Int. J. Human-Computer Studies (2000) **52,** 899–913
doi:10.1006/ijhc.1999.0361
Available online at http://www.idealibrary.com on IDEAL®

Some human dimensions of computer virus creation and infection

Andy Bissett
School of Computing & Management Sciences, Sheffield Hallam University, City Campus, Sheffield S1 1WB, UK. email: a.bisset@shu.ac.uk

Geraldine Shipton
Centre for Psychotherapeutic Studies, University of Sheffield, 16, Claremont Crescent, Sheffield S10 2TA, England

(Received 19 March 1999; accepted 3 November 1999)

Infection of computer systems by destructive computer viruses is a commonplace occurrence. Consequently, an extensive literature exists concerning the technical means of virus prevention, detection and disinfection. By contrast, in this paper we consider the human dimensions and implications behind the invention and release of computer viruses. We examine and discuss some possible conscious motivations: these include political, commercial and malicious. However, the paper is also concerned with unconscious motivations and goes on to look at possible meanings for these disruptive activities from within a psychodynamic framework based on the work of Melanie Klein. The paper draws upon previously published information about viruses and their makers in order to furnish material for these discussions. Of equal import in understanding the effect that virus infection has upon computer users. A personal anecdote illustrates the disruption to peace of mind brought about simply by the fear of virus infection. We conclude that virus creation means different things for different perpetrators, but that generally it is a destructive act aimed at dismantling what is apparently 'whole' and satisfactory. This reflects the reality that human life involves a constant struggle with processes of destructiveness as well as creativity. Paradoxically, the orderly, constructed world may become stronger through the process of learning and defending against each new virus, but this strengthening of defences may itself inflame the problem. We conclude by considering some concrete consequences for computer users, and areas for future investigation.

KEYWORDS: virus-maker; psychoanalysis; motivation.

1. Introduction

Computer viruses have become a common problem for computer users over the last decade, in fact it is claimed that 90% of companies experience a destructive virus attack each month (Taylor, 1997*a*). Computer viruses were initially theorized by Cohen (1994), and a refinement of his work has recently been presented by Thimbleby, Anderson and Cairns (1998). Both Cohen (1994) and Thimbleby (1990) have suggested that the mechanism of the computer virus can be employed for useful effect, for example in practical 'housekeeping' tasks around a network of computers.

1071-5819/00/050899 + 15 $35.00/0

Unfortunately, this benign aspect of computer viruses has not been widely, if at all, exploited. The overwhelming majority of computer viruses are destructive in their effect. The damage is often done even when the virus does not have an explicit destructive 'payload', since viruses often have unforeseen side-effects. The construction and propagation of such computer viruses is clearly a highly unethical practice. Their main effect is to disrupt and deny the resources of a computer or computer system to the people using it. This may result in considerable if not complete loss of work, and can have extreme emotional and financial consequences, or even safety or political consequences. Meckbach (1997) cites the case of an unnamed US 'financial institution' shutting down for three days due to a virus infection, at a cost of $2.3 million in lost transactions. The US National Computer Security Association (NCSA) estimated that in 1996 the costs of viruses to US companies and organizations was between $2 billion and $3 billion, up from approximately $1 billion in 1995. Virus infections had increased almost 10-fold compared to 1995 (Kehoe, 1996).

In 1997, an NCSA survey of 300 medium- and large-sized (Fortune 500) organizations in North America found that over 99% had encountered a virus within the previous six months (Berg, 1997; Meckbach, 1997). These organizations expected approximately 35 virus incidents per thousand PCs per month in 1997 (Berg, 1997). The survey shows that the rate of infection is rising, with the number of virus encounters in January 1997 almost equal to the total number of encounters between July and December of 1996. This increase is not surprising given the rate at which new viruses are being invented and released.

It is noteworthy, however, that many of these 'new' viruses are produced by making slight modifications to existing viruses. For example, the Stoned virus existed in a version which prints the message 'legalise marijuana' rather than 'legalize marijuana', and these are counted as two distinct viruses (Kane, 1994). Kane goes on to note that many 'new' but trivially altered viruses seem to satisfy their creators once they are officially noticed and recorded, the aim being to have one's virus entered on the 'roll of honour'. This is akin to the graffiti artist's 'tag' being prominently displayed.

The 1997 NCSA survey found that the average amount of server downtime caused by a 'virus disaster' (defined as the infection of 25 or more PCs) dropped from almost 6 h per incident in 1996 to 40 min in 1997 (Berg, 1997). The survey implies that companies are learning to deal with viruses more effectively. The cost of recovery from a virus disaster averaged $8300, and the time taken for full recovery averaged 44 h. These figures are similar for the previous year, 1996. However, the survey shows that the number of person-days needed to effect a complete recovery rose from 10 in 1996 to 22 in 1997. This may reflect an increased ease of virus propagation through inter and intranets—more people need to respond in an incident, although each for a smaller amount of time. Thus, it seems that virus encounters have become routine. Kephart and White (1994) have noted the distinctive plateau phenomenon in the rate of infection by a given virus. However, distinctly greater disruption is caused when a virus embodies a new way of propagating itself before the specific anti-virus measures are in place (Ford, 1999).

Several authors make the omnious point that once a virus has entered the public domain, it is a much simpler task to alter the existing virus rather than to invent a completely new one, and this implies ample scope for malicious augmentation of the

destructive effects. Since 1992 virus-making kits have been available, and these are widely disseminated via Internet facilities (Hruska, 1998).

By 1997, some 12 000 different viruses had been launched (Meckbach, 1997), and many more continue to be conceived and released, for it is generally held that there is no completely secure defence against them in the present environment. However, once a virus has been identified then a means of combating it may be formulated. Production and distribution of anti-virus programs has therefore become a lucrative industry. Thimbleby (1994) has proposed a technical means of preventing the spread of computer viruses, by using common encryption techniques in a radical way. Unfortunately, his scheme appears unlikely to be adopted wholesale due to entrenched commercial interests and practices.

In the next section, we briefly survey the different types of virus and some conscious motives behind them. Using examples of viruses we survey the effects, both intended and unintended. In Section 3 we examine likely unconscious motivations behind virus creation and dissemination.

2. Computer viruses

The naming of the process by which malicious software ('malware') affects computers is an important issue. Parker (in Denning, 1990) argues that it is unhelpful to continue to use euphemisms like virus-making which carry connotations of medical research, preferring the term computer program contamination, assigning a more precise and negative meaning to the activity. The nomenclature of the activity affects how we might think about the manufacturers of the products and how we might deal with them in terms of prevention and punishment. Certain authors have found the biological metaphor helpful in suggesting defence mechanisms against virus infection (Kephart, Sorkin, Chess & White 1997), although Thimbleby *et al.* (1998) warn that this metaphor has its limitations. For the purposes of this paper, we will continue with common usage and refer to viruses.

The distinguishing feature of a computer virus is that a threat of damage or destruction comes from a piece of software, rather than directly from a human being interacting with the computer system. The threat origin is very much at several removes, especially in time, and usually geographically. The first theoretician of computer viruses, Fred Cohen, describes this phenomenon as 'range' (Cohen, 1994). He identifies two further self-explanatory key characteristics of viruses as 'generality' and 'persistence'.

Another distinctive feature of computer viruses is that, like their biological analogues, they are self-replicating. They can copy themselves to other locations and computer systems. This means that they require a symptomless incubation period, which allows the virus a better chance to propagate before detection. The incubation period may be based on such factors as elapsed time since infection, a particular calendar time at or after which symptoms become apparent, or a count of the number of replications the virus has made, as in the Lehigh virus (Leiss, 1990). For example, the otherwise quiescent Michelangelo virus manifests itself on 6 March (the birthdate of the artist) by deleting files; the Jerusalem virus deletes any program run on Friday 13th, the CIH virus is triggered on 26 April, the anniversary of the Chernobyl nuclear disaster, (although one variant will tirgger on the 26th day of any month). One anti-virus company reports estimates that when CIH first triggered in 1999 it had already spread to as many as one

million computers in Korea, causing damage costing more than $250 million (Symantec, 1999).

The major impetus for computer viruses to exist other than as theoretical entities was the advent of individual (personal) computers, which provide a standardized, accessible, environment. In the 1990s, the widespread introduction of decentralized computer networks supplanted infected floppy disks as the main transmission medium. This opens up a fine distinction between viruses that exist within physical files in a computer, and more volatile viruses that propagate through networks without necessarily existing in files; these are usually called 'worms' or 'creepers'.

Macro viruses consist of sets of macros embedded in commonly used document formats (text, spreadsheets, presentation slides). The virus is thus incorporated in, and is spread via, the data rather than in executable code files. The 1997 NCSA survey mentioned earlier showed that macro viruses represented more than two-thirds of all virus attacks, with 25% of respondents reporting receipt of a virus in an email attachment (up from 9% in the previous year). A survey for the month of August 1999 implies that macro viruses have continued to increase in prevalence, and now account for 80% of incidents (*Virus Bulletin*, 1999).

A fundamental problem that has emerged with macro viruses is that of identifying which virus exactly is causing an infection (Bontchev, 1998). This is difficult because of the frequent presence of legitimate macros, and also because of the combinatorial aspect of sets of macros. A brief string matching identification is often ruled out. Bontchev explains that a virus disinfection product can damage users' data by removing legitimate macros or leaving fractions of the virus macro set *in situ* if the macro virus is not exactly identified. Ironically, virus disinfection products can then unwittingly synthesize new viruses by accidentally 'combining' macros from two or more different viruses. This is exacerbated by the design of some viral macros to copy ('snatch') and incorporate parts of other macros that they may find. Thus, polymorphism may be generated in hard to track forms, and fostered by anti-virus mechanisms rather than designed into the virus. The biological analogy here is that of recombinant DNA.

The regular introduction of new versions of popular applications such as Word has also created thorny problems, both technical and ethical, for the anti-virus industry in respect of macro viruses. Conversion of infected documents from earlier to the latest version also 'upcoverts' the macro virus, actually creating new viruses to be identified and guarded against (Bontchev, 1999).

With the ever greater interconnectedness of computers, some viruses such as the worms ExploreZip and PrettyPark, and the macro virus Melissa, have exploited automatic mailing mechanisms to replicate themselves across intra and internets (Ford, 1999). As interconnectivity increases, these network-aware infection mechanisms are likely to worsen in their frequency and extent.

2.1. THE EFFECTS OF DESTRUCTIVE COMPUTER VIRUSES

Different viruses will have different 'aims' and effects. The aims are consciously formulated by the virus 'designer'. However, as in other kinds of software construction, designs are not perfect, and the intended and actual effects may be disparate. Furthermore, unforseen circumstances arise in technically complex situations. These flaws

may lead to early detection of the virus, such as where, during the preliminary incubation period, the presence of a virus is revealed as its self-replication consumes storage space and other system resources. The same virus can have different effects on different kinds of computer systems. Sometimes the persistence of even comparatively innocuous viruses means that they disrupt computer systems simply because their incompatibility with newer versions of software (Alexander, 1997). The release of a computer virus is akin to opening a bag of feathers atop a tall building on a windy day. For example, the Scores virus was designed to sabotage programs at Electronic Data Systems (a large US company), but affected several US government agencies including NASA, the Environmental Protection Agency and the National Oceanic and Atmospheric Administration (Leiss, 1990). This is an illustration of Cohen's concept of 'generality'.

Viruses may be classified as destructive or non-destructive in their primary effect. The least destructive kinds of virus, such as the Freehand virus, simply print an innocuous message and then erase themselves. Sometimes the messages are insulting or obscene. Sometimes the messages are taunting in nature, and enumerate the damage being done to the computer as it happens. Destructive effects include halting a legitimate program. More destructive viruses erase or corrupt data or programs belonging to legitimate users of the computer. The virus may do this by (1) deleting files, (2) changing the contents of files, (3) gaining system previleges (for subsequent unauthorized access) or (4) damaging the computer hardware, as with the CIH virus which attempts to overwrite 'flash' memory holding the BIOS, necessitating replacement of the memory chip.

Secondary effects involve the progressive denial of system resources to computer users. This usually happens as the virus replicates and consumes system resources. This is what caused the severe disruption to computer systems across the world, including mainframes, in the internet worm attack of 2 November 1988, despite the fact that the virus did not delete or corrupt anything (Leiss, 1990). There follows a further period of disruption as infected computers are disinfected and immunized. Finally, even where a computer system can be made immune to virus attack, this can only be done at the expense of an extra effort. This effort incurs penalties of time, cost, and, usually, of making the computer system harder to use. In respect of the cost dimension it is worth noting that in 1997 one of the main anti-virus software suppliers reported a 63% increase in sales (and a doubling of profits) (Price, 1997).

2.2. THE CONSCIOUS MOTIVES BEHIND DESTRUCTIVE COMPUTER VIRUSES

We can identify several conscious, overt, aims behind the design and release of computer viruses:

- Non-specific malice.
- Revenge (commonly due to employee disgruntlement) (Cornwall, 1990).
- Ideological motives (political, freedom of information) (Clough & Mungo, 1992).
- Commercial sabotage (such as bankruptcy) (Mumford, 1998).
- Warfare (including espionage) (Dempsey, 1997; Taylor, 1997*b*).

Of course, we must recognize that some of these ostensible motives may be legitimations for unconscious processes. It is also true that conscious and unconscious motivations are difficult to separate.

3. The virus-maker and the hacker

The colloquialism 'hacker' denotes a person immersed in the details of building and modifying computer systems, often in an explanatory way (Cusumano & Selby, 1997). The term is often employed as a synonym for people who gain unauthorized access to computer systems, although in the USA the term 'cracker' is often employed for this more specific meaning. Whilst not all hackers become virus makers, it is fair to identify virus makers as a brand of hacker. Levy (1994) identifies a common constellation of values and behaviours as enshrining the 'hacker ethic':

- Obsession with hands-on use of computer technology—open access to all computers.
- Desire that all information should be in the public domain—dislike of secrecy.
- Mistrust of authority—espousal of decentralization, dislike of 'proper channels'.
- Judging others by pre-eminent criterion of hacking prowess, rather than by other norms.
- Belief in the creation of art and beauty using computer technology.
- Belief that using computers can change one's life for the better.

Levy traces the initial development of this movement from its origins at MIT (and a few other US universities) in the late 1950s, when computers were rare, the technology was new and fascinating, but access to computers was very restricted. The self-justifying (and self-glorifying) hacker ethic can be seen as a response to this environment. The initial motivation seemed to be to use and improve computer technology; self-aggrandisement followed on. By the early 1960s, this movement had become a nuisance to other computer users, and occasionally resulted in financial abuses, rather than merely being a question of curiosity and technical improvement. A strong desire to use other peoples' possessions has become apparent. Spying in various forms emerged as part of hacker practice. With a twist in circumstances this hacking approach can become openly malicious, rather than simply eccentric and disruptive under the guise of advancing technology.

Such people largely ignored the wider, political and social, consequences of what they were doing. The word of technology was cleaner than the complex, uncomfortable messy 'zoo' of humans and human relations. They had found an abstract, perfect domain for 'The benevolent exercise of power in the logical, unambiguous world of computers, where truth, openness and democracy existed in a form purer than one could find elsewhere … . The world in its purest form, where "the bit is there or it ain't there'" (Levy, 1994).

The 'hacker ethic' introduces a continuum of possible behaviour. At one extreme there is an intellectual curiosity and fascination with the technology. There is an impulse, as Levy identifies, to find world of beauty and purity. Moving along the continuum there may emerge an obsession to make all information free and accessible, for there to be no secrets possible within this beautiful world of technology, and for it all to be available to everyone. An anti-authority impulse begins to manifest itself in response to commercial or legal obstacles upheld by non-hackers, and Levy's original hackers next began to practice the aforementioned 'cracking' that is gaining unauthorized and forbidden access to information. This new obsession quickly gained a somewhat delinquent nature, and the hackers at one computer laboratory even went so far as to study locksmithing so that they could use, and misuse, other peoples' property that was officially denied to them behind locked doors and in locked desks.

It is a small step from here into unambiguously destructive and potentially criminal activity. The ugly and disturbing results of a contaminated web site have been displayed at Rootshell (1999). This activity is a long way from the 'beauty' and freedom that was originally claimed for the 'hacker ethic'.

It is a much smaller step from this point to destructive activities such as authoring and distributing computer viruses. These, as has been pointed out earlier, almost always have damaging consequences even when the virus author did not consciously recognize that to be likely. A disregard, and even a contempt, for other computer users is at least implicit here, and is often explicitly expressed, as we shall see in Section Four of this paper.

The notion of the computer hacker made familiar in the media is of an evil genius, usually male, usually acting alone, and employing fiendish cunning at the computer terminal to outwit a faceless bureaucracy or establishment. The virus maker has been compared to the media stereotype of the hacker: isolated, male, socially inept, possessing technical expertise, and a desire to display superior control of technology. The stereotypes of the hacker and the virus-maker may carry some truth but do not tell the whole story. Some virus-makers have been arrested who do not fit these descriptions. Morris (Fites, Johnston & Kratz, 1992), for example, was a postgraduate student at Cornell who claimed he was carrying out research when he introduced a destructive program onto the Internet. The divide between legitimate and illegitimate experimentation has not always been delineated clearly. However, the attraction of the intellectual challenge is clear in either case.

Levy writes that 'there never was a star quality female hacker', and the males mostly existed in 'bachelor mode'. By the time this movement had spread (along with the spread of computer technology) to California in the mid-1970s, Levy records that a female computer programmer 'noted the lack of female hardware hackers, and was enraged at the male hacker obsession with technological play and power. She summed up her feelings with the epithet 'the boys and their toys', and … worried that the love affair with technology might blindly lead to abuse of that technology'. Levy also notes that a well-known computer innovator (Ted Nelson) described the same group of hackers as 'chip-monks, people obsessed with chips. It was like going to a meeting of people who love hammers'.

The virus-maker has also been compared to any other vandal (see, for example, Fites, Johnston & Kratz, 1992). Some have also suggested that there is a direct addiction involved (Hruska, 1992) analogous to drug addiction. The case of the legendary hacker Kevin Mitnick, whom the authorities suspected might unleash a plague of viruses from within the prison where his activities had landed him, is relevant here. Mitnick himself felt that he had become addicted, and was sentenced to attend an anti-addiction treatment programme following his imprisonment (Sweeney, 1994). The addiction may be more like a kind of harassment akin to sending poison pen letters than the immediacy of substance abuse, since as we noted in Section 2, the virus marker exercises a kind of perverse destructive power at some remove in terms of both time and geography. There may also be a kind of technological voyeurism (see Hoffman, 1990) in situations when the virus-maker leaves a calling card so that the computer user knows he or she has been infiltrated by stealth, as with the Freehand virus.

It is, of course, difficult to gain direct access to the authors and distributors of computer viruses. Public pronouncements from this quarter are mostly hidden behind

anonymity or at least *noms de guerre*, and identity of any party is difficult to determine. However, on the available evidence it appears that some aspects of the stereotypes hold. The public perception is that the virus maker is male, young, and working alone. With the proliferation both of bulletin boards and of tool kits for virus makers and distributors, the last characteristic is questionable. It seems unlikely that the 14-year-old Venezuelan boy, the alleged author of the CAP. A macro virus, did not gain at least inspiration from international links. But most importantly, we found no evidence whatever of female virus authors. The hacker group 'Cult of Dead Cow' claims only one female member, though the 'white hat hacker' Carolyn Meinel is well known (Meinel, 1998). Gordon, in her contacts with the virus-making culture, only came across the 'girlfriend of a virus writer', and a female member of the virus writing group NuKE, 'However, it is uncertain as to whether or not she ever produced any viruses', and Gordon concludes that there is a 'marked absence' of female virus writers (Gordon, 1994).

The overwhelming impression gained from the spectrum of computer misuse, from 'cracking' onwards to virus making, is of adolescent or young adult, male activity. This is evident in the scatological, frequently obscene language and imagery deployed. The rebellious, anti-authoritarian tone of the Cult of Dead Cow pronouncements, spoofing 'official' pronouncements, peppered with sexual puns, and with web links to pornography expresses the ethos.

The authors of the best-known viruses, when apprehended, have turned out to be young males. David Smith, arrested by the FBI for allegedly creating the Melissa macro virus, typifies this phenomenon: the virus is supposedly named after a stripper that the accused admired. Meinel's scenario (1998) illustrates the ubiquity of pornography in computer misuse. In the course of their investigations into this world the authors of the present work became the recipients of obscene email messages, apparently generated automatically by daemon planted at a hacked web site. The content of these messages made it clear that their author was male. Writing on the highly peripheral involvement of women in this culture, Gordon (1994) writes that 'Females … are typically treated as inferior by a disproportionate number of members of the culture. Sexual slurs and harassment are common'. Preliminary investigations suggest that, in the information technology context, there could be a gender difference in moral development, and this may have some bearing on the seemingly uniquely male activities of virus-making and distribution (Bissett & Shipton, 1999).

Interviews with virus-makers are few and far-between. John Sweeney interviewed the former wife and friends of Kevin Mitnick who denied that Mitnick was the unsocial, nerdish character of the media stories (Sweeney, 1994; Flower, 1995). A telephone encounter with Mitnick also contradicted this image. 'Frank Drake', editor of WORM magazine, was interviewed by Dorothy Denning (Denning, 1990), and proved to be a lively and socially skilled interlocutor. 'Dark Avenger', who is alleged to have originated 20 or more viruses (Clough & Mungo, 1992) was interviewed by Sarah Gordon (Kane, 1994), and revealed a quite different personality. In the next section, we make several points about some possible motivations, based on the interview with 'Dark Avenger' in particular.

How the activity is understood is affected by the discourse within which it is discussed: linked to hackers it may be seen as an immature prank and not to be condemned too severely. Linked to former employees it may be seen as a vengeful attack by a mature

(presumably previously 'normal') worker and deserving of severe punishment. Linked to 'cyberpunks' it may be seen as libertarian activitism on behalf of freedom of information and against the power of the conglomerate and the corporate state, and also meriting stringent punishment from the state, or underground support from like-minded hackers (Manion & Goodrum, 1999). Another group which causes concern is the 'cyber-terrorist': Eastern European computer experts who once were expert dissidents in the Soviet Bloc and now subvert the technology of the West to which they can only gain remote access (*New Scientist*, 1992).

4. Destructive processes in the virus-maker's unconscious motivations

The impetus for this paper came from the experience of one of the authors who was accused by a colleague of 'infecting' his computer with a virus from a floppy disc that she had given him. She thought this was extremely unlikely and, panic-stricken, checked her computer and other floppy discs for viruses. She reassured him that to the best of her knowledge the disc was clean but she was horrified to be told she had probably imported the virus through email and it must be now attacking all her files. The rest of the saga need not be recounted here but the psychological impact is relevant because it demonstrates the anxiety and disruption made possible by the threat of virus infection. This threat, in particular, disrupts the working relationship between the computer user and the computer.

In psychoanalysis, there is a concept of 'holding' (which is an aspect of the working relationship between analyst and patient) and refers to the analyst's capacity to empathize with the patient and to 'hold' his or her anxieties and vulnerability in mind while the patient feels supported and gets on with his or her therapy work. This concept of holding comes from a psychoanalytic understanding of how psychological well-being depends on an early experience of a mother being able to be a good container for the infant's vulnerable self. A good enough mother is able to support the infant metaphorically and literally, just as she once held the baby inside her own body, until the infant develops a competent self. In the isolation and struggle involved in academic writing, or any other major task for which we use a computer, we may expect some of this holding capacity from our computers (a point originally made by Turkle, 1995). The author was writing a book at the time, and all her work had been done on this computer. As a matter of fact, there was no virus transmitted from her to her colleague, though his computer had indeed been infected, but by his girlfriend! However, the very idea of her computer now being host to a process which would destroy work was enough to create enormous anxiety, not to mention wastage of time, as up to date protection against more recent viruses needed to be installed. A corollary to the psychological effect of this experience was a realization that not being able to understand how a virus could be transmitted demolished confidence hitherto felt in relation to the enjoyment of the benefits of technology without an understanding of the underlying structure of the computer or the software. A realistic grasp of what a virus maker was likely to be able to achieve was momentarily replaced by an atmosphere of magic, where the exercise of calm reason seemed threatened. This experience prompted the authors to consider why someone should wish to make such an artifact, which could be so destructive, for no personal gain whatsoever, and to consider the meaning of the threat involved.

The motivations of the virus makers are clearly diverse and it is impossible to generalize because of the following:

1. There is no easily identifiable 'clinical' population to research as yet.
2. There is no psychoanalytic or psychological literature about virus-makers.
3. Conscious motivations vary as has already been outlined.
4. Very little material has been published containing direct interviews with virus-makers which can be analysed in a more psychobiographical fashion (a dubious activity anyway, since the object of analysis would have no opportunity to respond to hypotheses that an analyst might put in the form of interpretations).

Nevertheless, we can speculate about such matters based on the interviews at hand and on what is written about virus-makers, though bearing in mind that much of it is hearsay. We have no interest in attempting a spurious 'profile' of a virus-maker, but do want to consider some processes involved. This paper is, therefore, a preliminary investigation into understanding the impulses behind virus-making, and highlighting the need for further research and discussion. We do hope, however, to lay the foundations for a framework by introducing the discussion of motivations in virus-making.

Understanding the motivation of virus-makers needs to go beyond the stereotyping that the media tend to adopt in describing categories of criminal behaviour.

Christopher Pile, who had only had three short-term jobs since leaving school, when he was arrested for computer misuse, created an encryption engine which enabled the viruses to hide in different forms as they spread from computer to computer. Pile is credited with saying that he wrote viruses to increase his self-esteem and because he was disappointed there was no effective UK-produced virus in circulation (Mason, 1995). His counsel told the court at his hearing that he was a 'sad recluse' and 'a mad boffin' (Gibbs, 1995). Media reportage about virus-makers may be biased towards such simple stereotypes which can be understood in sound-bites. It serves only the interests of anti-virus product makers to promote a siege mentality, and to turn virus makers into folk-devils.

4.1. SARAH GORDON'S INTERVIEW WITH 'DARK AVENGER'

However, Sarah Gordon interviewed the Bulgarian virus-maker, 'Dark Avenger' via email for Virus News International (see Kane, 1994) and presented a more subtle picture. The most impressive aspect of the interview is Gordon's tenacity in trying to understand a confident man who denies any malicious intent and whose responses are in marked contrast to her own considered ones. She draws his attention to the possibility that his virus could have caused deaths but he avoids taking responsibility by arguing that his virus was so bad he imagined it would not even get 'out of town'. As he puts it: 'It all depends on human stupidity, you know. Its not the computer's fault that viruses spread', He combines denial of responsibility with a surprising identification with the computer, as if it represented him anthropomorphically. Gordon asks him why he wrote his first virus and whether he had any regrets. 'Dark Avenger' responds: 'I wrote it because I had heard about viruses and wanted to know more about them but nobody could tell me anything. So I decided to write my own one. I put some code inside it that intentionally destroys data and I am sorry for doing it'. His reaction to the question sounds bland and the apology hollow. We do, however, begin to detect what Klein would call an inner

phantasy, that others knew something which he felt shut out from knowing and he blames those who wouldn't 'let him in'.

Gordon wonders why he did not ask someone to show him a virus but he disregards this by saying he did not know anyone in Bulgaria who had one. His ingenuity in making a virus seems to be in inverse proportion to his resourcefulness to making use of human networks. 'Dark Avenger's identification with his virus is again indicated when he goes on: 'The American government can stop me from going to the US but they can't stop my virus. Ha ha ha ha ha ha ha ha'. This last comment underlines the extent of his sense of omnipotence, as if he can break through the restrictions of geography and limited technical resources. This is like being able to put himself in a virus in a concrete way, associated with a process called projective identification. It is as if he can secretly get into everything he wishes to possess and then control what happens from within it. However, his mind does not use such an idea for constructive purposes as is shown when he replies, in response to Gordon's query about why the code had to be destructive: 'Didn't know what else to put in.' He describes wanting to make people react by trying to get rid of the virus and justifies this by saying 'I didn't think that any data in PCs chould have great value'. Thus, he rationalizes to himself that it is acceptable to destroy other peoples' peace of mind and devalues any material they may have on PC. There is therefore no guilt to be attached to his activity.

This attitude to destroying something, not because it is bad, or a threat to oneself in some way, but simply because it is whole and satisfactory to someone else's mind (despite the attempted devaluation of it) is how Klein conceives of envy. Such a feeling is aroused in us, Klein says, at an early age when we are faced with having so little in comparison with those who look after us. With enough good parenting we learn to come to terms with what we do not have, and can get on with trying to enjoy what we and others do have, although we will always be prone to envious responses in the face of plenitude. Klein suggests that this attitude can even operate within the individual mind, so that one part of ourselves envies another (like when we sabotage ourselves just as things are going well). 'Dark Avenger's' envy is very close to the surface when he comments: 'So I just hated it when some asshole had a new, powerful 16 MHz 286 and didn't use it for nothing, while I had to program on a 4.77 MHz with no hard drive …'.

We can only speculate here but he may have felt even worse if the 'asshole' also did good work with his machine. He certainly expresses no regret when he proceeds to say: 'Ideas are not responsible for people who believe in them'. His identification is with the viruses: 'I couldn't care less for all the suckers that would see/use them'. There is no identification with other virus-makers, either. He sees them as inferior: 'not good programmers'.

The skills and interests of the virus-maker could be put to good use if it were not for envy. The virus-maker interviewed here cannot enjoy his ability in a constructive way: he spoils what he can do by wasting it on envious attacks on unseen others. Similarly, in Christopher Pile's case the ability to work to produce such artifacts, albeit illegal ones, shows clearly that a good mind had been put to a destructive use: Pile's own creativity was wasted. In her interview with 'Dark Avenger' Gordon, unflappably sensible in the face of such superiority and lack of concern for others, asks him if he has ever thought of making anti-virus products. He prefers not to, at first on the basis that they are simply a device to take money from people and then he follows through with an attack on the

victims of viruses: 'Viruses would spread much less if the "innocent" user did not steal software and if they worked a bit more at their workplace, instead of playing games'. The apostrophes around innocents remind us of the common defence of the sex-offender: 'she knew what she was doing—she was asking for it'. The Farooq brothers made a same-category comment about their virus, arguing that purchasers of software should have bought the products in which viruses had been implanted in their own country at their own prices rather than at the cost in Pakistan (see Hoffman, 1990). 'Dark Avenger' goes further, and accuses victims of causing more damage than the viruses by panicking. He explicitly does not recognize writing viruses as a crime.

4.2. BENEFITS OF UNDERSTANDING UNCONSCIOUS PROCESSES IN VIRUS MAKING

The virus maker may find his activities useful in coping with a range of unresolved issues such as: competition and rivalry; inability to sustain intimate attachments; the desire to control and disturb other people; envy. More research is needed in this area. Perhaps a key difference between a virus-maker and other kinds of hacker is the extent to which the individual is prey to envy and capable of withstanding the urge to act on it. Levy's last two points about the hacker ethic involving the creation of art and beauty, and valorizing the computer's potentials to make life better for people, would certainly not fit the virus-maker. The destructive aspect makes it difficult to engage in discursive interchanges with virus-makers themselves, although Sarah Gordon has shown that it is not impossible (Gordon, 1994).

This paper has also noted the relationship of virus-making to gender. Woman is the *ur* example of the good holding environment personified. Women are just as envious as men but it may be possible that because of the restricted way women use public space (see Young, 1980) they are more inclined than men to make envious attacks on their own bodies as holding environments (see Welldon, 1988). Men, on the other hand, may be more inclined to attack the capacity to hold and contain in others, through activities like virus-making. The envy of others cannot be prevented, but perhaps in understanding the relationship between users and their computers we can recognize that a special link is created which feels devastating when disrupted, and prepare others to deal with the psychological dimension on training courses.

We can protect, on a practical level, employees' impulse to play and to bring in pirated software for this purpose. This can be recognized as opening the door to virus-makers, though without attaching blame to victims. Bennee has suggested (Dempsey, 1994) that 'viruses are totally defeatable, purely by procedures. One of the best devices at your disposal is terms-and-conditions of employment'. If playing games in catered for legally and safely by the company then staff would not need to bring in their own games. Disciplinary action would deter staff from using anything other than a dedicated standalone machine for this purpose. However, beyond such measures we are left with a difficult scenario. As knowledge about viruses develops then so will anti-viruses proliferate; indeed, this is already a huge industry. This factor, plus the inclination of hardware and software manufacturers to place the onus for virus detection, disinfection and prevention onto the users of computers militates against more radical solutions such as Thimbleby's (1994).

Gordon (1995) and Forcht (1994) both suggest that education about the ethics and consequences of information technology would help curtail activities such as virus-making and distribution. Gordon tellingly makes a comparison with public campaigns against drunken driving in the USA; she claims that it is no longer thought 'cool' to drink alcohol and drive, and proposes that education may do the same for the status of virus-making.

Such initiatives are worth investigating, for, as is clear from Section 1, computer viruses are continually increasing in number and scope. There is also a pressing need to develop the present approach in order to inform such possible initiatives. In the next section we outline areas for further work.

5. Future investigation

Probably, the major problem for investigating unconscious motives in virus-making and distribution is the difficulty in reaching the people responsible for these activities. Access is difficult, and material from case studies is sparse. We propose that ongoing monitoring of Internet resources for virus originators, such as bulletin boards and discussion forums, should provide information for further analysis of unconscious motivation. However, what is needed most are some in-depth case studies.

It may be possible to enter into dialogue with virus-makers, but their privacy and anonymity would be jeopardized. Without face to face meeting, one would not really know with whom one is communicating: a man, a woman, or a group, and it would be difficult to establish veracity. However, legitimate sources which monitor virus activity could be used to contrast and check accounts, and infer some indisputable technical details of virus patterns which could be used to corroborate the stories of virus-makers.

It would also be useful to investigate the impact of viruses upon computer users, in particular, whether there is a gender difference in user reaction to virus infection. Fear of virus infection, and the attendant hoaxes and rumours, can cause as much disruption as actual virus outbreaks (Gordon, Ford & Wells 1997).

There is an urgent need to investigate how the Internet is changing the pattern of virus creation and dissemination. In particular, we should monitor the relationship between the production of anti-virus products and the production of viruses. Where anti-virus strategies have been launched, both within organizations (where machines are set aside for games or other imported software) and within society at large (via education as suggested by Gordon and Forcht above), it is important to study their success or otherwise. It may be possible to use an understanding of both conscious and unconscious motivations to inform and guide these strategies.

6. Conclusions

We conclude that virus creation means different things for different perpetrators, but that generally it is a destructive act aimed at dismantling what is apparently 'whole' and satisfactory to others, and that it enviously disrupts the holding relationship between a computer user and the computer. This reflects the reality that we have to deal with destructiveness as well as creativity in ourselves and other people and the consequences of mass access to technological modes of operationalizing our plans. Paradoxically, in

developing anti-virus measures, the constructed world becomes more fortified against each new virus, but freedom of information is then likely to be more curtailed, thus generally increasing the sense of alienation and, disenfranchizement that has exercised hackers in particular. Moreover, such practical defense measures will not alter the virus-makers' envy and sense of being excluded, and it may intensify their attacks and encourage a siege mentality in computer users which can be exploited by anti-virus product makers.

The authors would like to thank Professor Harold Thimbleby for his helpful suggestions, and also the two anonymous referees for their informative and constructive critique of an earlier draft of this work.

References

ALEXANDER, S. (1997). Viruses. *Computerworld*, 2 June, **31,** 88.
BERG, A. (1997). More infections than ever. *LAN Times*, 23 June, **14,** 35.
BISSETT, A. & SHIPTON, G. (1999). An investigation into gender differences in the ethical attitudes of IT professionals. In A. D'ATRI, A. MARTURANO, S. ROGERSON & T. WARD BYNUM, Eds. *Proceedings ETHICOMP* 99. LUISS Guido Carli, Rome.
BONTCHEV, V. (1998). Macro virus identification problems. *Computers and Security* **17,** 69–89.
BONTCHEV, V. (1999). The problems of WordMacro virus upconversion. *Computers and Security* **18,** 241–255.
CLOUGH, B. & MUNGO, P. (1992). *Approaching Zero*: *Data Crime and the Computer Underworld*. London: Faber and Faber.
COHEN, F. B. (1994). *A Short Course on Computer Viruses* (2nd edn). New York: Wiley.
CORNWALL, H. (1990). *Data Theft*: *Computer Fraud*, *Industrial Espionage and Information Crime*. London: Mandarin.
CUSUMANO, M. A. & SELBY, R. W. (1997). How Microsoft builds software. *Communications of the ACM*, **40,** 53–61.
DEMPSEY, M. (1997). Computer security. *Financial Times*, 2 April.
DENNING, P. J. Ed. (1990). *Computers Under Attack*. New York: ACM Press.
FITES, P., JOHNSTON, P. & KRATZ, M. (1992). *The Computer Virus Crisis* (2nd edn). New York: Van Nostrand Reinhold.
FLOWER, J. (1995). Catching Kevin and his friends. *New Scientist*, 2nd September, **147,** 32.
FORCHT, K. A. (1994). *Computer Security Management*. Danvers MA. Boyd & Fraser Publishing Co.
FORD, R. (1999). No surprises in Melissa land. *Computers and Security*, **18,** 300–302.
GORDON, S. (1994). The generic virus writer. *Proceedings of the 4th International Virus Bulletin Conference*. Jersey, UK. [http://www.av.ibm.com/Publish/Scientificpapers/Gordon/].
GORDON, S. (1995). Technologically enabled crime: shifting paradigms for the year 2000. *Computers and Security*, **14,** 391–402.
GORDON, S., FORD, R. & WELLS, J. (1997). Hoaxes and hypes. *Proceedings of the 7th International Virus Bulletin Conference*. San Francisco, USA. [http://www.av.ibm.com/Publish/Scientificpapers/Gordon/HH.html].
GIBBS, G. (1995). Black Baron's computer virus plague. *The Guardian*, 16 November 1995, Home 2.
HOFFMAN, L. J. (1990). *Rogue Programs*: *Viruses*, *Worms and Trojan Horses*. New York: Van Nostrand Reinhold.
HRUSKA, J. (1992). *Computer Viruses and Anti-virus Warfare* (2nd edn). London: Ellis Horwood.
HRUSKA, J. (1998). The future of computer viruses. [http://www.sophos.com/virusinfo/whitepapers/futirevi.html].
KANE, P. (1994). *The PC Security and Virus Protection Handbook*. New York: M&T Books.
KEHOE, L. (1996). Technology: infectious behaviour. *Financial Times*, 7 May.

KEPHART, J. O., SORKIN, G. B., CHESS, D. M. & WHITE, S. R. (1997). Fighting computer viruses. *Scientific American*, **277,** 56–61.
KEPHART, J. O. & WHITE, S. R. (1994). Measuring and modelling computer virus prevalence. *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 2–14. Oakland, California, May 24–25, 1993.
KLEIN, M. (1946). Notes on some schizoid mechanisms. *International Journal of Psycho-Analysis*, **27,** 99–110.
LEISS, E. L. (1990). *Software Under Siege*. Oxford: Elsevier Advanced Technology.
LEVY, S. (1994). *Hackers*: *Heros of the Computer Revolution*. London: Penguin Books.
MANION, M. & GOODRUM, A. (1999). Terrorism and civil disobedience: towards an international ethic of hacktivism. In A. D'ATRI, A. MARTURANO, S. ROGERSON & T. WARD BYNUM, Eds. *Proceedings ETHICOMP 99*. LUISS Guido Carli, Rome.
MASON, J. (1995). Computer virus 'baron' is jailed for 18 months. *Financial Times*, 16 November.
MECKBACH, G. (1997). Viruses growing out of control. *Computing Canada*, 21 July **23,** 1–2.
MEINEL, C. P. (1998). How hackers break in … and how they are caught. *Scientific American*, **279,** 98–105.
MUMFORD, E. (1998). *Cybercrime Seminar*, Sheffield Hallam University, 15 January.
NEW SCIENTIST (1992). Feedback. *New Scientist*, 21 March, **133,** 54.
PRICE, C. (1997). Dr. Solomon's doubles to £3 m. *Financial Times*, 10 April.
ROOTSHELL (1999). [http://www.rootshell.com].
SWEENEY, J. (1994). To catch a hacker. *The Observer*, 4 September, Life 14.
SYMANTEC (1999) [http://www.symantec.com/avcenter/venc/data/cih.html].
TAYLOR, P. (1997*a*). Businesses warned over email. *Financial Times*, 19 April.
TAYLOR, P. (1997*b*). Cyber terrorism. *Financial Times*, 2 April.
THIMBLEBY, H. (1990). Turning viruses to good use. *New Scientist* **126,** 23 June.
THIMBLEBY, H. (1994). An organisational solution to piracy and viruses. *Journal of Systems and Software* **25,** 207–215.
THIMBLEBY, H., ANDERSON, S. & CAIRNS, P. (1998). A framework for modelling trojans and computer virus infection. *Computer Journal* **41,** 444–458.
TURKLE, S. (1995). *Life on the Screen*. New York: Simon & Schuster.
WELDON, E. V. (1988). *Mother*, *Madonna*, *Whore*. New York: Guilford Press.
VIRUS BULLETIN (1999). [http://www.virusbtn.com/Prevalence/199908.html].
YOUNG, I. M. (1980). Throwing like a girl: a phenomenology of feminine body comportment, motility and spatiality. *Human Studies*, **3,** 137–156.

Paper accepted for publication by Associate Editor, Prof. H. Thimbleby