# OPINION 1

## The Lawful Truth

*Eddy Willems*
*Data Alert International, Belgium*

How a law works depends on what country you are in, although you should be aware that if you commit a crime in a country other than your own, authorities there may be able to extradite you to face prosecution (for example, this happened to Dr Popp over the Aids Information Diskette Trojan). Sometimes I hear people saying that virus writing does not need to be made illegal. If it is not illegal to write viruses, the law should concentrate on the damage caused by the virus, but this is not always easy.

Maybe a virus writer should not be held responsible – unless his virus appears somewhere where it is not wanted. But if it does, then its creator must be prosecuted (if known, of course) – even if he is not directly responsible for spreading the virus.

Naturally, the person who spreads a virus intentionally is even more guilty and should be prosecuted more severely, but the original author should be held responsible too, for letting his creation escape. I overheard someone saying that the proper legal term for this kind of occurrence in Belgium is 'criminal negligence'.

I have been working in the anti-virus business for ten years but it seems that I was one of the first in Belgium to complain about the unbelievably old laws we are still subject to over here. I have enquired of and complained to the Federal Police on a regular basis, but they have not been able to do anything about the virus exchange boards and sites because, until recently, there has been no relevant legislation. This has made me angry sometimes but a change is on the way.

**New Legislation: An Improvement?**

A few years ago the only way to deal with a hacker or virus writer in Belgium was to prosecute them for 'misuse of electricity'. This was a really an old law dating back practically to the Napoleonic ages which was still active. After years and years of long meetings where I and a lot of others asked for new, improved legislation, it happened that some fairly recent viruses and fast-spreading worms shook the Belgium Government itself really hard. At last, this resulted in completely new legislation concerning so-called cyber crime being implemented early this year .

Let us see what came out of the brilliant minds of our Belgian Government. Individuals who intentionally break into a network will now face a 625 Euro fine and/or risk incarceration of from three months to two years. The same punishment will be meted out even if you try to break into an area of your employer's network to which you do not have access. It is exactly the same if the break-in was started and did not work out completely as foreseen. So, even an attempted break-in will be punished.

If a hacker actually causes damage or if he used the hacked system to gain illegal entry, then that individual will face a fine of 1250 Euros and three years in a state prison. The person who helps him with hacking tools like password-stealing devices and so on will be fined 2,500 Euros and awarded a spell in prison of between one and three years.

Furthermore, if someone hacks or write a virus 'by order of…' (i.e. on behalf of or at the behest of someone else) then that accessory will be held responsible too, and faces up to five years in prison and/or a 5,000 Euro fine. Virus authors themselves risk a fine of 2,500 Euros and/or three years in gaol.

Individuals who unleash viruses, worms or Trojans (or other malicious code) onto a system, whether or not it is intentional, will also be threatened with up to three years in prison. If such a virus causes damage such as file deletion, the writer concerned could be locked up for up to five years and have to pay a 2,500 Euro fine. If someone re-attempts the same thing, then the punishment is doubled.

I think this is an improvement. Up until now we have had no formal, legal redress with which to deal with all our virus writers and cyber terrorists. I hope with these laws in place that we will experience a decrease in virus and security problems.

However, it could also turn out that laws forbidding virus writing and malware distribution will not deter virus authors, and in some cases could even spur them on. Despite calls from the anti-virus industry and users for tougher legislation covering the writing and distribution of viruses, this may not be the answer and could even do more harm than good.

Police intervention does not always offer a significant deterrent. Even the well-publicised conviction of virus writers such as David Smith (author of the notorious

VIRUS BULLETIN **©2001 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. / 2001/$0.00+2.50**

Melissa virus) failed to impact the number of new viruses appearing throughout the world. Maybe we could try to educate people or even children that virus writing is not a 'good' thing to do in order to prevent a new generation of virus writers developing. But how do you do that?

### The e-Security Team: Another Good Move?

After the VBS/LoveLetter outbreak, the Belgian Government wanted to do something special for the Belgian people. Following a day of brainstorming, one minister came up with the idea of putting up a Web site where everyone could find alerts of security issues such as viruses. The goal was to alert the Belgian people before anything else was published on the Internet and before an outbreak could begin. An attractive goal and an interesting new approach – that was the idea, anyway.

In order to run this Web site and its associated alarm system, the minister's cabinet duly decided to set up a security team which consisted of relevant experts. Thus, on 5 May 2000, what is known as the e-Security Team of *BIPT* (*Belgian Institute of Postal services and Telecommunications*) was established.

Despite the fact that Belgium does not boast many anti-virus or IT Security experts, after just two days this team was formed. It included individuals from ISPs, some TV stations, several large corporations and two security companies. So, where are the real experts? *Data Alert International*, the company I work for, volunteered me as the only anti-virus expert within the whole team. The other security company donated a general security expert. I really have my doubts about the persons they gathered from the other companies. I also have my doubts about the system being used to alert Belgian citizens. This is how it works.

When one member of the e-Security team hears about a new virus or security breach, he must alert the *BIPT*-system (let us call it *BIPT* for simplicity's sake). This alert can be communicated by email, phone or fax. After that, *BIPT* must attempt to reach everyone concerned by email and mobile phone.

This is done in the following way: an email, with an attachment, is dispatched to everyone on the team. The attachment is a *Word* document in .DOC format, containing details about the facts of the problematic new virus, worm, Trojan or hoax. At that moment, an SMS message is also sent to everyone on the list to ask them to have a look at their email. The document attached can then be used to send additional and more precise information about the virus to *BIPT*. Can you imagine the feeling I had when I saw the first email they sent to me? If someone in the chain has inadequate protection they could send a virus round within the email itself! Immediately, I asked that some other method be used to send this information around.

So, what happens next? After receiving this information our job is to respond within one hour. If this is done properly an article can be published on the Web page within that time, and a national security alert can be prepared – nice, if it works. However, the details of the first message I saw were rather disappointing; it would appear that some members of the team cannot even tell the difference between a hoax and a virus. Neither can they distinguish if something is of low or high importance. In one case I was just in time to prevent a warning for a non-existent virus!

The alerts often seem to be based on personal feelings or thoughts, and are often superfluous. They also change depending on the person who is responsible for editing the site at that specific moment. Indeed, there seems to be a sort of shift system. The articles change too – a few months ago everything was translated. Now, they have stopped doing this and instead, they just add some links to various anti-virus developer Web sites. Would it not be more helpful to point to all AV Web sites and only select genuine alerts? But, how do you define a real alert?

At those times when I am out of contact with the team, members tend to gather information about the 'problematic' virus direct from an anti-virus developer's Web site. It is then consolidated and put on the official team Web site even if it has not been verified. I am afraid that I have lost sight of the original goal. Furthermore, I would say that at such times as that described above the system certainly does not act as an early warning.

### Making it Work

Now, do not misunderstand me. The original concept of an early warning system has some potential. I have already explained the problems I see to the team and improvements are being made. And the system has worked in the past! We managed to get an early warning out about the 'Big Brother' hoax even before it showed up on the anti-virus developer Web sites. This, in my opinion, is the best example that shows the system is functioning efficiently.

It occurs to me that the *BIPT* e-Security Team is actually more of a political game than it appears, but nevertheless the idea behind the project should be honoured, because it is a responsive and a helpful one. The question remains, however, could a new virus or worm with all the latest and perhaps even unknown spreading techniques be quicker than this system?

Despite my busy schedule doing consultancy work, giving presentations, analysing viruses and seeing to *EICAR* matters, it seems to me that I have always got several channels open to help the team when it is really needed. I sincerely hope that I will be on time at that moment! You can take a look at the *BIPT* Web site at www.bipt.be, where you will find all the warnings posted in Dutch and French, our national languages. Oops! An SMS message from *BIPT* just came through on my mobile phone as I was finishing this article. It seems that I am working more on behalf of the Belgian people than for *Data Alert International* at this moment!