International Journal of Law and Information Technology, Vol. 11 No. 2

A Critical Look at the Regulation of Computer Viruses

MATHIAS KLANG[1]

Abstract

There is a witch-hunt taking place today. Without a deep understanding of the phenomena of computer viruses legislators are attempting, both nationally and internationally, to prohibit what they do not understand. The computer virus is both misunderstood as a concept and abused as a term. Despite this the rallying cry is that all viruses are evil and must be destroyed in the same way as witches were seen as evil in the middle ages. The uncritical criminalisation of computer viruses does not lead to a better society nor does it cure all the ills for which viruses are blamed. This paper is not a defence for viruses but it does explore the alternative uses of computer viruses of which a legislator should be aware and take into consideration when in the processes of defining the legal status of computer code.

1 Introduction

There is a need to clarify something from the outset. This author does not condone nor advocate the production or spread of malicious or harmful software.

Having said that this paper is an attempt to look at the computer virus

[1] University of Göteborg Box 620, 405 30 Göteborg, Sweden. klang@informatik.gu.se.

This paper was written as part of the Safe Street Project http://www.safestreet.nu/ at the Viktoria Institute http://www.viktoria.se in Göteborg and with the financial support of Vinnova http://www.vinnova.se. It is included in a larger study on the security of technology and public safety.

and at some present and future attempts to legislate the phenomena. The questions posed by this paper are whether the virus requires legislation and if so what form should the legislation take and which are the values which require legal protection.

2 What is a Virus?

While the first use of the term virus to refer to unwanted computer code appeared in the 1970's and the first better definition in the early 1980's the term computer virus continues to be inexact. While the term does have a certain amount of precision in the computer science field this precision is based upon a loose consensus as opposed to exact definition. For the computer scientist this loose consensus is satisfactory but for the law the lack of definition is a major problem in the creation of fair and balanced legislation.

The first problem occurs with the actual term virus. It was chosen to represent three characteristics: first the fact that the code self-replicates, second that it is unwanted and third that it is ominous. This is fine for most cases but not all programs which are seen under the law as viruses self-replicate.[2] The attempts to define the term have not all been too successful. The first formal attempts were made in Fred Cohen's (1985) doctoral dissertation and included all types of computer code with the ability to self-replicate. This definition will therefore include many non-harmful or even useful or beneficial programs.

The term has also captured the interest of the media. The media have used the term carelessly and wrongly in defining almost any occurrence of computer software failure or the loss of data due to anything from carelessly written program code to user error.

The problem faced by the law is to be able to define which behaviour it wants to criminalize and to do so preventing rightful or legitimate behaviour.[3] To be able to do this the definition the law chooses to use must take into consideration alternative factors such as the occurrence of benign viruses, the need for virus research, the role of the recipient of a virus and the role of social engineering etc.

Using the metaphor virus to describe malicious computer code (malware) is not a well-chosen one. Based on the Latin word for poison and equated in everyday speech with something that should be avoided the legislator often forgets that the virus in itself is not necessarily bad.

Before continuing a working definition of the computer virus must be given. While definitions have been debated and argued upon a working

[2] Worms and sometimes even Trojans and Logic bombs are seen as viruses under the law.

[3] Despite the fact that states have the power and legitimacy to legislate, legislation should only be enacted to further a legitimate cause.

definition for the purpose of this paper is necessary. I will use the definition quoted by Brontchev (1996) 'We define a computer "virus" as a self-reproducing program that can "infect" other programs by modifying them or their environment such that a call to an "infected" programs implies a call to a possibly evolved, and in most cases, functionally similar copy of the "virus".'

One must remember that even those who are staunchly against viruses agree that viruses can cause greater or lesser harm. Theoretically viruses can be described as being destructive or benign. If benign they cause no damage, some may not be noticed by the user at all or they may, for example, display a message on the screen or play a sound. If the virus is destructive it is able to cause serious damage to the computer system anything from taking disk or memory space, occupying the central processing unit and introducing the risk of incompatibilities and conflicts.

Phenomena which are often confused with the virus are Worms or Trojans. While these are not viruses they tend to be referred to as viruses by the media or the uniformed. This causes additional complexity when discussing the legal status of computer viruses. The worm is a program that can run independently and travel through networks from one computer to another. The worm is also capable of having different segments of itself on different machines acting in harmony with each other. Worms traditionally do not alter other computer programs but they can be used to carry other viruses which have the ability to affect other programs. The fact that the worm replicates have led many to class them as viruses since they fall naturally into Cohen's formal virus definition. This paper will include worms in the definition of viruses even though they are technically not viruses. This is necessary since the legislation is often enacted without any particular concern for the correct terminology.

This paper will focus on the legal concept of computer virus. The next section will be a brief history and explanation of traditional viruses. Which is then followed by an explanation of the possible crimes involved. This is followed by some current legislative approaches to the computer virus exemplified by the legislation England, the United States and Sweden. Then follows a view of what the future has in store for virus legislation by way of the convention on cyber crime. This is followed by an alternative look at the computer virus and the paper is concluded by a discussion section.

2.1 *Evolution of Viruses*[4]

There are two ways of defining the history and evolution of computer

[4] For more details on this subject see, for example, F.B. Cohen – A short course on computer viruses (1994); D. Harley, U.E. Gattiker & R. Slade – Viruses revealed (2001); R. Skardhamar – Virus: Detection and Elimination (1996).

viruses, first by looking at the technical development of the virus and second by taking a strictly chronological view of viruses. Since this paper is concerned with the regulation of the computer virus the presentation here will be based upon the technical development of the computer virus, explaining briefly what each stage of development entails and when suitable presenting historical data.

The presentation here is a simplification. Many viruses are hybrid of several stages of virus evolution. The purpose of this section is to give the reader a general understanding of what the computer virus is and what it can do.

2.1.1 *What is infected?*

In keeping with the metaphor of malicious software as virus, the virus can be seen as having a life cycle of stages in which it progresses. The dormant phase is when the virus is idle awaiting activation by a specific event such as a date or the presence of a program or file. The propagation stage is when the virus replicates itself and makes an identical copy of itself into other programs or onto system areas on the disk. Each copy is able to propagate and therefore recreate itself. The next stage is known as the triggering stage, this is when the virus is activated and this moves it to the execution stage where the actual event occurs. This could be anything from the destruction of data to a more benign message on the screen.

Viruses may also be defined via this last stage. From the execution stage viruses can be inserted into four different categories: the file infectors, system or boot infector, multi-partite infector and the macro infector.

The file infectors most commonly attaches itself to program files but are generally able to infect any file containing executable code (for example script or configuration files) the virus is activated once the file is executed. System or boot-record infectors do not necessarily infect a file but tend to target the portion of the hard drive used for system processes, including the boot-record (the section responsible for booting the operating system). On diskettes the viruses can attach themselves to the Master Boot Record and replicate themselves onto any media in which the disk is inserted. Multi-partite viruses infect boot records as well as files. This hybrid virus therefore manages to create more damage than either of the two mentioned above. It is also therefore more contagious than the previously mentioned viruses. The Macro viruses infect macro enabled documents.[5] When such a document is opened, the document executes its macro commands automatically. Sometimes the virus is such that the execution does not occur unless accidentally triggered by the user.

Another commonly used method in virus description and definition is by observing the historical evolution of the virus. This is not the historical

[5] A macro is a set of executable commands designed to run in place of a repetitive task.

evolution of a single virus but rather the development of virus code. The evolution of viruses has been sub-divided into five different eras, known as generations. These generations do not necessarily represent a historical overview since first generation viruses are still created today. The generations represent the development of virus creation techniques. Often the later generations include techniques from the earlier generations.

The first generations, sometimes known as simple viruses were not especially impressive. Their main ability, sometimes only ability was their ability to propagate. While the effects could be serious, such as the case of boot sector viruses which would cause a long chain of linked sectors. In program infecting viruses the viruses tended to keep re-infecting the infected program. The viruses do nothing to disguise or hide their presence. This open re-infection increases the size of the infected programs which facilitates detection by either noting an increase in size or the repletion of a section of code.

The second-generation viruses were able to remedy the flaw in early virus manufacture, this was done by making the virus aware of itself. Since the first generations continuous growth facilitated detection and therefore destruction the second generation would only infect previously uninfected files. This is usually done by the virus, creating a special signature during the first infection. The virus then searches any file for the signature prior to propagation. If the signature is present propagation does not take place.

The third-generation of viruses is sometime known as the stealth virus. They are called stealth since they differed from earlier stages of virus evolution by the ability to disguise themselves. Scanning the secondary storage and searching for a pattern of data unique to each virus could discover earlier generations of viruses. Virus writers counteracted this by employing stealth techniques. These viruses subvert selected system service call interrupts when they are active. For example attempts to perform scans where intercepted by the virus and the scan returned therefore returned the false answer that the disks were uninfected.

The armoured viruses heralded the fourth generation of viruses. This strain was designed to evade the anti-virus software by confusing it. Methods which were used could be the adding of unnecessary code to make detection, identification and destruction more difficult. Some fourth generation viruses used the concept of attack being a form of defence and have the ability to directly attack the anti-virus software.

The latest generation of viruses, the fifth, encrypted or polymorphic viruses are again attempting to disguise their existence by mutating. The virus infects the target, not with an identical copy of itself but with a mutation. The mutation takes the form of a modified or encrypted version of itself. The virus is able to modify the code sequences it uses to infect the target or encrypting the infecting virus with random encryption keys. This shape shifting makes the virus difficult to detect by simple byte matching and identification therefore requires the employment of more sophisti-

cated algorithms which must be able to decrypt the virus to detect the presence of the infector.

3 Legislative Approaches

The legislative approaches to computer viruses tend to follow the general arguments found in the relatively uninformed media debates. Those who would speak in favour of computer viruses are considered to be naïve or misguided since they do not comprehend the damage malicious viruses cause and since malicious viruses cause damage to property they are inherently bad and must be prohibited. Those who argue against the computer virus are often seen as being either anti-virus corporations attempting to create scares or law enforcement officials who have no appreciation of either the rights and necessities involved in the use of computer viruses.

Spanning the possible width of legislative approaches is the liberal laissez-faire combined with the free expression arguments to the restrictive approach of full criminalisation. The free expressionists tend to attempt to argue that the law cannot limit their expression via viruses. The laissez-faire approach seems often to be seen as a lack of action or it can take the position of 'wait and see'.

The arguments for full criminalisation are based upon the concept of the virus as an indisputable evil and as such has no place in society. Kellman (1997) equates virus writers to murders and terrorists.

> 'As a staunch defender of Free Speech and the rights of young people to experiment with their lives in recent months I have had to face up to some unpalatable facts – virus writing is evil and cannot be justified in any circumstances. It follows that prosecution of virus writers is something which should be universally accepted as appropriate action. Virus writing needs to be recognised as a criminal act by international conventions and virus writers should always be subject to extradition. Just like murderers and terrorists, virus writers should find no escape across national boundaries. And the investigation of computer viruses needs to be a regulated activity with failure to apply for regulation being a criminal offence.'[6]

Kellman therefore advocates the addition of the computer virus writer to the list of criminals which, under international law, are to be seen as terrorists or war criminals they are to be offered no harbour or defence for their actions. This approach is frightening since it is all to simple to point to

[6] Kelman, A. (1997) The Regulation of Virus Research and the prosecution for unlawful research?', Commentary, 1997 (3) *The Journal of Information, Law and Technology* (JILT). http://elj.warwick.ac.uk/jilt/compcrim/97–3kelm/.

other actions or uses of technology which have caused more pain, suffering or human and property damage without achieving any of the status argued for here.

While both these extremes are positions which should be avoided the latter position is more worrying since it does not attempt to define what it is that actually makes a virus writer a terrorist. Without an adequate definition anyone who writes or modifies computer code can fall into this category.

3.1 *What is the crime?*

One question in looking at what should be protected and what should be criminalised in connection to computer viruses is the question of which effects the virus has. There are basically seven different basic criminal acts which could be of special interest in connection to viruses. The first is the actual writing of the code which could be seen as a preparation to commit a crime, second is unauthorized access which occurs when the virus enters into a new computer without the authority of the legitimate user. Third is the question of unauthorized modification which could be the infection of a file, boot sector, or partition sector. Fourth, is loss of data, the effects of the virus may be that the data is no longer accessible by the legitimate user. Fifth may be the endangerment of public safety due to the failure or reduction of efficiency of the computers. Sixth, the making virus code available to others may be seen as incitement. This includes making available viruses, virus code, information on virus creation, and virus engines. Seventh is denial of service, which may be the effects of the virus.

A secondary issue which must be addressed is how to deal with the actions of preparation to commit and attempt to commit. Also the legislation should take into consideration mitigating circumstances, minor offences and the actions of the recipient.[7]

The issue is not one of regulation or not. There is obviously a need for anti virus legislation. But not in the sense of virus legislation as it is today. There is a need for the legislation of malicious software no matter the form. There is also a necessity of clarifying the responsibility of legitimate software which causes harm or property damage but this last point is beyond the scope of this brief paper.

4 Legislation Today

4.1 *The United Kingdom approach*

Prior to legislating for computer viruses, tort law and the Criminal Damage

[7] Little or no room has been given to this issue. The role of the recipient is crucial in the limitation or damage.

Act where used. In the case of Cox v. Riley charges were brought under the Criminal Damage Act 1971 which states:

> 'A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property. . .shall be guilty of an offence.'

Cox was employed to work a computerised saw. The equipment in question consisted of a powered saw whose operations could be controlled by means of the insertion of a printed circuit card containing a number of computer programs. The equipment contained a program cancellation facility. This was used by Cox, deliberately and without due cause, so that the programs were erased and the saw rendered useless until it was reprogrammed. The Divisional Court held that the critical factor was that as a result of Cox's conduct, the saw's owner was required to expend time and money in restoring the saw itself to its original condition,

The need to improve legislation to also include computer equipment into the Criminal Damage Act was clear. The Law Commission expressed the view that difficulties had been encountered in the bringing of prosecutions under this Act. Acting on its recommendations, the Computer Misuse Act was enacted which provides in section 3 that an offence will be committed by a person who causes a modification to the contents of a computer system with the intention of impairing its operation. The Act also modifies the Criminal Damage Act to make it clear that for the purposes of the Criminal Damage Act 1971 a modification of computer software shall not be regarded as damage unless the effects impair the physical condition.

Section 3 of the Computer Misuse Act 1990 refers to the unauthorised modification of computer material and states:

> (1) A person is guilty of an offence if
>
> he does any act which causes an unauthorised modification of the contents of any computer; and
>
> at the time when he does the act he has the requisite intent and the requisite knowledge.
>
> (2) For the purposes of subsection (1) (b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing –
>
> to impair the operation of any computer;
>
> to prevent or hinder access to any program or data held in any computer; or
>
> (c) to impair the operation of any such program or the reliability of any such data.
>
> (3) The intent need not be directed at –

any particular computer;

any particular program or data or a program or data of any particular kind; or

any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable –

on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

This section must be read in conjunction with section 17, which is concerned with the interpretation of the Act. From section 17 we can surmise that section 3 covers a wide range of different activities. It covers all form of intentional alteration and erasure of programs and data[8] where the intention is to impair the operation of the computer or hinder the use for the legitimate user. It is important to note that recklessness is not sufficient mens rea for this offence.[9]

Soon after the enactment, the Court of Appeal delivered its judgment in the last computer related case brought under the 1971 Act. In R v Whitely,[10] the intentional alteration of information contained on a computer disk caused significant impairment to a range of computer systems including some used in connection with medical research. He was convicted of offences under the Criminal Damage Act. The Court of Appeal sustained the convictions holding that damage to the contents of computer systems

[8] Computer Misuse Act 1990 (s.17(1)(a)).

[9] Wasik, M. (2000) Hacking, Viruses and Fraud, in Akdeniz et al (eds) The Internet, Law and Society, Pearson Education.

[10] [1993] FSR 168 (CA).

constituted criminal damage in the same manner as damage done to tangible property under the same Act despite the fact that changes in the magnetic particles on the disk could not easily be viewed.

A more recent case was that of 'the Black Baron' – Christopher Pile released a toolkit, named SMEG, which could randomise the code of existing viruses and therefore making them more difficult to detect, he also released two SMEG viruses called Pathogen and Queeg. These viruses where both polymorphic and encrypted, they displayed messages such as this one for the Pathogen virus:

> Your hard-disk is being corrupted, courtesy of PATHOGEN!
>
> Programmed in the U.K. (Yes, NOT Bulgaria!)
>
> [C] The Black Baron 1993–4.
>
> Featuring SMEG v0.1: Simulated Metamorphic Encryption Generator!
>
> 'Smoke me a kipper, I'll be back for breakfast.....'
>
> Unfortunately some of your data won't!!!!!'[11]

Pile was charged under the Computer Misuse Act and in 1995 he was sentenced to 18 months in prison.[12]

4.2 *The US approach*

Before legislation in the eighties the American courts used common law principles to prosecute computer crime. Most often drawing analogies between ordinary crimes and the new situations created by the new technology. It became a difficult task to attempt to analogise virus distribution to traditional common law transgression such as trespass. The increase in technology use led to further cases and the widespread realisation that legislation was required to improve the situation.

The Computer Fraud and Abuse Act of 1986

This Act of 1986 replaced the first piece of legislation (The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984) and was a marked improvement in clarity and usability. The new Act specified that 'unauthorized access to a government computer' was a felony, and 'trespass into a federal government computer' was a misdemeanour. The difficulties with this act became clear in its usage. It soon became clear that the Act prescribed a too narrow standard of culpability.[13] The Act required

[11] http://securityresponse.symantec.com/avcenter/venc/data/smeg.pathogen.html.

[12] R. v. Pile (1995) unreported.

[13] Colombell, M (2002) The Legislative Response to the Evolution of Computer Viruses, *Richmond Journal of Law and Technology*, Spring 2002.

that the virus writer or distributor must 'knowingly' or 'intentionally' cause the damage. This becomes difficult to prove due to the fact that once the virus is released it is almost impossible to know how and where it will strike.

More recently there have been amendments to the legislation concerning virus regulation in the form of the 2001 Patriot Act.[14] The Patriot Act amends the penalties for hackers that damage computers and also it eliminates mandatory minimum sentences.[15] Prior to the amendment offenders violating section 1030(a)(5) could receive no more than five years imprisonment while repeat offenders received up to a maximum of ten years. It was felt that these sentences where inadequate to deal with such offenders, such as the creator of viruses, like the Melissa virus[16] which caused such huge damage[17]

Previous law also included mandatory sentencing guidelines with a minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4) (accessing a protected computer with the intent to defraud).

The amendment[18] raises the maximum penalty for violations for damaging a protected computer to ten years for first offenders, and twenty years for repeat offenders.[19] At the same time the amendment removes the mandatory minimum guidelines sentencing for section 1030 violations.

4.3 *The Swedish Approach*

As early as 1992 the Datastraffrättsutredning[20] suggested that a new type of (allmänfarligt) crime should be created in Swedish law. The crime was to prevent the manufacture and spread of computer virus. The wording of the legislation was to prevent the manufacture of program code which was created with the intent to alter data without the consent of the data owner. It was also to prevent the spreading of code which had the ability to cause a danger of data loss. Despite the interest in this proposed legislation no measures have been taken by the government in the creation of any such legislation.

There is no specific prohibition on the manufacture of viruses or malicious software under Swedish law. However, the manufacture and spreading of malicious code (computer virus) can fall into several criminal categories such as illegal computer entry (dataintrång), criminal damage (skadegörelse), and sabotage (sabotage).

---

[14] Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001 http://www.cybercrime.gov/PatriotAct.htm.

[15] Section 1030(c).

[16] http://securityresponse.symantec.com/avcenter/venc/data/w97m.melissa.a.html.

[17] Estimated damages of between $80,000,000 – $800,000,000 see for example http://www.cybercrime.gov/PatriotAct.htm.

[18] Section 814 of the Act.

[19] 18 U.S.C. § 1030(c)(4).

[20] SOU 1992:110.

Illegal computer entry[21] states that anyone who without authorisation gains access to data or without authorisation makes changes or erases data will be sentenced to illegal computer entry to fines or imprisonment for up to two years.

The legislation on criminal damage[22] is both simple and clear. Destruction of, or damage to, property which affects another's rights to said property will be sentenced to fines or imprisonment for a maximum of six months.

Sabotage[23] is more concerned with the damage or destruction of property which is of vital importance to the defence of the realm, public maintenance, the process of justice or administration or the maintenance of public order and public safety shall be sentenced to imprisonment fir the crime of sabotage for a period of a maximum of four years.

The ability to prosecute the perpetrator involves a problem of a legal-technical nature. This is due to the fact that for responsibility for these actions to be sentenced, the attack must be directed towards a certain target, for example a certain data. The prosecutor must also be able to show that the perpetrator had intent to cause the damage to the target. This is often very difficult to prove since the virus manufacturer or distributor are usually unaware of the full extent of the damage their virus may cause.

If data which is damaged by a virus can be seen as damage to property (sakskada) then this can lead to a claim of damages even in a non-criminal use of viruses. A condition for a successful claim for damages is that they have been caused by criminal negligence.

Since July 1, 2001 the law has been amended to also criminalize the manufacture of viruses. The purpose of the change was also to clarify that not only physical, but also 'immaterial' objects can be seen as such criminal aides that are included in the crime of 'preparation to commit a crime'.[24] The preparatory works specifically mention computer viruses, computer programs exclusively manufactured to gain illegal entry or other types of crimes such as forgery.[25]

In the crime of 'preparation to commit' the law does not require that the manufacturer of a virus has had the intent to commit a specific attack but rather that he had the intent to commit a certain crime, sooner or later.

5 Convention on Cyber-Crime

The Convention on Cyber-Crime includes provisions dealing with illegal access and interception of computerized information of any kind,

[21] Swedish Criminal Code (Brottsbalken) Chapter 4 Article 9(c).
[22] Swedish Criminal Code (Brottsbalken) Chapter 12.
[23] Swedish Criminal Code (Brottsbalken) Chapter 13 Article 4.
[24] Swedish Criminal Code (Brottsbalken) Chapter 23.
[25] Förberedelse till brott m.m. Prop. 2000/01:85 page 50.

including data and system interference. Some provisions contained in the treaty limit the production, distribution, and possession of the software used by hackers to exploit computer vulnerabilities.

The most important piece of legislation on the horizon is the Cybercrime Convention.[26] This convention has been heavily criticized for many things, amongst others, the way in which it was developed, its lack of concern for privacy and human rights and its tendency to grant sweeping powers to police and investigatory agencies. Amongst the many acts which the convention attempts to regulate is the creation and distribution of the computer virus.[27]

> Article 4 – Data interference
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
>
> 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

The aim of Article 4 is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

In paragraph 1, 'damaging' and 'deteriorating' refer to the alteration of computer programs or data. Deletion is equated with the destruction of a corporeal thing since deletion makes data useless or unrecognisable. The concept of suppressing data is the making of data unavailable to the legitimate user. Alteration refers to the modification of existing data and would include the addition of viruses, Trojan horses and logic bombs etc. The actions in Article 4 are only punishable if they are committed without authorisation and the offender must have acted with intent.

The second paragraph allows for legislation to include the proviso that criminalisation must require serious harm. The concept of serious harm is left up to each legislating state to decide but each state is under obligation to notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility.

> Article 5 – System interference
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when

[26] Convention on Cybercrime, Budapest, 23.XI.2001 http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[27] The relevant Articles are 4, 5 and 6.

committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

The purpose of this provision is to criminalise the intentional sabotage which prevent the lawful use of computer systems, here computer systems also include telecommunications facilities, by using or influencing computer data.

The attempt is to create a level of protection for the legitimate interests of the users of computer or telecommunications equipment. The term 'hindering' refers to any and all actions that interfere with the proper functioning of the system. This could be anything from inputting, transmitting, damaging, deleting, altering or suppressing computer data.

To create criminal sanctions it is not enough that hindering has taken place it is also necessary for the hindrance to be of a serious nature. Each state shall be able to define for itself what the level of seriousness may be. The drafters of the convention, however, consider serious 'the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate 'denial of service' attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).'[28]

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2–5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing any of the offences established in Articles 2–5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of

[28] Convention on Cyber Crime, explanatory report (adopted 8 November 2001) http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

the offences established in Articles 2–5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1(a)(2).

Misuse of devices (Article 6)

With paragraph 1(a)1 the idea was to criminalise the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in Articles 2–5 of the present Convention. In this section 'distribution' refers to the active act of forwarding data to others, while 'making available' refers to the act of making available by the placing of said devices online for others to download and use. This also includes the disputable act of linking to a computer virus.

The convention goes quite far in its criminalisation of the computer virus. The creation of a virus will become, a criminal offence, the same with the distribution of any virus programs. The interesting issue is that even a hyperlink to a virus will entail prosecution for distribution. One cannot help but wonder how far the crime of linking to material can be interpreted as being a criminal act.

6 Alternative Viruses

The original latin word virus meant poison, our culture has learnt that a virus is something to be avoided, catching a virus is not something to be envied. The whole subject matter is connected to negative connotations. In the digital world the word has had the same negative connotations and this has led to the almost unanimous idea in society, which is reflected in legislation, that the virus is bad and therefore the virus must be eradicated. Anyone intentionally creating a virus must be a bad person and therefore deserves to be punished.

In this section I would like to present some alternative views on the

computer virus. My intention is not to belittle the importance of viruses or anti-virus workers. I merely want to suggest that the virus is not indisputably bad. If there may be alternative interpretations to the virus then this must be reflected in any existing or proposed legislation.

Bontchev (1996)[29] argues that viruses are bad even if they may have potentially 'good' or beneficial uses. He begins by stating that technology is in itself a neutral and is therefore neither good nor bad it is only the use of technology that can be deemed as bad. Cohen (1994) has also argued that there could, in theory, be 'good' and beneficial viruses. This position is not without its opponents, Kelman (1997) argues that virus writing is evil and cannot be justified under any circumstances.

The position of this paper is not to argue the absolute good or evil of viruses, virus writers or virus spreaders. It is not the role of the law to define what evil is. The position of this paper is to discuss the importance of recognising the alternative uses of viruses (if any) and to discuss their importance. If there may be important social roles for viruses to play then their outright damnation or criminalisation is not a step forward and this is something that any legislation and court must address.

6.1 *Virus as Art*

Art may be defined as 'the use of skill and imagination in the creation of aesthetic objects, environments, or experiences that can be shared with others. The term art may also designate one of a number of modes of expression conventionally categorized by the medium utilized or the form of the product; thus the term art can refer to painting, sculpture, filmmaking, music, dance, literature, and many other modes of aesthetic expression, and all of them are collectively called the arts. The term art may further be employed to distinguish a particular object, environment, or experience as an instance of aesthetic expression, as distinct from others of its ilk.'[30]

Any definition of art will either be too vague to be useful or too limiting. Art almost defies any real definition. As such it was inevitable that the computer virus would eventually be connected to art. The Venice Biennale is one of the more important European art events. At the 49 Biennale in 2001 a European Net Art Collective presented a computer infected with the virus 'biennale.py'. The virus was developed by the collective 0100101110101101.ORG[31] in collaboration with another group known as epidemiC.[32] The virus is written in a programming language called Python and they hope that the main spread of the virus will be limited to the source

[29] Bontchev, V. (1996) Are 'Good' Computer Viruses Still a Bad Idea? ftp://ftp.informatik.uni-hamburg.de/pub/virus/texts/viruses/goodvir.zip.

[30] Encyclopædia Britannica http://search.eb.com/eb/article?eu=9772.

[31] http://www.0100101110101101.org/.

[32] http://www.epidemic.ws/.

code printed on t-shirts and cd roms. The group has also contacted the main anti-virus companies with their virus[33] in an attempt to minimize any ill effects of the virus.

6.2 *Virus as Advertising*

Advertising is all about transferring information about products, services, opinions, or causes to public notice for the purpose of persuading the public to respond in a certain way toward what is advertised. There is little dispute about the power of advertising to inform and influence the intended audience, nor is their much dispute of the importance of advertising to the advertiser. The ability to market the message and inform the public is often a matter of survival for the advertiser. There are, however, important issues concerning the ability of small organisation to reach a wider audience. Established marketing techniques are often too costly and beyond the reach of smaller organisations.

The use of information technology has been suggested as a method for less wealthy groups to be able to reach a wider audience. Human rights organisations have seen an upswing due in part to their ability to find new members via information technology.[34] The question then is what part of the information technology can be used as a part of advertising.

One such example is the Prolin worm. The W32.Prolin.Worm uses Microsoft Outlook to email a copy of itself to everyone in the Outlook address book. The worm moves all .mp3, .jpg, and .zip files to the root folder. It renames each of these files and appends the following text to the extension of each file:

> change atleast now to LINUX

The W32.Prolin.Worm uses Microsoft Outlook to email a copy of itself to everyone in the Outlook address book. It sends an email with the subject message 'A great Shockwave flash movie' and contains the message 'Check out this new flash movie that I downloaded just now . . . It's Great Bye' in the body. The attachment is named Creative.exe. The worm creates a copy of itself with the name Creative.exe in the C:\Windows\Start Menu\Programs-\Startup folder. The worm will run each time Windows is started. The worm then moves all .mp3, .jpg, and .zip files to the root folder. It renames the files and adds the message to each 'change atleast now to LINUX' Finally the worm leaves this text message in the root folder:

> 'Hi, guess you have got the message. I have kept a list of files that I have infected under this. If you are smart enough just reverse back the process. i could have done far better damage, i could have even

[33] Reena, J. (2001) Want to See Some Really Sick Art? Wired News http://www.wired.com/news/culture/0,1284,44728,00.html.

[34] Hick et al (eds), *Human Rights and the Internet, (2000).*

completely wiped your harddisk. Remember this is a warning & get it sound and clear . . . – The Penguin'[35]

Another example is the MacMag Peace virus**.** The MacMag virus printed this message on the screen of Apple computer users: 'Richard Brandlow, the publisher of MacMag, and his entire staff would like this opportunity to convey their universal message of peace to all MacIntosh users around the world.'[36] After displaying the message, the virus deletes itself. Although MacMag is not designed to be malicious, infected systems can display a variety of problems.[37]

These two examples show how viruses may be used to transmit messages to a wider audience. While the recipient may not be pleased to receive this message or he may even be annoyed to receive it the question is whether this is enough of a reason to prohibit such communication. It is a relatively easy task to find people who are disturbed by more traditional advertising such as billboards and neon signs but this alone is not enough to stop this form of provocative communication.

6.3 *Virus as Free Expression*

Freedom of expression is a fundamental human right described the first session in 1946 by the United Nations General Assembly as the touchstone of all the freedoms to which the United Nations is consecrated.[38] Freedom of expression is often described as the precondition of individual self-expression, self-fulfilment and true democracy. The right of expression is, to paraphrase Orwell, the right to tell people what they do not want to hear. It is just this value of telling society what it does not accept to be true or given where free expression plays its most important role. To express an opinion shared by everyone is not something which requires legal protection. To express that which is uncomfortable does.

Despite its importance it is not an absolute. The freedom of expression can easily come into conflict with other rights enjoyed by society and this balance of rights must be carefully weighed and balanced in an open society.

This raises an important issue which unfortunately must be dealt with only briefly in this paper. First, can a virus writer or distributor be exercising the right of free expression and if so should this right be curtailed? While the first part of this question could be answered in several volumes it cannot be allowed in this paper. Suffice to say that whether we

[35] http://securityresponse.symantec.com/avcenter/venc/data/w32.prolin.worm.html.

[36] Branscombe, A. (1995) Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime, in Johnson & Nissenbaum (eds) *Computer Ethics & Social Values*.

[37] http://securityresponse.symantec.com/avcenter/venc/data/macmag.html.

[38] (A/RES/59(1): Para.1).

choose to look at philosophy from Mill to Habermas, international or regional conventions or national law in most cases the writing and distribution of programming code, benign or malicious must be viewed as a communicative act of expression.

There is, however, no doubt that this expression may be curtailed. The classical example that no man may cry 'fire' in a crowded theatre is an excellent analogy. The freedom exercised must not cause harm. This then is the necessary balance which must be achieved if the legislator is to attain the goal of both freedom of expression in the case of computer viruses while maintaining a secure environment and protecting property.

There is little or no discussion on the rights of the programmer in the legislation or preparatory works pertaining to the criminalization of computer viruses.

6.4 *The Helpful Virus*

There have previously been theories proposed as to what a beneficial virus could be. Researchers such as Cohen and Bontchev have proposed both beneficial uses for viruses and rules for which these may be used. The creation and study of viruses under controlled conditions is an often-cited need for the advancement of anti-virus research.

Another issue is the fact that the term 'virus' is often inadequately defined in legal texts. This lack of adequate definition leads to the problem that many benign, healthy and helpful programs fall under the definition of computer virus. This does not necessarily mean that the creators and distributors of these programs will be prosecuted but what it does mean is that there is an uncertainty in the law. The need for predictability and certainty is not satisfied when the law states not what a virus is but allows the virus to be either the fact that unwanted damage occurred or the fact that the judiciary disapproved of the program.

6.5 *Virus as Artificial life*

In 1997 the Tierra project announced that they had successfully conducted and experiment with the evolution of artificial life. The research was based upon computer programs which were capable of darwinistic evolution. The study was to increase the further knowledge on evolution and the biologist Dr. Thomas Ray used computer programs similar to viruses to be able to understand how the evolutionary process works. The goal of the project was to show that the organisms could survive under conditions of free evolution and secondly, to develop a digital model of the Cambrian explosion of life which took place on Earth about 530 million years ago.[39]

The question as to whether computer viruses also may be seen as

[39] This was when the first multicellular creatures with hard parts suddenly evolved.

artificial life was discussed by Spafford[40] in this article he discusses ten criteria for the definition of life and compares them to the behaviour of computer viruses. He concludes that the computer virus is a something akin to artificial life but cannot be refined to develop into an artificial life form. Despite the fact that Spafford does not believe that the virus may be refined into an artificial life form he concedes that the study of viruses is an important one.

7 Conclusion

Once again it is necessary to be clear upon one point. The spreading of software which causes damage to others property is not what this paper seeks to defend. The question of this paper is to question which issues present and future legislation must tale into consideration when dealing with computer viruses. One point which becomes quickly clear is the fact that the term virus is not one which can, or should, be used by legislators since the term does not clarify the problem. When it is defined it is badly defined at best and without definition the term serves no useful purpose except to create a spectre which to persecute.

Besides the point that the term virus is exceedingly inaccurate this paper attempts to show that the term virus can, and does, include several uses which may not be such as to warrant criminalisation.

If we are able to create a virus as an art form which must necessarily include the proviso that it does not damage other peoples property or harm their persons the suppression of a creative form of expression is to be equated with censorship. Censorship is not only an abusive practice it is also today frowned upon in open societies. The practice of censorship has, however, long been used to suppress that which does not please the mainstream of society. The question which must be posed is whether a virus can be spread without damaging other peoples property, this question is often answered in the negative. The reason for this negative response is the fact that viruses take up space on other peoples computers which therefore prevents them from using their property to the full extent. There are three interesting points which can be raised against this. The first is the question of whether today computer storage memory can still be seen as the limited resource it once was. Secondly there is the question of whether the argument of disk space can be used against many badly designed programs which tend to use more than their needed space on the disk[41] and finally,

[40] Eugene H. Spafford; Computer Viruses as Artificial Life; *Journal of Artificial Life*, 1(3), pp. 249–265, 1994.

[41] This is due in part to bad programming, non-requested added functions and Easter eggs (for Easter eggs see http://www.eeggs.com/).

can this be a valid argument if the program code destroys itself and leaves no lasting damage. Any legislation which states that viruses are forbidden will go beyond that which is necessary and border upon censorship.

If there can be such a thing as an advertising virus which fulfils the same requirements as the artistic (self destructing and non-damaging) the question again can be posed – should the law go so far as to outlaw the virus. The marketing virus should be dealt with under marketing law in much the same way as spam or the irritating pop-up windows.

The question of viruses being used either to market human rights groups is no different from the marketing argument above. But one of the least discussed issues is whether a damaging virus can be used for good. As earlier mentioned Bontchev (1996) reminds us that viruses are only technology and as such neutral, this means that it is only in the actual use that we can define if the virus is good or evil.

In the legal debate we often see actions not only from their effects but also we attempt to value the actions based upon the intentions of the perpetrator. In certain cases we allow harmful acts if they are done to prevent a greater evil. One such example is the permissibility of the use of force in self-defence or in the protection of property. On the web there is a growing practice of hacktivism.[42] This is the use of hacker techniques to either change the message on others web pages or to use multiple browsers to access a site thus preventing (in theory) legitimate use of the site. These denial of service attacks can be seen as being a form of picketing or demonstration, but they can also be seen as being a form of trespass. What would be the role of a virus used for these purposes and how should the law deal with the desire of the populous to protest and the rights of corporate individuals.

There is also the issue of useful software containing much of the same characteristics as the computer virus. Both naturally helpful programs which help the user carry out tasks such as copying files, updating systems and more and the more specific programs created for either virus research or research into such areas as the Cambrian explosion mentioned above. The limitation of the use of any programs which would fall under a definition of virus would in these case be more of a hindrance than a help to the legitimate user or society at large.

The question therefore remains whether legislation has gone too far? And what should the alternative approach be. One interesting methodological approach is the use of functional equivalency. Used in the UNICTRAL Model Law on Electronic Commerce[43] the concept that '... it is necessary to establish not only functional equivalents of written information ... but also functional equivalents of the performance of

[42] See for example http://www.thehacktivist.com/ or http://www.fraw.org.uk/ehippies/index.shtml.

[43] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm.

[actions] through the use of paper documents. Functional equivalents are particularly needed for the transfer of rights and obligations by transfer of written documents.'[44]

The main concept is transferable to virus legislation. Instead of creating new and nationally diverse legislation the idea is to allow the courts a greater amount of independence when deciding upon cases involving new technology. This approach is most closely seen in the type of legislation adopted by Sweden in its attempts to come to terms with viruses.[45]

Nomatter which legislative approach is chosen the problem is here to stay. Not only have we only seen the beginning of the problem with the insertion of more technology and more computer code into everything from mobile telephones, cars, fridges and any hand-held device, the computer virus as a menace and as a fact will become a common event.

The width of choices for different countries in legislating viruses will make for interesting cases where countries such as the United States penalising virus writers with jail terms running into decades while other countries may be choosing to fine its viruses writers. The cybercrime treaty is one way to go but as we have seen with other such ideas the application of multinational treaties are difficult to ensure.

Today, and for a long time into the future it is still up to the legitimate user to take precautionary measures to ensure the integrity of their systems. The question is when will the law begin to demand a reasonable standard of care from the legitimate users. Is it fair to cry foul when a virus infects a system and damages data if it was triggered by an employee wishing to read an anonymous love letter[46] or see nude pictures of tennis stars.[47] The effects of the social engineering of the virus must eventually be taken into account if virus legislation is to become well balanced. By now anyone who opens unknown attachments should know (or should be informed) that they are playing with fire.

The legislation of viruses is a serious affair. The concept itself is shrouded in mystery and fear. This is not a good basis for a balanced and fair debate but tends to be the basis of a witch-hunt. The creation of destructive software must obviously be dealt with swiftly and efficiently by the law in the same manner as any other form of criminal damage. At the same time the new legislation must not be used to give sweeping powers to the courts to remove anything that does not conform to the mainstream of computer usage.

---

[44] *Ibid.*

[45] This however has not been a conscious decision to follow a functional equivalency approach.

[46] http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html.

[47] http://www.wired.com/news/politics/0,1283,47153,00.html.