Virus Writers: The End of The Innocence?

Sarah Gordon

IBM Thomas J. Watson Research Center

sgordon@watson.ibm.com

Abstract

Earlier research has empirically demonstrated the cyclic nature of virus writing activity: as virus writers "age out", new virus writers take their places. Enhanced connectivity amplifies the existing problem and various technical factors result in new types of virus writers surfacing as the cycle repeats.

However, a new variable has recently been introduced into the cycle: high profile legal intervention. The virus writing community now has experienced visits by concerned law enforcement personnel; there have been arrests and there will be sentencings. New laws are being considered, enacted, and acted upon. Thus, the virus writing scene is no longer a casual pastime of kids on local Bulletin Board Systems.

What has been the impact, perceptually and operationally, of these visits, arrests, and sentencings? In other words, as the virus problem gets more and more "real world" attention, where are we actually going in terms of shaping acceptable behavior in our virtual communities and what, if any, effect are these legal interventions having on the impact of viruses upon users' computers?

In order to produce a scientifically meaningful answer to this question, pre and post intervention data on various aspects of the virus problem have been gathered. We solicited opinions on a variety of topics related to computer viruses and legal countermeasures via e-mail and direct survey. Opinions are not only interesting; they must be considered, as we know the opinions of today shape how people behave in the future. However, we are also concerned with immediate real-world impact. To this end, impact will be examined in terms of viruses found both In the Wild[1] (ItW) and on the World Wide Web (WWW), as a function of time. The data gathered before and after various types of high profile intervention is considered; in particular we are interested in any decrease noted in the graph of virus growth both ItW and on the WWW, and in online references to legal concerns.

An analysis of the data is presented and suggestions for future research are made.

---

[1] Using The WildList (http://www.wildlist.org)

Introduction

During the last eight years, a wealth of information has been gathered concerning virus writers and the various motivations behind their work (Gordon, 1994a; Gordon, 1994b; Gordon, 1995; Gordon, 1996; Gordon, 1999). In this paper, that earlier research is expanded upon and updated to consider an increasingly important facet: intervention by legal/government bodies.

It is natural, given the way societies tend to develop, that antisocial activities tend to lead to legislation designed to contain or eradicate the activities. This paradigm of control is influencing both technological development and societal direction (Gordon, 1994b). There is now increased pressure on the legislature and law enforcement to deal with a problem which purportedly costs corporations millions of dollars per year (Cobb, 1998). The goal of this paper is to gain insight into the efficacy of high-profile legal countermeasures, and assess how well they achieve the objective of lessening the spread of computer viruses.

In order to accomplish this analysis, this paper is structured as follows: First, the research to date is summarized, in order to provide the reader with insight on the "generic" virus writer, the target of laws and intervention. Second, the legal countermeasures which are in place at the time of writing are discussed, outlining the goal of legislation, and summarizing the laws employed in past high-profile arrests of virus writers. Next, the potential drawbacks and costs associated with this approach are discussed, to provide a counterpoint to the intuitively obvious application of laws and high profile interventions as a solution to the "problems" of virus writing. The lack of useful metrics as to the effectiveness of the legal approach is covered, before discussing a research methodology that provides scientifically valid data for assessing the result of the interventions. Finally, results of this research are presented, analysing the effectiveness of laws in the prevention of virus writing and various forms of distribution.

Virus Writer Demographics

Research published by (Gordon, 1994a) examined the demographics of a large number of virus writers. This was accomplished by the use of surveys, email interviews, online chat and in-person sessions. The data gathered was used to assess the ethical development[2] of individual virus writers, with a view to understanding why they chose to write viruses, and what, if anything, was likely to deter them.

The paper focused on four primary groups of people: the adolescent virus writer, the college student, the adult virus writer, and the ex-virus writer. The findings for each group are summarized below[3].

The Adolescent

Studies of the adolescent virus writer were remarkably consistent. The data tend to show that the adolescent virus writer is ethically normal and of average/above average intelligence. Responses from members of this group showed respect for their parents and for authority (to some degree). While members of the group tended to understand the difference between what is right and wrong, (i.e. directly damaging data that belongs to other people is wrong) they typically did not accept any responsibility for problems caused when their own viruses appeared in the wild.

The College Student

Members of this group also appeared to be ethically normal on the Kohlberg scale. Despite expressing that what is illegal is "wrong", members of this group were not typically concerned about the results of their actions related to their virus writing.

---

[2] based upon the Kohlberg model (Kohlberg, 1981; Panzl & McMahon, 1989)

[3] other models produced similar results

The Adult

Of the four classes studied, the adult virus writer was the smallest, and the only one which appeared to be ethically abnormal, appearing below the level of ethical maturity which would be considered normal on the Kohlberg scale.

The ex-virus writer

Once again, this group was ethically normal. The ex-virus writers typically cited lack of time and boredom with virus writing as the primary motivator for the cessation of their "hobby". Appearing socially well adjusted, the ex-virus writer seemed to bear no ill-will toward other virus writers, and was undecided concerning the ethical legitimacy of virus writing.

These results are of particular relevance to the question of legal countermeasures. The virus writing adults in the study appeared to be below the norms in ethical development; adults who are below these norms are more likely to be motivated by fear of punishment than by respect for law. For the adult virus writer, therefore, it is not the laws that are important, but their perception of the likelihood of being prosecuted under those laws. For the minors involved, the presence of laws is unlikely to be very effective for several different reasons that will be discussed in more detail later. For the youngest virus writers, it tended to show that virus writing was a naturally self-limiting phenomenon, and that the "perpetrator" would tend to cease their activity without the need for legal intervention.

The research shown above was completed in 1994. The update of the paper two years later (Gordon, 1996) showed some disturbing trends related to virus writers at the higher age limits considered. Whereas virus writers were typically aging out as their ethical development continued, mixed messages from many different sources appeared to make virus writing appear "less wrong", pushing up the age of aging out, if the process occurred at all.

Legal and High Profile Intervention

According to (ICSA, 1999) the median cost of virus disasters is $1,750, with some respondents reporting costs of up to $100,000 in a single virus incident. Another study (Ernst, 1998 cited in Cobb, 1998) suggests that virtually every organization in the world has experienced at least one virus infection, and that viruses continue to cause businesses hundreds of millions of dollars each year in damages and lost productivity. Given the purported high cost[4] to businesses it is not surprising that some people have looked to the law for help in dealing with the problem.

Legal intervention in the case of the Melissa virus has been highly publicized. Regarding this case, (Jenislawski, 1999) citing ICSA, states

> *"This case, the company says, proves that virus writing is 'indeed illegal', despite arguments to the contrary.* [This prosecution] *will be a decisive event that will tend to reduce the relentlessly increasing threat and resultant risk of computer viruses to society as a whole. By locking up perpetrators, the cycle of mounting numbers, rate, and virulence of computer viruses will get at least a pause and perhaps, a reversal. '"*

(Tippett, 2000), suggests that Congress look at making it illegal to write a computer virus. "*Making a bomb is illegal but writing about how to make a bomb is not*", he noted. *"But with a computer virus, the words are the bomb"*. (Kabay, 2000a) calls for a view of computer programs as "not speech". [5]

---

[4] social effects related to lack of trust are outside the scope of this paper

[5] an in-depth discussion of viruses as speech is outside the scope of this paper

How effective are these legal counter-measures likely to be in addressing problem of viruses found in the real world? In (Lemos, 1999) we read

> *"Despite an expected four- to five-year sentence for admitted Melissa virus writer David L. Smith, the number of new viruses appearing on the Internet appears to be accelerating as the end of the millennium draws near, anti-virus firms said Friday*."[6]

Laws to combat computer crime are not new. The first comprehensive proposal for computer crime legislation was a federal Bill introduced in the US Congress by Senator Ribikoff in 1977. (Schjolberg , 2000). Since that time, many U.S. states have introduced various computer crime laws, several of which mention viruses specifically (Bordera, 1997).

Some of these laws and statutes even attempt to define what a virus is. For example (Bordera, 1997) cites the revision of the State of Maine's statute title 17-A, ßß 431 to 433 (West Supp. 1996)

> *"any instruction, information, data or program that degrades the performance of a computer resource; disables, damages or destroys a computer resource; or attaches itself to another computer resource and executes when the host computer program is executed.*"

The State of Maine has a particular subsection dealing with viruses, ß433c, citing

> *"intentional or knowing introduction or allowing the introduction of a computer virus into any computer resource, having no reasonable ground to believe that the person has the right to do so.*"

The offense is classified as a Class C crime.

In (Froehlich, Pinter, and Witmeyer, 2000) documentation of differentiation between naivete and malice is made:

> *"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.*"

There have since been various committees formed worldwide that have attempted to deal with the problem from a legal perspective (Schjolberg, 2000). From some of these committees international laws addressing computer crime have emerged, some of which address virus issues specifically. For example, in 1995, the Iranian Government approved a computer crime law prepared by the High Council of Informatics. Program damage caused by viruses, Trojan horses, worms, and logic bombs are spelled out in this law. Other countries have laws that forbid the spreading of and in some cases the writing of, computer viruses (Iran, 2000). How have the existing laws been used so far? First, we will consider three individual cases.

Research by (Akdeniz & Yaman, 1996) documents the case of Dr. Joseph Popp, an American who was apprehended and arrested by the FBI at the end of 1989. Dr. Popp had sent free computer diskettes to ~20,000 people in London and around the world; these disks contained a program which supposedly assessed the user's risk of contracting the AIDS/HIV virus, but which in reality introduced a trojan horse to the users computer. According to Akdeniz,

> *"Recipients of the disk were warned that their computers would stop functioning unless they paid the license fees of £225 to a bank account in Panama. This case is thought to be the world's most ambitious computer crime. While Dr. Joseph Popp was extradited to the UK, his case never came to trial due to a deterioration of Popp's mental state; he was found mentally unfit to stand trial*."

---

[6] this assertion is examined later in this paper

(Taiwan, 1999) describes how, in 1999, the Computer Crime Unit traced the CIH virus to a young man then serving in the military. He confessed he had written the virus, claiming he was motivated by pure research, and had not himself spread the virus. According to this report,

> *"if 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."*

Christopher Pile, known as the "Black Baron" in the computer underground, was sentenced to 18 months on 15 November 1995. Pile was charged with violations of Section 3 of the Computer Misuse Act 1990. He pled guilty to five charges of gaining unauthorized access to computers, five of making unauthorized modifications and one of inciting others to spread the viruses he had written.

Laws – Effective?

In order for a crime involving a virus to be prosecuted, it must first be reported. Minnesota statute ßß 609.87 to .89 presents an amendment which clearly defines a destructive computer program, and which designates a maximum imprisonment or 10 years; however, no cases have been reported. Should we conclude there are no virus problems in Minnesota?

In (Grable, 1996) the ineffectiveness of the laws, both Federal and New York State, as a solution to the virus problem are clearly spelled out:

> *"Both the federal and New York state criminal statutes aimed at virus terror are ineffective because the methods of enforcement… The combination of the lack of reporting plus the inherent difficulties in apprehending virus creators leads to the present situation: unseen and unpunished virus originators doing their damage unencumbered and unafraid. Add to that the slap on the wrist afforded to even the most infamous of virus propagators, and the recipe is right for even greater damage from malevolent software."*

How likely are laws to affect the young virus writer? We first examine legal intervention related to young people engaged in other antisocial activities.

(McDowall & Loftin, 2000) analyze the success of curfew laws in controlling crime. They state that while several police departments report a decrease in youth offenses after the enforcement of curfew ordinances (Bilchik, 1996) claim that statistics supporting the efficacy of curfew laws in reducing crime rest on uncertain comparison groups, and that few evaluations have considered more than a single area. They conclude there is *not* strong evidence that the curfew laws reduce juvenile offending or victimization rates. However, despite this lack of evidence, these laws have been embraced by many communities; (Hemmens & Bennett, 1999) state that while it is unclear whether they are effective in reducing crime, it is clear that they are being embraced by communities across the country (Davidson, 1997).

In other studies of youths living in areas where anti-social activity is normal, some youth may accept confronting danger and being involved in these activities as features of living in such environments (Halliday & Graham, 2000). There is insufficient data to conclude if this phenomenon maps to virtual environments.

Research by (Foglia, 1997) supports the hypothesis that while the possibility police involvement, or legal sanction does not offer significant deterrence for youths who engage in antisocial behaviours, they *are* likely to be influenced by parents and peers. In (Gordon, 1994a), the conclusion that the "common" young virus writer is not likely to be affected by laws is supported, citing both the non-universality of the laws as well the mixed messages sent societally to the young people as they integrate into the cyber-culture.

Difficulty in sentencing minors is also to be considered; some research is being done in this area. (Simpson, 1999) examines research into state statutes in the United States that help make parents legally responsible for personal injury or damage to property made by their minor children. There are details on a case in Minnesota (the land of no viruses ☺), and another in Oregon, where such provisions currently exist.

Finally, we must *not* ignore the mixed messages sent to young people regarding virus writing. (ZiffDavis, 1999) reports

> "[the firm that hired the virus author]…*competed with a score of high-tech rivals attempting to lure* [the virus author]..."
>
> *"'Our chairman felt he* [the virus author] *was a rare computer professional and we decided to accept him with an open heart,' said Wahoo spokeswoman Vivi Wang."*

Contrast that to the alleged writer of the Melissa virus, David L. Smith. Apprehended at the beginning of April, Smith is looking at a maximum sentence of 40 years if convicted in New Jersey State Court. The immense differences in punishment illustrate a large rift in perceptions over the seriousness of computer viruses.

Lack of Metrics

Perhaps one of the reasons that there are so many different opinions on the effectiveness of legislation is that little quantitative data has been gathered. How does one go about measuring the effectiveness of a law? While it is tempting to simply measure the number of arrests as a function of time and law, this is not a good approach given the small number of virus writers who have been arrested and tried. Indeed, this lack of arrests is one of the primary indicators used by some to argue that laws are not a good deterrent.

One of the ways in which we can judge the efficacy of law as a deterrent is the overall view of society toward the acts which have been criminalized (Bagaric, 1999). However, we must be careful not to impose our view of the act on others when attempting to use the criminalization as a "proof" that the act is "wrong". For example, the use of marijuana is a criminal offense in some places/situations; in others, it is a misdemeanor, and in yet others, it is an acceptable act.

New Metrics and Research Techniques

As virus writing is a relatively infrequent "crime", a better measure of efficacy might be to study the number of times this "crime" has resulted in viruses let loose into the user community. However, how shall we define this output of "crime"? While it is true that in practical terms, a measure of the virus problem can be derived from the infection rate per 1000 PCs, this figure is affected by far more than just the number or activity of virus writers. New types of virus, a virus "getting lucky", or simply press coverage for a well-known virus can skew this number. Similarly, the total number of known viruses is not necessarily a good indicator, as this number is somewhat artificial in its creation. Thus, we propose the following new metrics for measuring, albeit indirectly, the efficacy of legislation with respect to the virus "problem".

One possible way of measuring the prophylactic effect of laws is obvious: ask! Based upon previous research, we have built a reliable and open dialogue with many of today's more visible virus writers.

As this "known" population is relatively small (but has a large impact on many developments in the virus world) a directed survey was created and administered. Questions (shown in the results section) were initially distributed via electronic mail and in-person sessions to virus writers in North and South America, Asia, Europe and Australia. The questionnaire was also posted to the Usenet News Group alt.comp.virus. The theory is that by re-administering the questionnaire after a high-profile criminal case concerning viruses, any suppression in the tendency to write viruses could be documented.

Unfortunately, the sentencing of David Smith has been delayed several times, so at this time the administration of the post-test questions and analysis of that data is not possible. Following the sentencing of David Smith, the post-test will be administered and the results posted on the online version of this paper[7]. One drawback with this approach is that we expect some virus writers to become more socially aware as they "age out"; thus a significant delay between administering the two tests could make the results difficult to interpret for individual subjects. However, the average population should remain reasonably static, making the test a possible metric for evaluation of effectiveness of laws.

As intimated above, the full measure of the scope of the virus "problem" itself is extremely hard to measure. How "bad" is the "problem"? Can it be measured by the number of known viruses on a particular date? The number of viruses encountered "In the Wild"? The infection rate per 1000 PCs?

The answer to this question depends partly on perspective and partly on the need for the measurement. 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 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[8]).

As it seems unlikely that *writing* a virus that never ever is distributed would be made illegal in The United States, we propose that a suitable measure of the problem for a legislator is the number of viruses found "in the wild". Thus, it might be interesting to correlate the rate of change of the number of new viruses in the wild with high-profile prosecutions of virus writers. To this end, we have charted viruses "in the wild" as a function of time. If a noticeable decrease in the number of new ITW viruses is observed following an arrest/sentencing, the case could be made that the trials were helping the overall computer user population.

Another metric for the efficacy of laws is the availability of viruses on the WWW. We performed an in-depth analysis using one popular search engine, with the keyword of "virii", as a way of locating web sites that appeared to have content bearing further analysis. Once again, if the number of "virus exchange" web sites (sites containing live viruses or viral source code) could be shown to decrease with new legislation/prosecution, there would be evidence for the effectiveness of the current legislative attempts at controlling the spread of computer viruses.

Finally, there is the question of a possible backlash against legislation outlawing the development and distribution of computer viruses. As tracing a virus author is extremely difficult *if* the virus writer takes adequate precautions against a possible investigation, there is a possibility of a backlash against any legislation which a person or group deems unconstitutional or as an infringement.[9]

---

[7] http://www.av.ibm.com, http://www.badguys.org

[8] Liabilities and legislation related to naturally occurring software or hardware induced corruptions are beyond the scope of this paper.

[9] further discussion on cyber-activism or civil disobedience is outside the scope of this paper

To this end, a survey was conducted at the 2000 DEFCON conference held in Las Vegas. The conference, attended by many "white hat and black hat hackers" represents an important part of the computer security "counter culture", and in many ways attracts the exact group that laws against virus writing would be aimed at. We selected people randomly as they entered the conference foyer[10]. To help ensure people could understand the survey questions, and answer coherently, the selection was done on the first day of the Conference, early in the day, in order to sample people before they were intoxicated.

Results

The results from direct interviews provide an entirely subjective (but collectively representative) view of how people said they felt about the following four questions:

1. What (if any) impact do you believe the arrest of David Smith has had on virus writing and virus distribution to date?
2. What (if any) do you believe is a fair and just sentence for David Smith?
3. What do you believe his sentence will actually be?
4. What (if any) impact do you think the sentencing of David Smith will have on virus writing and virus distribution post-facto?

We shall now consider each question in turn, and show data from several differently classified sources.

The Impact of the Arrest of Smith

The following results are broken down into those involved in the virus writing/virus exchange scene, and those who are not (primarily, but not exclusively, virus researchers)

Virus writers and exchangers:

> *"I'm not sure I've seen any change in virus distribution. There's as little interesting code being released as there was, and as much crap as ever. More to the point, those who are clueful knew that someone was going to be 'tracked down' and 'busted' soon. Those who are clueful aren't releasing code anyway (at least, not to the public). Those who aren't clueful don't understand how David Smith got busted and are probably still doing what they were doing before Smith got busted.*
>
> *If anything, the effect was on virus writing. There were probably people out there who thought about writing viruses for fun, but got scared out of it for fear of 'getting busted'. I don't think we'll see it making a big impact on the quantity or quality of viruses out there--but it probably stopped a few kids from 'turning to the dark side'. :)"* (Anonymous, 2000a)

> *"His arrest has made some authors more cautious about handing out their work to just anybody, or even putting their name on it. However at the same time, it has outraged many other authors who are now using it as an excuse [and justification] to speak out about the ills of our society, and dare I say "justice" system.*
>
> *I'd say that overall it has balanced things out, and had no real long term effect in the minds of authors, it's only set a legal precedent."* (Anonymous, 2000b)

[10] 161 subjects, 90% confidence level, 6.0 confidence interval

On the writers side, none. Foul things can happen when you code such programs, and most writers know that already. The thought of a guy getting screwed by media hype is not going to stop most people from coding what they think is interesting.

The distribution side is a bit different. Alot has changed since the shitstorm (pardon me, but there is no nicer way to describe it) of april 99. The loss of the sourceofkaos server was a big deal to us. The vx scene had a voice, and was stripped away due to the incident. The guy who hosted (we knew him as jtr) it was running the machine at his place of business. He was placed on paid leave for a few weeks, and was let go. Im sure the fbi had a field day sorting through that box. Media, the av industry, government organizations would connect to the irc which didnt help much, due to kids that didnt really know the half of what was going on a spreading rumors and publicly discussing things that they shouldnt have. Ugh, it was a mess. Those were some stressful days. This has changed alot on the distribution side. People are afraid to release information. I was the first one to come forward and give the source of iworm.zippedfiles to the public because i had to. After the minimal heat it created, a handful of news articles and such on how the fbi was in search of its author, nobody (well, only a handful had the source in the first place) wanted to come forward with it. Posting source code is not breaking the law in most of the world. People should be afraid. (Anonymous, 2000c)

Antivirus researchers:

"It has had the impact that many very active virus writers have "retired" (seen anything from the 1nternal guy any time recently?), others have become less productive, and many have refrained from releasing their viruses into the wild. I think that if Smith wasn't arrested so swiftly, we would have seen much more Melissa variants and many more from them would have been released into the wild in a similar fashion.

*Of course, sooner or later this beneficial effect will wear off. People tend to forget, and young people, like most virus writers are, tend to forget even faster. That's why the law enforcement must not "sleep on their laures" (*sic*) but must prosecute similarly swiftly offenders like Mr. Smith in the future, too."*(Bontchev, 2000)

*"I would hope that maybe it has scared away few would-be writers or discourage some from distributing their creations but I have seen no clear evidence of this. I'd say there would have to be at least *some* positive effect from this (I just don't have any evidence for that though.)"*(Stiller, 2000a)

"It did not have any and will not have any. Virus writer wrote, write and will go on writing viruses, whether one of them folks was, is or will be sentenced or not. …None. We do not saw a change after Black Baron was arrested and I do not saw a decrease of new viruses..." (Marx, 2000a)

Two other responses are worth further examination. First, from the ever-scientific (and correct!) Mich Kabay (Kabay, 2000b)

"Don't know without research. What I hope is that it will discourage some of the virus writers, but that's pure conjecture."

The second sums up a practical point of view with good evidence behind it:

"Very minimal. Most virus writers (in my opinion) think that it was a fluke that he got caught. Very little, I thing that a one off situation will not change the ways of virus writers. Only if a lot of writers - distributors where caught would this make a impact." (Pineda, 2000).

Fair and just sentence for David Smith:

Virus writers had mixed opinions.

"Hard to call. I don't really know the facts of the case. If he was maliciously distributing the code, I don't have much in the way of sympathy." (Anonymous, 2000d)

> *"An apology for ruining his life of future employment in the computer industry, a smile, and a handshake from every person that has cursed him. And perhaps a job. That's right".* (Anonymous, 2000e)

> *"To be honest, I really haven't been following the David L Smith case. But I'd say approx. 10 years max. As I once studied the law and jail sentances in an assignment about the meaning of life imprisonment (my best bit of school work that was) - and Life is only about 15-20 years. Computer data is far less important than human life, and should be judged accordingly"* (Anonymous, 2000f)

> *"A slap on the wrist. Im not saying it was right to post a virus to a newsgroup from a stolen aol account. What he has already had to deal with should be enough though. I don't think anyone would go the same route twice. Being held at gunpoint and treated as a terrorist is a bit disturbing im sure. Jail time or fines wont help, nor will locking him away trying to set an example to others. Look at kevin mitnick, doing almost 5 years without a trial and denied bail hearings. Have people stopped or even cut back on cracking machines? Of course not."* (Anonymous, 2000g)

Antivirus researchers expressed a variety of opinions:

> *"He certainly deserves substantial jail time and fines."* (Stiller, 2000b)

> *"That's for the judges to decide. He has to be punished. Something like a year in prison and a BIG fine would do."* (Gryaznov, 2000)

> *"I personally believe that David was stupid, rather than malicious, and I therefore think the sentence should be similar to the one handed out to the author of the famous 'Internet Worm' (whatever that was - I'm not sure)"* (Shipp, 2000b)

> *"… a suspended prison sentence (or time already served), some community service that will mean nothing to him, a fine he won't be able to pay, all resulting in an extremely high paying job in the field of computer security for an obscure consulting firm who will brag about their proven expertise in computer viruses."* (Pichnarczyk, 2000)

What will the sentence will actually be.

Virus writers were uncertain; a typical response is shown here:

> *"It will probably begin by looking insanely harsh, and come out to something that is soft on prison time, and nasty for his future. Some of that 'unable to be within 500 yards of a computer' bullshit, probably.* "(Anonymous, 2000h)

Antivirus researchers opinions were diverse:

> "*Probably a small amount of jail time".* (Stiller, 2000c)

> *"I think he will get a large fine, and 10 years*." (Shipp, 2000)

> "*Some years arrest... maybe much too long, even if the virus clean-up etc. costs very much.*" (Marx, 2000b)

> *"Suspended sentence, probation for a couple of years, specific interdiction of further computer-virus writing, and a fine of a few thousand dollars*." (Kabay, 2000c)

What (if any) impact do you think the sentencing of David Smith will have on virus writing *and* virus distribution post-facto.

Virus writers were consistent within their grouping:

> *"None. It is the fear of being caught that is more important to an author, than the results that occur after. For example, even if this particular case was settled in David's favour, he would still be ruined in the computer industry. That's enough."* (Anonymous, 2000i)

"None. Things like this only effect people when its in the spotlight. Its all said and done, its old news, the media wont rave about it, the end. It wont be forgotten, but it wont effect the future. Nothing changed from the black baron did it?" (Anonymous, 2000j)

Antivirus researchers:

"Marginals will stop. Hard-core will continue. After the Next One (tm) goes down, more will stop". (Thompson, 2000b)

"It depends upon the amount of media exposure and the severity of his sentence. I expect it would discourage some virus writers from distributing their creations." (Stiller, 2000d)

"Future arrests so as to make them commonplace will have such an effect. The precursor to that is "interest" from the authorities. As David Smith is responsible for creating the "interest," he will have had a tremendous impact on the future of such. But only if the authorities maintain the vigilance" (Kuo, 2000)

"An overly harsh sentence / treatment could make him into a martyr (cf. Kevin Mitnick). Too light a sentence would reduce the deterrent effect.

Overall, not a great deal, I strongly believe that the probability of getting caught is as important as the severity of the sentence in deterring potential criminals. For example, it is illegal to smoke in lifts (sorry, elevators in American translation) in HK, and lifts have signs saying the penalty is HK$5000. However, I often enter a lift and smell cigarette smoke, and I have never seen or heard of someone being fined. The chance of getting caught is (virtually) nil, so the heavy fine is no deterrent. If the fine was HK$100, but offenders were caught 50%+ of the time, the practice would quickly stop. Very few virus writers or distributors have been caught, so the severity of punishment is small deterrent." (Dyer, 2000)

"It's a mixed message. On the deterrent side, it's the classic "they'll think twice because they might go to jail" (if my desired sentence is carried out). On the flip side, it also shows virus writers how hard it is to prosecute & convict, as well as suggesting new methods for not getting caught. Ultimately, the impact will be low until the conviction volume increases." (Renert, 2000)

Survey Results and Analysis

This data shows an interesting cross section of views from both the anti-virus community and the Virus Writer/vX community. Interestingly, the vX community seems less convinced that laws will help the situation. This position does not appear to be based upon a vested interest in the unsuitability of laws, but a genuine feeling within the community that legislation will not be an effective preventative.

Perhaps the most cogent summary of this logic comes from (Dyer, 2000) quoted in response to Question 4, "Will the arrest and sentencing of David Smith have any long-term impact?": if the law will not be enforced or is unenforceable, it has little effect regardless of the penalties.

Table 1 shows a summary of the results from our survey:

	Yes	No	Maybe
Virus Writers			
Has the arrest of Smith had any impact in the virus writing community?	0	11	0
Will it have any long-term impact?	0	11	0
AntiVirus Researchers			
Has the arrest of Smith had any impact in the virus writing community?	8	7	1
Will it have any long-term impact?	7	6	3
***NB: Incidental comments include (1) too harsh sentences would be bad (2) more computer ethics classes would help and (1) requires more research**			

Table 1: Survey data. A questionnaire concerning the impact of the arrest of David Smith was presented to two different groups: those involved or in some way associated with virus writing, and those active in the anti-virus community. Note the strong reaction from the virus writers, who were emphatic that neither Smith's arrest nor any conviction/sentencing would influence them or the virus writing community in general.

Interestingly, the data is reasonably similar to a comparable survey conducted in (Briney, 2000). In the Briney survey, an informal poll was conducted among 25 well-known information security professionals, asking "will the sentencing of David Smith reduce virus writing". Of the 25 respondents, 11 said, "No", the Smith conviction will not deter others, while 9 said, "Maybe". Only 5 said "Yes".

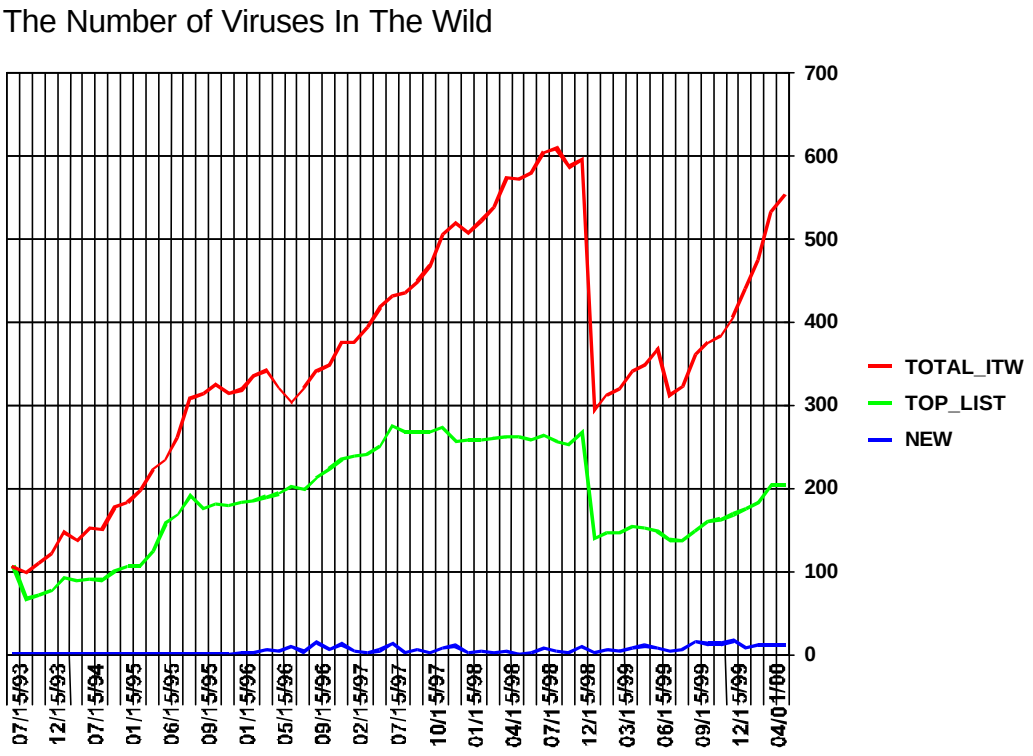

Figure 1: The Number of Viruses on the WildList as a function of time. This graph shows the number of viruses reported on the WildList as a function of time. The top (red) line shows the total number of viruses in the wild, the middle (green) line indicates just those viruses that are on the top portion of the WildList. Finally, the bottom (blue) line shows the number of new viruses added to the top part of the list per month.

As described above in the section *New Metrics and Research Techniques*, the total number of viruses In The Wild could be used as a metric of the efficacy of laws. In particular, we are interested in any discontinuity noted in the graph of viruses both newly ItW and also on the total number of viruses.

Before analysis can take place, the following descriptors should be made clear. The x-axis on the graph represents months of the WildList. The top (red) line represents the total number of viruses on the WildList, and the middle (green) line is those viruses reported by two or more reporters. Finally, the bottom (blue) line represents the rate of addition of new viruses per month. [Note that this information was only tracked from month January 1996, and so before this time the value is set to zero.]

The large discontinuity in the first two lines around January 1999 is an artifact of the change in methodology in the reporting structure of the Wildlist which resulted in a significant cleaning of the Wildlist data; rules concerning how long a virus must go unreported before being dropped from the list were enforced, leading to a significant drop in the total number of viruses listed. Note no corresponding discontinuity in the lower line; this is due to the fact that the corrections were not related to the rate of addition of new viruses, merely the renormalization of those already reported.

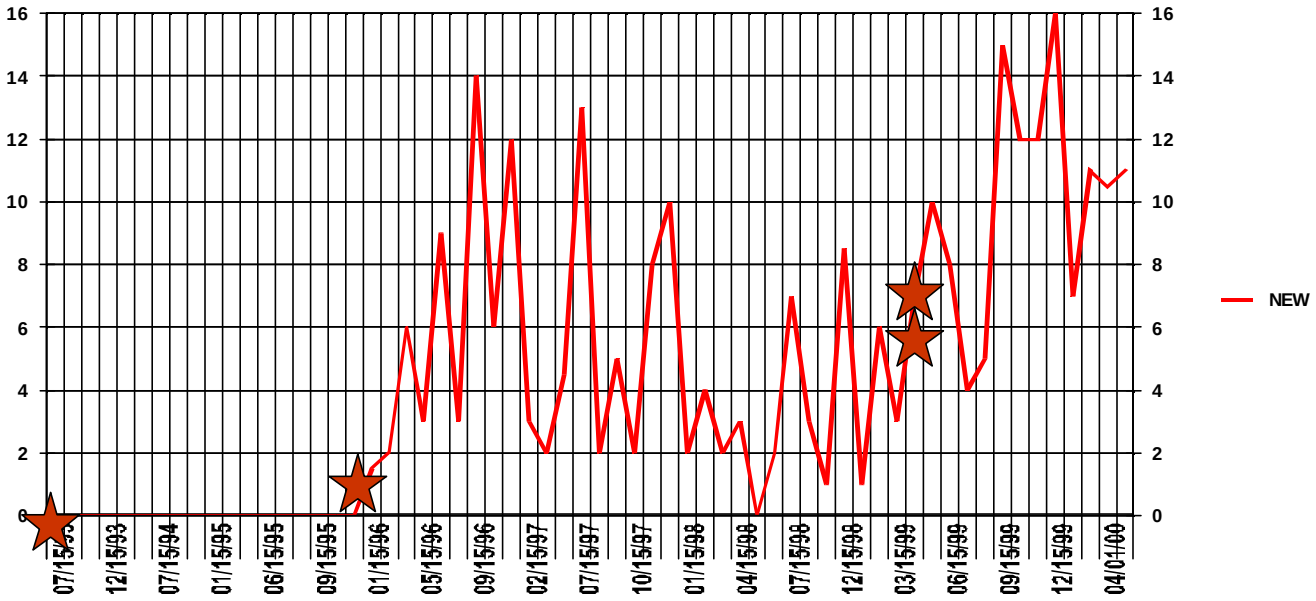

Figure 2: Detailed view of the number of new viruses added to the top portion of the WildList per calendar month. The red line shows the number of new viruses added to the WildList per month. The red stars indicate high-profile interventions. Note that there is no obvious drop in the rate of new viruses after these interventions.

As the most interesting, and arguably most relevant, data is the rate of new viruses becoming prevalent ItW, Figure 2 shows a detail of this data: On this graph, we have added stars to note prominent virus/trojan interventions or prosecutions[11]. As can be seen, the graph presents no clear evidence of any suppression in the rate new viruses were added to the Wildlist. While it can be argued that the data is (a) noisy (b) made up of more than one factor (that is, perhaps if there were no prosecutions, the graph would show a much-increased gradient) (c) lagging behind of real-world events due to the time it takes for a newly-released virus to spread and reporting cycles, one must also agree that the Wildlist data *provides no evidence to indicate that these high profile cases and*

[11] Popp, Pile, Ing-hau, Smith

prosecutions have helped depress the virus problem as measured by the rate of addition of new viruses in the wild.

As this paper represents a snapshot of ongoing research and data gathering, not all the results have yet been gathered. One important metric proposed in the proceeding section was to measure the availability of computer viruses on the WWW. In order to do this, we measured the number of hits generated upon searching for the word "virii", using the Google™ search engine[12]. We examined each site to see if it offered viruses. The following results were noted:

On March 15, 2000 Google results netted 5080 for "virii". A manual examination of the first 1000 hits netted 65 sites with viruses (in executable or source code form) available for download. This means that approximately 6.5% of those sites surveyed contained live viruses or source code.

On August 18, 2000, Google results netted 20,600 results for "virii". An examination of the first 360 hits showed 102 sites with viruses (in executable or source form). This means that 28% of the sites surveyed contained viruses; a significant increase over the first data set.

It should be noted that the interesting figure in this experiment is **not** the total number of hits, but the percentage of those hits which contain viruses. As can be seen from the results, the percentage of sites which contain the word "virii" that also have live viruses has increased. While some optimization in search ordering may be responsible for this increase, this change in percentage is not likely to be due to a simple increase in the number of sites surveyed. Thus, this test does not show any convincing evidence for a decrease in the availability of computer viruses – if anything, viruses are more readily available now than ever before. After the sentencing of Smith, it will be interesting to note any effect on these figures.

One interesting by-product of the research was that some web authors noted that laws (or more correctly, fear of legal consequences) have certainly suppressed the dissemination of virus samples from some of the sites. Here are some examples of verbiage used on some of the sites:

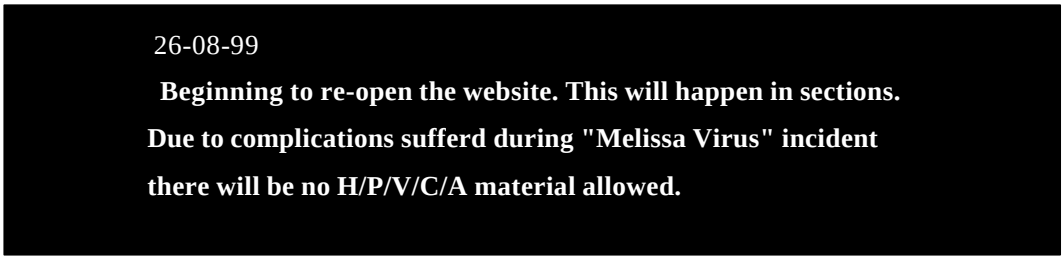

Figure 3: Screen shot from a vX site on August 8, 1999

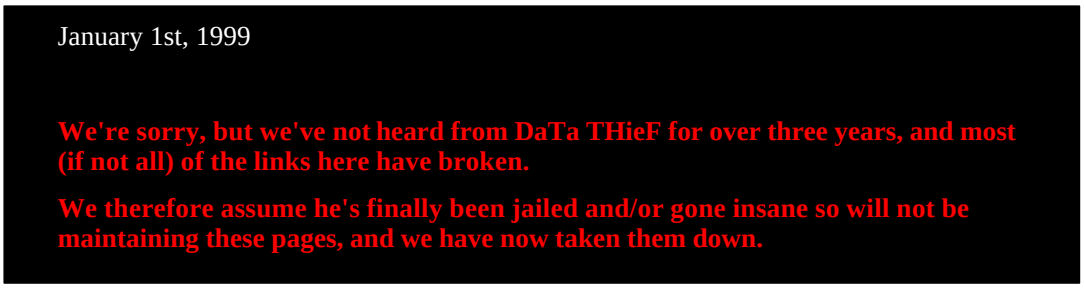

Figure 4: Screen shot from a vX site on January 1, 1999

---

[12] Google displays web sites based on page-rank. Thus, it retrieves pages based on the number of other pages which point to it. Therefore, the more highly visited pages are ranked first, with new pages being added as they become more popular

However, new sites have taken their places, including this one in The Netherlands, where such activity is illegal.

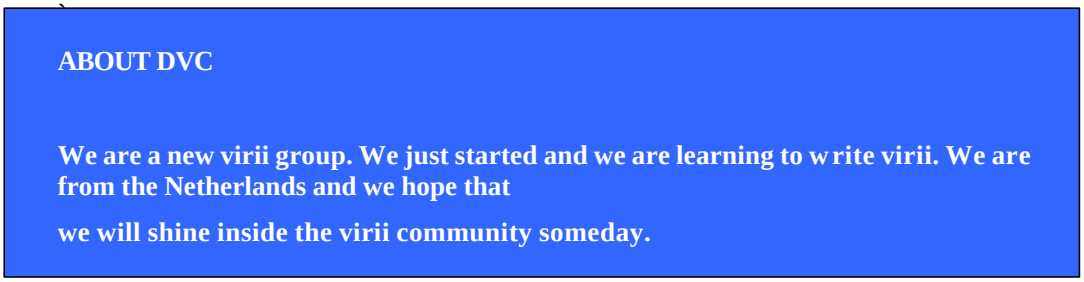

Figure 5: Screen shot from a vX site in August, 2000.

DEFCON Survey Data

A survey regarding reactions to proposed virus-writing legislation was also conducted. In this portion of the study, we chose the population of attendees at DEFCON (www.defcon.org), and asked two questions (The exact questionnaire is reproduced in Appendix A; however, the questions were posed verbally using the document as a reference):

- If virus writing were to be made illegal, would that make you less likely to write a virus (noted as Group 1); more likely to write a virus (noted as Group 3); or make no difference to your likelihood of writing a virus (noted as Group 2)?
- Given that what a person thinks is generally viewed as their own business, and that intentionally going out to cause someone problems with a virus by intentionally infecting their computer is viewed as "not ok", where on this scale of "how far would you go" do **you** personally draw the line at acceptable behaviour?

Then, we presented ordinally scaled actions ranging from those that would be almost universally accepted as right/okay, to an action that was almost universally accepted as wrong[13]. The resulting data is presented below as a set of histograms.

There are several different levels of analysis that can be performed on these data. At the simplest level, we can examine the data related to the first question: what was the stated effect of proposed laws. Interestingly, it seems that there is a significant set of people who claim that the criminalization of virus writing would encourage them to write computer viruses. Based upon verbal comments by the respondents, this was primarily due to their feeling that such a law would unfairly restrict their free speech.

Next, one can examine whether there is any correlation between the first answer and the second; that is, if we group the sample set based upon their reaction to laws, does one group appear more ethically developed than the other? Calculating the sample mean and standard deviation from each of the groups, we see that it is difficult to show any significant differences on the samples answers to question II based upon group. This is partly due to the fact that the data is clearly not normally distributed, although a visual analysis of the data does also tend to show a strong relation between the different groups.

[13] Time did not allow the preparation of a true Likert scale; this would be an interesting project for future research.

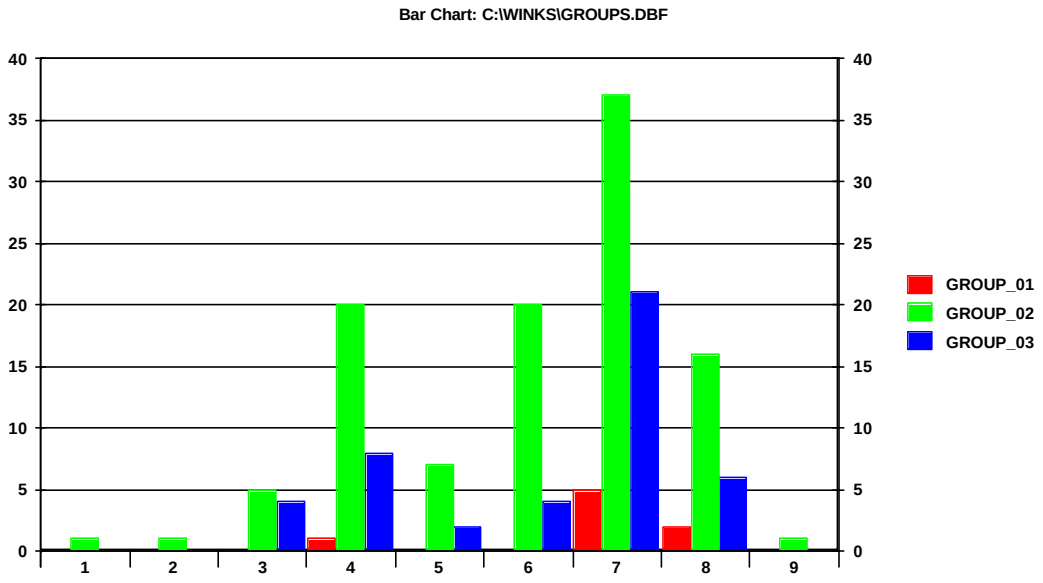

Figure 6: The effect of laws. Respondents were grouped depending on answer: those who would be deterred by laws (Group_01), those for whom laws made no difference (Group_02), and those who would be incited to write viruses by a new law (Group_03). Thus, new laws may cause an increase in the number of computer virus writers.

The fact that individuals with a low tolerance for virus exchange in general expressed that proposed legislation against virus *writing* would make it more likely they would write a virus is interesting.

It would be interesting to compare this data with that from students in a computer science course, in order to get some measure of the another population. However, in *ad hoc* studies conducted by the author within such environments, at least the reaction to proposed new laws appears to be similar.

Finally, it is interesting to note that some individuals mentioned that letting a virus you have written out of your own personal control accidentally was much more wrong than giving that virus to a friend; “stupidity” was cited as more wrong than intentional distribution.

Conclusions and Suggestions for Future Research

The focus of this research has been to gauge the impact of legal and high-profile intervention to the problem of damage caused by computer viruses. The data has shown that laws are of some limited effect in certain sections of the population, but that there could be a backlash in the United States to a law that was viewed to be a violation of an individual’s rights to speech. While the free speech question as it pertains to computer viruses is unclear, this is immaterial: the key issue is that there are certain segments of the computing population within the United States who would *view* such a law to be unconstitutional, and state they would act accordingly. Further research on the likelihood of follow-through on electronic civil disobedience would appear to be an important next step in assessing the impact of legislation directly aimed at virus writing. Additionally, as the virus writing subculture is an international population, civil-disobedience and activism crossover between populations with laws and without laws bears further investigation.

A comparison of the number of viruses in the wild to high-profile virus writer cases/actions does not show any clear correlation with a decrease in the creation of new viruses. Indeed, despite much effort, the rate of addition of new viruses to the WildList appears to be increasing.

Tests and assessments should never be interpreted in isolation; thus, considering the strength of the responses can be as important in seeing the overall picture as the consideration of the statistical data. Additionally, this “strength of conviction” must be considered alongside the worldview of the

population. Consider that any laws created/enforced are aimed at a very small, but active virus writing community; the strength of conviction related to the DEFCON data seems to indicate that the creation of such laws would actually create more new virus writers than deter existing ones. This, coupled with the relative unenforceability of such laws could lead to a situation that is actually worse than the one we have currently.

Thus, examining all the data currently available, we are unable to show that the aggressive legislation directed toward, or intervention related to, virus *writers* will have any positive impact on the virus "problem" as defined by a number of different metrics.

We await the outcome of the post-sentencing interviews with interest. If the interviews show a significant change from their pre-sentencing results, proponents of thorough police follow-up of virus writers will have some hard data with which to back up their position. Conversely, if there is no appreciable difference in the data, we must, as a judiciary, re-evaluate the costs associated with pursuing legal remedies and high-profile "legal" interventions to a primarily sociological phenomenon.

Perhaps instead of attempting to raise support for making virus writing illegal, the energy and associated funds currently being expended would be better spent on education, with legal action or high profile intervention reserved for cases where an individual's clear and direct intent to damage could be shown.

An obvious objection to the lack of interventions is, quite simply, that the virus author should be held responsible for the results of his creation. After all, whether an infection occurs as the result of direct action from the virus writer (i.e. the virus is written, and uploaded to a Usenet News Group, masquerading as a legitimate utility) or is put into circulation via the WWW (i.e. clearly labeled as a virus on a virus exchange WWW site), the fact remains: someone created the virus that is responsible for the infection. The question is what, if any, responsibility does the creator of the virus hold?

In cases where a direct relationship between the virus author and a crime involving his virus can be shown, adequate existing legal measures can be applied. However, in cases where a virus author claims a "right" to make his or her virus freely available, or gives the virus away to knowing and willing recipients, but does *not* directly cause an infection, should we assume the question of responsibility dissipates? Opinions on the degree of responsibility vary, but one respondent's comments on this issue bear further examination:

> *"Shouldn't they really know by now that these things can cause problems whether they mean for them to or not!?"*

Unfortunately, in many cases we continue to see a typical pattern of older virus writers "aging out", while a new, inexperienced batch is still being birthed. By the time a virus writer is of age to know better, and to recognize the impact of these actions on others, they are already beginning to disassociate with their virus writing activities. Thus, while in some ways there is an "end of innocence" by those who realize their mistake, and exit the field, there is a complete pipeline of new authors just beginning their exploration. For this reason, it is flawed to simply assume that there is no innocent in the virus writing world; far from it: there are many.

This innocence and naivete, combined with the rapidly accelerating growth and evolution of technology, create a problem that is far more complex than socio-technological problems of the past. Other technologies that have been hugely influential on our societies have developed relatively slowly, thus enabling us to keep pace, predict future trends, and impart values related to those technologies to our young people. Now, however, the technology upon which we are attempting to base our projections is evolving rapidly. As the virus writing subculture continues to evolve, we are likely to see an exacerbation of problems relating to the technologies we are developing. The real question is how to best deploy our resources to protect us from this learning process, in which we are all participants.

Bibliography

Akdeniz & Yaman. 1996. *The Computer Misuse Act 1990: an Antidote for Computer Crime* First Published in Web Journal of Current Legal Issues in association with Blackstone Press Ltd.

Anonymous, 2000a-j. *Private e-mail correspondence*. Used with permission.

Bagaric, M. 1999. *Sentencing: The Road to Nowhere.* Volume 21 Number 4. December. The Sydney Law Review. University of Sydney, Australia.

Bilchik, S. 1996. *Curfew: An Answer to Juvenile Delinquency and Victimization?* OJJDP Juvenile Justice Bulletin .

Bontchev, V. 2000. *Private e-mail correspondence*. Used with permission.

Bordera, M. *The Computer Virus War: Is The Legal System Fighting or Surrendering?* Computers & the Law Project. Computers and Law, University of Buffalo School of Law.

Briney, A. 2000. *Private e-mail correspondence*. Used with permission.

Cobb, S. 1998. *Taming Wild Code.* Information Security Magazine. April.

Davidson, M. 1999. *Do you know where your children are?* Reason Online. November. http://www.reason.com/9911/fe.md.do.html

Dyer, A. 2000. *Private e-mail correspondence*. Used with permission.

Foglia, W. 1997. *Perceptual deterrence and the mediating effect of internalized norms among inner-city teenagers*. Journal of Research in Crime & Delinquency, Vol. 34 Issue 4, p. 414

Froehlich, J., Pinter, E. & Witmeyer, J. 2000. *Making The Time Fit The Crime.* Legal Column Archives. http://www.fmew.com

Gordon, S. 1994a. *The Generic Virus Writer.* From the Proceedings of the International Virus Bulletin Conference. Jersey, Channel Islands. pp.121 – 138

Gordon, S. 1994b. *Faces Behind the Masks.* Secure Computing Magazine. November 1994.

Gordon, S. 1995. *Technologically Enabled Crime: Shifting Paradigms for the Year 2000.* Computers and Security Journal. December 1995.

Gordon, S. 1996. *The Generic Virus Writer II.* From the Proceedings of the International Virus Bulletin Conference, 1996. Brighton, UK. pp. 177 – 188.

Gordon, S. 1999. *Viruses in the Information Age*. Virus Bulletin. June, July, & August. 1999. http://www.badguys.org/vb3part.htm

Gryaznov, D. 2000. *Private e-mail correspondence*. Used with permission.

Halliday, C. & Graham, S. 2000. Personality & Social Psychology Bulletin, May 2000, Vol. 26 Issue 5, p. 5480.

Hemmens, C. & Bennett, K. 1999. *Juvenile curfews and the courts: Judicial response to a not-so-new crime control strategy*, Crime & Delinquency, Jan99, Vol. 45 Issue 1, p99.

Grable, J. 1996. *Treating Smallpox with Leeches: Criminal Culpability of Virus Writers and Better Ways to Beat Them at Their Own Game.* Computers & the Law Project. University of Buffalo School of Law.

ICSA. 1999. *ICSA Releases 1999 Computer Virus Prevalence.* http://www.icsa.net/html/press_related/1998/virusprev98.shtml

Iran. 2000 http://www.gpg.com/homePages/peik/policies.htm

Jenislawski, S. *Melissa Virus Author Admits $80 Million in Damage.* http://www.policy.com/news/dbrief/dbriefarc439.asp

Kabay, M. 2000a. *Viruses are not Speech*. Virus Bulletin. "Comment" July 2000

Kabay, M. 2000b. *Private e-mail correspondence*. Used with permission.

Kabay, M. 2000c. *Private e-mail correspondence*. Used with permission.

Kohlberg, L. 1981. *The Meaning and Measurement of Moral Development*. Clark University Press. Worcester, MA.

Kuo, J. 2000 *Private e-mail correspondence*. Used with permission.

Lemos, R. 1999. *'Tis the Season for Computer Viruses.* http://www.zdnet.co.uk/news/1999/49/ns-12098.html. December.

Marx, A. 2000a. *Private e-mail correspondence*. Used with permission.

Marx, A. 2000b. *Private e-mail correspondence*. Used with permission.

McDowall, D. & Loftin, C. 2000. *The Impact of Youth Curfew Laws on Juvenile Crime Rates.* Crime & Delinquency, January 2000, Vol. 46 Issue 1, p.76.

Panzl, B. & McMahon, T. 1989. *Ethical Developmental Theory and Practices.* From the 71st Annual Meeting of the National Association of Student Personnel Administrators. Denver, Colorado.

Pichnarczyk, K. 2000 *Private e-mail correspondence*. Used with permission.

Pineda, R. 2000. *Private e-mail correspondence*. Used with permission.

Renert, C. 2000 *Private e-mail correspondence*. Used with permission.

Schjolberg, S. 2000. *The Legal Framework- Unauthorized access to Computer Systems.* Byrett, Norway.

Shipp, A. 2000a. *Private e-mail correspondence*. Used with permission.

Shipp, A. 2000b. *Private e-mail correspondence*. Used with permission.

Simpson, Michael. 1999. *Laws That Make Parents Pay.* National Education Association Today, Mar99, Vol. 17 Issue 6, p25.

Stiller, W. 2000a. *Private e-mail correspondence*. Used with permission.

Stiller, W. 2000b *Private e-mail correspondence*. Used with permission.

Stiller, W. 2000c *Private e-mail correspondence*. Used with permission.

Stiller, W. 2000d *Private e-mail correspondence*. Used with permission.

Thompson, R. 2000. *Private e-mail correspondence*. Used with permission.

Tippett, P. 2000. http://www.thesunnews.com/news/stories/2074548.htm

Taiwan, 1999. *Caught in the Net. Is Cyberspace a new haven for crimes*. Taiwan He@dlines. No. 70. http://www.taiwanheadlines.gov.tw/19991214/1999121413.htm

ZDNET, 1999. http://www.zdnet.co.uk/news/1999/51/ns-12354.html

Appendix A

These questions were presented verbally to a random sampling of attendees of the DEFCON conference.

Some people want the writing of self-replicating computer code to be illegal. If this were to become a reality, would you be:

(a) Less likely to write self-replicating code

(b) Not influenced one way or the other (makes no difference)

(c) More likely to write self-replicating code

Given that what a person thinks is generally viewed as their own business, and that intentionally going out to cause someone problems with a virus by intentionally infecting their computer is viewed as not ok, where on this scale of "how far would you go" do **you** personally draw the line at acceptable behaviour?

1. Thinking about writing the virus
2. Talking on a BBS about how you might write the virus
3. Writing the virus on your own computer, but never giving it to anyone.
4. Writing the virus on your own computer and having it escape accidentally
5. Writing the virus on your own computer and giving it to one or two friends
6. Writing the virus and uploading it to a VX site, labeled as a new virus.
7. Writing the virus and posting it to Usenet labeled as a useful application
8. Writing the virus and deliberately infecting other people's computers with it.