.[277] Unlike most mediation procedures, VOM operates within the context of the criminal justice system rather than the civil court system.[278] The purpose of VOM is to facilitate the negotiation of restitution agreements between the victim and the offender.[279] The underlying rationales of VOM are to achieve "reconciliation, expression of feelings, greater understanding of the event, [and] of each other."[280]

The philosophical foundations of VOM are outside of the usual theoretical principles of criminal justice. Whereas the modern criminal justice system is based upon theories of retributivism and utilitarianism, embodied and enunciated in the works of Immanuel Kant and Jeremy Bentham, respectively,[281] VOM is associated with the "restorative justice" movement.[282]

---

[277] Jennifer Brown, *The Use of Mediation to Resolve Criminal Cases: A Procedural Critique.* 43 EMORY L.J. 1247, 1262 (Fall, 1994).

[278] *Id.*

[279] *Id.*

[280] HARRIET FAGAN AND JOHN GEHM, EDS., VICTIM-OFFENDER RECONCILIATION AND MEDIATION PROGRAM DIRECTORY.

[281] See Stephanos Bibas, *Harmonizing Substantive Criminal Law Values and Criminal Procedure: The Case of Alford and Nolo Contendere Pleas*, 88 CORNELL L. REV. 1361, 1390 (2003) (describing philosophical origins of theories of punishment). Jeremy Bentham believed that "criminals commit crimes because doing so benefits them," and to "counteract these benefits, the criminal law incapacitates and deters offenders by attaching to crimes sufficiently unpleasant and restrictive punishment." Immanuel Kant believed that punishment "ought to be done in order that every one may realize the desert of his deeds." Professor Bibas points out that Kant's use of "realize" here

VOM has been described as "the oldest and most widely used expression of restorative justice throughout the world."[283] The central premise of restorative justice is that crime is a violation of people and relationships, and justice in that context is a process in which all the parties search for reparative, reconciling, and reassuring solutions.[284] The search for justice in this context thus involves the offender, the victim, and the community.[285]

B. *Practical Purposes of Victim-Offender Mediation*

VOM has developed as one alternative response to crime, delinquency, and victimization.[286] In a typical criminal trial, the victim's interaction with the offender is limited and functional, whereas VOM promotes "face-to-face negotiations between victim and

---

has two meanings. "First, offenders realize punishments in the way that entrepreneurs realize profits: they reap what they have sown, the retribution that they have earned. Second, punishment is a powerful "symbol" of moral blameworthiness that is "medicinal for the criminal and [sets] an example for others.""

[282] MARK S. UMBREIT & ROBERT COATES, VICTIM OFFENDER MEDIATION: AN ANALYSIS OF PROGRAMS IN FOUR STATES OF THE U.S. 1 (1992) ("The development of victim offender mediation in recent years has occurred within the larger context of restorative justice theory . . . 'Restorative justice' emphasizes that crime is a violation of one person by another, rather than simply against the State.").

[283] Mark Umbreit et al., *The Impact of Victim-Offender Mediation: Two Decades of Research*, 65-DEC FED. PROBATION 29 (2001).

[284] HOWARD ZEHR, CHANGING LENSES: A NEW FOCUS FOR CRIME AND JUSTICE 181 (1981).

[285] *Id.* (1981). *See generally* DANIEL NESS, KAREN STRONG, RESTORING JUSTICE 15-31 (2d. ed) (describing the origins of the restorative justice movement).

[286] Harry Mika, *The Practice and Prospect of Victim-Offender Programs*, 46 S.M.U. L. Rev 2191 (summarizing the criminal justice system's two decades of experience with victim offender mediation, and noting the prospects for further use and development of VOM. Issues that will need to be focused on in assessing the benefits of VOM's use include case selection, program development, victims, research and impact, and restorative potential.)

offender."[287] The beginning of VOM is usually traced to a 1974 incident in Kitchener, Ontario, in which a court ordered two young men guilty of vandalism to speak to their victims and negotiate restitution.[288] The novelty and success of this model resulted in the first Victim-Offender Reconciliation Program (VORP), and the Ontario model was eventually adapted in the United States.[289] VORP programs focus on four constituencies: victims, offenders, the community, and the justice system.[290]

One obvious benefit of VOM is that the victim is actively engaged in the process and is allowed to describe the result of the crime and express his anger.[291] The victim is made to feel that his needs are being met (unlike what is often the case in a typical criminal justice procedure, whether trial or plea bargain).[292] VOM provides a forum in which "the victim's participation is essential to achieve justice."[293] Meanwhile the offender is confronted with the actual and

---

[287] *Id.* Mika provides a helpful comparison between retributive justice (by which he means traditional criminal justice) and restorative justice in the context of understandings of crime, understandings of accountability, and understandings of justice. *See Id.* at 2204.

[288] *Id.* at 2195. *See also* Mark Umbreit, *Mediation of Victim-Offender Conflict,* 1988 J. DISP. RESOL. 85, 87.

[289] Mika, *supra* note 286, at 2195.

[290] Umbreit *supra* note 283, at 87.

[291] *Id.*

[292] Mika *supra* note 286, at 2198.

[293] Ilyssa Wellikoff, *Victim-Offender Mediation and Violent Crimes: On the Way to Justice*. 5 CARDOZO J. CONFLICT RESOL. 1 (2003). According to Wellikoff:

> The benefits of victim-offender mediation are numerous. Overall, the victim-offender mediation process creates a more humanizing effect that the traditional criminal prosecution system cannot match. Victim-offender mediation provides an opportunity for victims to heal, emotionally and psychologically, through meeting and communicating with their offenders. Since victims are

personalized result of his actions. The offender is able to see the object of his harm, and understand the need for restitution.[294] In the VOM setting, offenders are "placed in an intimate encounter with their victims."[295] Because of this, "the harm caused by their crime is no longer an abstraction but very real."[296] This often achieves the goal of preventing recidivism among the offenders. Research indicates that recidivism is reduced through VOM at the same rate as

---

> traditionally left out of the criminal justice process, victim-offender mediation provides an opportunity to be a part of the outcome of justice. Through dialogue, victims are given the chance to tell the offender how the crime committed against them affected their lives and their families' lives. Since victim-offender mediation is a dialogue-based program, victims are granted the invaluable opportunity to question their offenders about why they committed the crime against them. This portion of the mediation has a cathartic benefit that liberates victims from their "haunting questions" and ruminations. Ultimately, these answers prompt victims to heal from the repercussions of the crime.

[294] Mika *supra* note 286, at 2198.

[295] Wellikoff, *supra* note 293, noting that:

> [W]hen offenders participate in victim-offender mediation, they are placed in an intimate encounter with their victims where they are expected to acknowledge their wrongdoings. In this setting, the offenders have difficulty defending and "rationalizing" their criminal actions; therefore, "the harm caused by their crime is no longer an abstraction but very real." Through the human nature aspect of the mediation, victim-offender mediation has proven to generate sincere feelings of remorse within the offender.

[296] AMERICAN BAR ASSOCIATION ENDORSEMENT OF: VICTIM-OFFENDER MEDIATION/DIALOGUE PROGRAMS, PART 1 (Aug. 1994).

traditional criminal procedural approaches, and sometimes at a better rate.[297] The benefits to both victims and offenders in turn benefit the community.[298]

C. *Criticisms of Victim-Offender Mediation*

VOM has also received substantive criticism. Many commentators do not consider mediation appropriate in the context of criminal law.[299] VOM is problematic because the state's interest in punishing crime may be different than the victim's interest in confronting the offender.[300] Thus the benefit of victim involvement may actually be considered a loss in the larger scheme of criminal justice as an articulation of societal disapproval.[301] VOM creates procedural difficulties, such as disputes over confidentiality.[302] When critiqued from a

---

[297] Mark Umbreit et. al., *The Impact of Victim-Offender Mediation: Two Decades of Research*, 65-DEC FED. PROBATION 29, 32 (2001).

[298] Marty Price, *Crime and Punishment: Can Mediation Produce Restorative Justice for Victims and Offenders?*, *Available at* http://www.vorp.com/articles/crime.html (last visited Feb. 6, 2005). Price believes that the stated utilitarian justifications for criminal punishment such as incapacitation, deterrence, and rehabilitation are disingenuous, and that retribution is the true goal of the criminal justice system. Prince then proceeds to articulate why restorative justice as embodied in VOM is superior to retribution, as seen by practical results such as reduced recidivism rates.

[299] Dave Gustafson, *Debunking the Myths: Victim Offender Reconciliation in Serious Crime*, in 2(1) VICTIM-OFFENDER MEDIATION 8-9 (1990).

[300] *Id.*

[301] *Id.*

[302] Jonathan Hyman *The Model Mediator Confidentiality Rule: A Commentary.* 12 SETON HALL LEGIS. J. 17 (1988).

"restorative justice" point of view, VOM is often considered coercive despite using the language of reconciliation.[303] For these reasons, VOM remains controversial.[304]

D. *Criticism of Victim-Offender Mediation for Failing to Fulfill the Traditional Theories of Punishment*

VOM has been criticized for not fulfilling the traditional purposes of criminal punishment. The traditional purposes of punishment are retributive (assaultive, protective, and victim-vindicative), and utilitarian (deterrence, rehabilitation, and incapacitation). VOM typically does not fulfill these traditional purposes.[305] The criminal offender may not feel punished by VOM, and sometimes may even be empowered by it (negating retributivism). And VOM has been critiqued for being ineffective in accomplishing the utilitarian goals of deterrence, rehabilitation, and incapacitation because offenders often consider VOM to be an easy way out of prison time.[306] Before proceeding to discuss this critique, it is necessary to review what those theories hold.

1. *Retributivism*

---

[303] Sally Merry, *Myth and Practice in the Mediation Process*, in MEDIATION & CRIMINAL JUSTICE 239, 244 (Martin Wright & Burt Galaway eds., 1989). ("Mediation risks creating a coercive process under the rhetoric of voluntariness, participation, and community involvement.").

[304] See Mika et al., *Listening to Victims – A Critique of Restorative Justice Policy and Practice in the United States*, 68-JUN FED. PROBATION 32 (2004) (describing various criticisms of VOM).

[305] Brown, *supra* note 6, at 1296. ("At times cooperative, at other times openly hostile, the rhetoric of VOM proponents lacks a clear theory of how VOM relates to the traditional goals of criminal justice—retribution, deterrence, rehabilitation, and incapacitation…. [I]n the name of "reconciliation," VOM proponents too readily dismiss the traditional goals of the criminal law and fail to reconcile their programs' procedures and results with those of the larger criminal justice system.")

[306] *Id.*

Retributivism is based on the concept that because people can choose whether to act in violation of the law or not, once someone commits a crime he deserves the punishment inflicted.[307] Retributivism can be based on premises described as "assaultive" (it is right to hate criminals),[308] "protective" (punishing the criminal is treating him with respect),[309] and "victim-vindicative" (sending message to victim that society is righting the wrong).[310]

2. *Utilitarianism*

Utilitarianism is based on the concept that punishment should be inflicted when it is for the greater good of society.[311] Utilitarians believe that sometimes punishment is desirable and the lesser of two evils, because punishment might prevent crime, and the pain of the punishment is

---

[307] See Jean Hampton, *Correcting Harms versus Righting Wrongs: The Goal of Retribution*, 39 U.C.L.A. L. REV. 1659 (1992) (arguing that "retribution is a fundamental and necessary component of any morally respectable system of punishment carried out by the state, but not the *only* component," and that "not all retributive responses are punitive responses."

[308] See Margaret Radin, *Cruel Punishment and Respect for Persons: Super Due Process for Death*, 53 S. CAL. L. REV. 1143, 1168 (1980).

[309] See Herbert Morris, *Persons and Punishment*, 52 MONIST. 475 (1968).

[310] See Hampton, *supra* note 34, at 1698. ("[R]etribution is actually a form of compensation to the victim. Whereas tort damages are supposed to be awarded to place the victim in the situation she would have been in had the tortfeasor not acted, retribution is supposed to be inflicted to nullify the wrongdoer's message of superiority over the victim, thus placing the victim in the position she would have been in had the wrongdoer not acted.")

[311] Louis Michael Seidman, *Soldiers, Martyrs, and Criminals: Utilitarian Theory and the Problem of Crime Control*, 94 YALE L.J. 315, 320 (1984) ("Traditionally, utilitarians have begun with the premise that the criminal justice system should minimize the sum of the costs of crime and crime prevention. Since everyone's welfare is included in the social calculus, the cost of crime prevention includes not only enforcement costs (police) and process costs (courts), but also the suffering imposed upon criminals made to undergo punishment.").

less than the amount of pain we are saving ourselves from.[312] Utilitarianism can be broken down into three separate basic theories: deterrence, incapacitation, and rehabilitation. General deterrence theory holds that you punish a person for the benefit of society, since you will deter others who are watching what happens to that person.[313] Specific deterrence theory holds that through punishment, society will intimidate that specific person from committing the crime again.[314] Specific deterrence is closely related to the theory of incapacitation, which focuses on preventing the specific offender from repeating that crime through imprisonment.[315] Rehabilitation is a more modern utilitarian theory holding that in order for punishment to prevent further crime, the offender himself must be changed.[316] The criminal justice system must look at the characteristics of the offender, figure out why he committed the crime, and then deal with the underlying problem. The purpose of punishment is therefore to make the person less likely to commit crimes in the future. This may involve helping a person with drug problems, training them to overcome illiteracy, or treating their mental illness.[317]

E. *Using Victim-Offender Mediation in a New Context and Fulfilling the Traditional Theories of Punishment*

---

[312] *Id.*

[313] HERBERT L. PACKER, THE LIMITS OF THE CRIMINAL SANCTION 39, 45 (1968).

[314] Steven Klepper & Daniel Nagan, *The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited*, 27 CRIMINOLOGY 721 (1989).

[315] Linda Beres & Thomas Griffith, *Do Three Strikes Laws Make Sense? Habitual Offender Statutes and Criminal Incapacitation*, 87 GEO. L.J. 103 (1998) ("Under an incapacitation rationale, imprisonment is justified because it prevents an inmate from committing crimes against the public during the period of confinement.").

[316] *See* Packer, *supra* note 41, at 53 (the goal of rehabilitative punishment is the reformation of an offender so that he will not have the desire to commit additional crimes once he is released).

[317] See Dan Kahan, *What do Alternative Sanctions Mean?*, 63 U. CHI. L. REV. 591 (1996).

There is one potential use of VOM which has seldom been discussed, and which would avoid these legitimate criticisms. Crimes which occur in cyberspace ("cybercrimes") provide a unique challenge which may justify the use of VOM as an alternative means of punishment. And this use of VOM might fulfill the traditional theories of punishment in a way that is not effectuated by its use in other contexts.

1. *VOM Fulfills the Traditional Theories of Punishment in this Context*

There are numerous benefits to applying VOM to virus-creators and script kiddies. VOM in such instances may fulfill traditional purposes of criminal punishment. A virus-creator who is confronted by a person he has harmed is likely to feel that he is being punished (fulfilling retribution). Potential virus-creators may be less likely to engage in such activity if they are aware that those they harm can confront them. (fulfilling general deterrence). Particular virus-creators (such as juvenile delinquents) are likely to be rehabilitated if they are exposed to the consequences of their actions (fulfilling rehabilitation). And VOM may be included as part of regular prison or probationary sentence, or it may serve as a substitute for prison or probation (fulfilling incapacitation).

2. *VOM for Cybercrimes Meets the Needs of both the Victim and the State*

The state's interest in punishing cybercrime through VOM, because it accomplishes the previously mentioned theories of punishment, is similar to the victim's interest in confronting the offender. VOM provides a new procedure for confronting a new type of crime. VOM is a recent and more flexible mechanism as a vehicle for punishment, and yet it has been used substantially enough to provide a trustworthy and understandable framework.[318] VOM localizes both the

[318] *See generally* Christina L. Anderson, *Comment: Double Jeopardy: The Modern Dilemma for Juvenile Justice*, 152 U. PA. L. REV. 1181 (Jan. 2004) (describing the benefits of VOM when used for juveniles). *See also* Stephanie

criminal and the victims, overcoming the jurisdictional problems inherent in cybercrimes. VOM overcomes the problems of anonymity over the Internet—providing the victim an opportunity to make himself/herself known, and forcing the virus-creator to be publicly known and identified.[319] VOM can force a virus-creator to face the individual victims of cybercrimes, as well as victims on a larger scale, such as businesses and governmental entities.

F. *Virus Creators are Ideal Offenders for the Purposes of VOM*

Virus creators appear to be the best category of cybercriminals that can properly be penalized with VOM, fulfilling both the traditional theories of punishment and the alternative ones usually associated with restorative justice. They are often juveniles.[320] Unlike hackers or identity thieves, they are more indiscriminate in their crime (i.e. sending out a virus on the Internet without concern for where it goes, as opposed to focusing on a particular victim (company, government entity, person).[321] Although they have a *mens rea* to cause harm, they are unlikely to realize the extent of that harm except through news reporting, and even then, especially when juveniles, are unlikely to understand the personal dimensions to the results of their crime.[322] They often intend to merely "make mischief" as opposed to cause true harm.[323] Virus creators resemble the offenders most often considered by VOM advocates and restorative

---

A. Beauregard, *Note & Comment: Court-Connected Juvenile Victim-Offender Mediation: An Appealing Alternative for Ohio's Juvenile Delinquents*, 13 OHIO ST. J. ON DISP. RESOL. 1005 (1998) (endorsing VOM as an alternative to traditional sentencing for juvenile offenders).

[319] *Id.*

[320] See e.g. Leef Smith, *Web Marauder Pleads Guilty*, WASH. POST, Sept. 8, 1999 at B2.

[321] See Thompson, *supra* note 1.

[322] See Clarke, *supra* note 48.

[323] See Thompson, *supra* note 1.

justice theorists, in that the traditional justice system may not produce the best results in addressing their crime. A virus-creator, for example, may intend to cause general harm without specifically intending to cause, for example, a business to go bankrupt or a hospital to be forced into a crisis situation.

G. *Virus Creators do Not Typically Understand the Consequences of their Actions*

The virus-creators and script kiddies who can cause so much damage are not likely to recognize the harm that can result.[324] For example, one virus creator's motive was to combat existing viruses and remove them from infected computers, but his viruses (and their derivatives) caused unintended damage. [325] Officials stated that he seemed genuinely taken aback at the damage he caused. [326] Virus-creators tend to be young, and often cease pursuing their interest by the time they might be prosecuted as adults.[327] Many virus-creators stop writing viruses when they begin to consider the potential consequences of computer viruses.[328] Those who continue creating viruses are usually very immature.[329]

---

[324] Zetter, *supra* note 149.

[325] See Dalton, *supra* note 205

[326] *Id.*

[327] See Schwartz, *supra* note 148 (quoting Susan Gordon, "They don't realize the impact – they don't realize there are real people at the other end of the computers. They don't tend to recognize the consequences of their actions.")

[328] Zetter, *supra* note 149.

> "Evul" is one who says he stopped spreading viruses once he saw himself in his victim's shoes. Now 30, he began coding six years ago after a hiatus and unleashed several programs with his e-mail address embedded in the code. He felt a bit chastened when recipients wrote to him and described the data they'd lost because of his creations. But he didn't stop until an Internet service provider terminated his Web site account for posting viruses at the site.

According to one researcher who has had numerous interviews with virus creators, the people who do this have an attitude "typical of youths in crisis." They have an "ethical immaturity" because of which they fail to recognize that sending out viruses is wrong. [330] Their private mail generally embodied "frustration, anger and general dissatisfaction followed by small glimpses of conscience - often resulting in a decision to at least consider the consequences of their actions."[331]

Virus-creators may believe that they are "simply lashing out at what they often perceive as the big, greedy, distant, corporatized world," without realizing the actual human consequences. "They don't quite grasp that the entities on the other end are human beings whose feelings can be hurt and whose personal and work lives can be disrupted." [332]

H. *VOM will Properly Punish Virus Creators*

The virus-creator or script-kiddie is likely to benefit far more from VOM than if he serves jail time. VOM will force him to see the damage he has done, and hear it described and articulated explicitly. The anonymity and distance allowed by cyberspace will be stripped away,

---

"The first thing I yelled was, 'What gives you the right to destroy my hard work!'" Evul recalls. "After a moment of reflection, it hit me like a brick wall ... what gives *me* the right? I decided I don't have the right to tamper in anyone else's hard work."

He still writes file and boot sector viruses, but says he posts only the source code, which he claims is too complicated for most would-be writers to cobble into a program. He says he intensely dislikes anyone who intentionally writes and spreads a virus that could destroy someone's work.

[329] See Schwartz, *supra* note 148 (quoting Susan Gordon, "They don't realize the impact – they don't realize there are real people at the other end of the computers. They don't tend to recognize the consequences of their actions.")

[330] Zetter, *supra* note 149.

[331] See Gordon, *supra* note 5.

[332] Katz, *supra* note 169.

and the offender will be dramatically confronted with the fact that he actually caused tangible harm to real people. The harm may be personal (i.e. important files or business records that were lost) or even sentimental (i.e. family photos that were lost). If the harm was dangerous to society, VOM allows that to be described (i.e. preventing or hindering the work of a hospital or governmental agency). It is likely that certain offenders, especially juvenile ones who look at virus creation as a relatively innocent amusement, will be shocked by the actual realization of real damage they have caused. They will be compelled to accept their responsibility in causing the damage described to them.

I. *VOM will Remove the Virus-Creator's Anonymity*

Whereas protecting Internet anonymity is a legitimate civil liberties concern,[333] in the case of a cybercriminal who has already been convicted or plead guilty there is not the same need to keep his identity hidden. "Because cyberspace enables truly anonymous communication to flourish on a scale never before experienced, its existence promotes anonymous criminal acts."[334] The virtue of VOM as applied to cyberlaw, and in particular to virus-creators, is that the anonymity is removed in its entirety, not only by being identified as the perpetrator, but by being forced into a face-to-face confrontation with the victims of his act.

J. *VOM is an Especially Appropriate Forum for the Victims of Computer Viruses*

The victims of computer viruses are a particularly apt class of people whose needs can be met in this context, fulfilling the concerns of restorative justice. VOM is based on the belief that

---

[333] See David L. Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J.L. & TECH. 3 (2000) (maintaining that anonymity is essential for the cultivation of free speech and free expression).

[334] *The Criminalization of True Anonymity in Cyberspace* , 7 MICH. TELECOMM. TECH. L. REV. 191, 215 (2000).

victim's needs are not met by the criminal justice system.[335] This is especially true in regard to computer viruses. If a virus-creator is charged, it is unlikely that the victim of that virus will even know of it (except through media reports if the virus caused substantial damage). Because computer viruses (and cybercrimes in general) implicate a peculiar set of legal issues, victims of computer viruses are seldom able to obtain civil sanctions.[336] And a victim of a virus is most likely located far from the source of the harm.[337]

It is possible that a victim of a computer virus, if given a convenient opportunity to confront the source of harm done to his computer, will take advantage of that opportunity. While the Internet allows for anonymity with its benefits as well as its drawbacks, a legally-sanctioned removal of anonymity may be welcomed when it accomplishes punishment of the offender. The victim may in some instances (perhaps out of fear of reprisals, from the actual offender or from future ones who wish to take some sort of revenge) wish to remain anonymous. Ironically, VOM allows the victim in this case to be anonymous and the offender to be named (especially if done electronically).

K. *VOM Fulfills the Needs of the State*

One of the purposes of VOM is to allow victims more input and involvement within the criminal justice system. This can become a problem in that the state's goals for prosecuting the offender are not necessarily the same as the victim's interests. But because VOM accomplishes the previously mentioned theories of punishment with regard to computer virus-creators, the state's interest in punishing such cybercrime is similar to the victim's interest in confronting the

[335] See Wellikoff, *supra* note 293.

[336] Colombell, *supra* note 15.

[337] *Id.*

offender. Thus there is not the inherent conflict between the victim and the state which often accompanies criminal prosecutions. Thus the state's goals are met, and not at the expense of the victim.

L. *VOM Accomplishes the Traditional Theories of Punishment when Used for Computer Virus-Creators*

The unique nature of virus-creation as a cybercrime lends itself to VOM, with the surprising result that in this context VOM accomplishes both the traditional theories of punishment and the alternative ones of restorative justice.

1. *VOM for Computer Virus-Creators Fulfills Retributivism*

A virus-creator who is confronted by a person he has harmed will probably feel that he is actually being punished. This fulfills retributive theory from the perspectives of "assaultive" retribution (the offender knowingly committed the crime and deserves the punishment inflicted),[338] and "protective" retributivism (by treating him with a form of respect as the initiator of the harm).[339] It also fulfills "victim-vindicative" retributivism, perhaps more than a traditional criminal procedure would, by sending a specific message to the victim that society is righting the wrong, but by allowing the victim a place in the process.[340]

2. *VOM for Computer Virus-Creators Fulfills Utilitarianism*

VOM in this context also fulfills the utilitarian theories of criminal punishment. Potential virus-creators are less likely to engage in such activity if they are aware that those they harm can confront them. In this regard the stripping away of anonymity accomplishes general deterrent

[338] Cf. Radin, *supra* note 308.

[339] Cf. Morris, *supra* note 309.

[340] Cf. Hampton, *supra* note 307.

purposes. Particular virus-creators (such as juvenile delinquents) are more likely to be rehabilitated if they are exposed to the consequences of their actions,[341] accomplishing not only rehabilitation but specific deterrence. In this context it is hopeful that VOM may serve as a substitute for more typical criminal sanctions, but if need be VOM may be included as part of a regular prison or probationary sentence. VOM also allows the fulfillment of the goals of the restorative justice movement, allowing opportunities for communication, reconciliation, and forgiveness.

M. *Electronic Dispute Resolution Allows VOM To Be Used for Virus-Creators*

If VOM is used for virus-creators, there are practical considerations that will need to be discussed. How, for example, will the victim confront the offender if (as is most likely) he lives far away? One framework may be provided through the very means of their criminal activity—the Internet. There has been much advancement in using the Internet for the sake of "Electronic Dispute Resolution" (EDR).[342] In the same way that traditional ADR (i.e. negotiation, mediation, arbitration) was a response to problems in the legal system, EDR may be an appropriate reaction to the "radically new" legal problems raised by the Internet.[343] If jurisdictional problems arise in the context of VOM for cybercrimes, EDR may provide a slightly ironic way of handling the dispute, allowing the victim of the cybercrime to confront the offender and hopefully providing the same benefits of an actual face-to-face meeting. The benefits of EDR would be the same as in a civil context (and the same generally as the benefits to legitimate communication by the

[341] *See* Anderson, *supra* note 318.

[342] *See* Beatrice Baumann, *Electronic Dispute Resolution (EDR) and the Development of Internet Activites.* 52 SYRACUSE L. REV. 1227 (2002).

[343] *Id.*

Internet). EDR would reduce time problems and eliminate distance problems.[344] "[W]herever the parties are, they can interact with one another without delay."[345] This would also be a way to include a number of people in the process. EDR would also reduce the cost of VOM for cybercrimes.[346] "Face-to-face mediation involves costs, including, for example, the costs of the mediator, lost wages and earning opportunities, travel expenses. In e-mediations, these costs are greatly reduced."[347] The use of EDR provides a means for making VOM practical and realistic when applied to the creation and distribution of computer viruses.

VII. CONCLUSION

The growing problem of computer viruses is only likely to get worse. But the characteristics of the people involved will probably stay the same: young, immature and unable to understand the harm resulting from their activity. Victim offender mediation would be an effective way of punishing creators of computer viruses and the script kiddies who send them out into the wild. If potential virus-creators and distributors know that once they are caught, their anonymity will be stripped away and they will be forced to confront those they harmed, such a realization may deter their criminal conduct. Victim offender mediation is a novel punishment for a new and unusual crime, and it should result in beneficial consequences, namely the taming of the Internet wild.

---

[344] *Id.*

[345] *Id.* at 1233.

[346] *Id.*

[347] *Id.*