

DAWN OF THE DEATH OF DISTRIBUTED DENIAL OF SERVICE: HOW TO KILL ZOMBIES

LILIAN EDWARDS*

TABLE OF CONTENTS

I. INTRODUCTION TO THE PROBLEM	23	R
A. <i>Prevalence and Effects of DDOS</i>	28	R
B. <i>Who Suffers DoS/DDOS and Why</i>	32	R
II. LEGAL RESPONSES TO DoS AND DDOS.....	35	R
A. <i>Criminal Law</i>	36	R
B. <i>DoS and Intent: the “Possessed by Aliens” Defense</i>	41	R
C. <i>Civil Law</i>	43	R
1. <i>Sue the Zombies?</i>	46	R
2. <i>Sue the Software Writers?</i>	51	R
III. SECURITY IS FOR EVERYONE, NOT JUST FOR CHRISTMAS .	56	R
A. <i>Targets</i>	58	R
B. <i>ISPs</i>	59	R

I. INTRODUCTION TO THE PROBLEM

According to Wikipedia, the on-line encyclopedia, a “*denial of service*” or “DoS” attack is:

an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.¹

In layman’s terms, a DoS attack has the effect of making a computer system—whether it is operated by a business, a public sector resource, or an individual—unable to supply its services to clients. CERT, based at Carnegie-Mellon University and the leading center for Internet security, categorizes a “denial-of-service” attack as “an explicit attempt by attackers to prevent

* LLB (Hons)(Glas), LLM (Cantab), MSc in IT(York); Co-Director, Arts and Humanities Research Council Centre for Research into Intellectual Property and Technology Law, University of Edinburgh, and Chair of Law, University of Southampton. The title of this essay derives from perhaps the most famous zombie film of recent years, George Romero’s *Dawn of the Dead* (1978), the source of numerous parodies, including Edgar Wright’s excellent *Shaun of the Dead* (2004). As will be discussed below, “zombie networks” are the proximate cause of the blight of distributed denial of service (DDOS), and are increasingly the main conduit for distribution of spam, malware, and phishing attacks.

¹ Wikipedia, *Denial-of-service attack*, <http://en.wikipedia.org/wiki/DDOS> (last visited Feb. 26, 2006).

legitimate users of a service from using that service.”² Examples of DoS they give include:

- attempts to “flood” a network, thereby preventing legitimate network traffic;
- attempts to disrupt connections between two machines, thereby preventing access to a service;
- attempts to prevent a particular individual from accessing a service; and
- attempts to disrupt service to a specific system or person.³

As Ofcom, the UK communications regulator, has pointed out,⁴ there are a number of means by which a target computer system can be stopped from delivering its services. First, it can be physically attacked, for example, by stealing or damaging hardware.⁵ However, this has obvious disadvantages as the attacker needs to be physically present and most businesses now have physical security, including ID requirements, in place to prevent such attacks. Next, the target computer can be damaged at a distance by altering or modifying the software which runs on it, for example, by hacking, or virus dissemination.⁶ However, strong authentication and access controls, as well as virus checking and firewalls, make the effectiveness of this type of attack less certain than was once the case. Hence, the final—and now most—common way to bring down a computer system remotely is to tie up its essential and scarce resources, such as the number of connections that can be made from outside, bandwidth, processing power, or memory available.⁷ The system becomes overwhelmed and can no longer meet the demands of legitimate users.⁸

The interesting point about a typical DoS attack is that it is accomplished by making a very large number of nonetheless *legitimate* demands upon the target’s computational resources. It is impossible for law enforcement authorities to distinguish between (for example) web page requests made by legitimate users and those made for the illicit purpose of bringing down the system. The act in both cases is identical; only the intent behind it is

² See CERT Coordination Center, *Denial of service attacks*, http://www.cert.org/tech_tips/denial_of_service.html (last visited Feb. 26, 2006).

³ *Id.*

⁴ Peter Ingram, Chief Technology Officer, Ofcom, *Denial of Service*, presentation to Cambridge-MIT Institute: Communications Innovation Institute, DOS-Resistant Internet Working Group, Jan. 14, 2005, available at http://www.ofcom.org.uk/media/speeches/2005/01/resistant_internet_working.pdf (last visited Feb. 26, 2006).

⁵ *Id.*

⁶ *Id.*

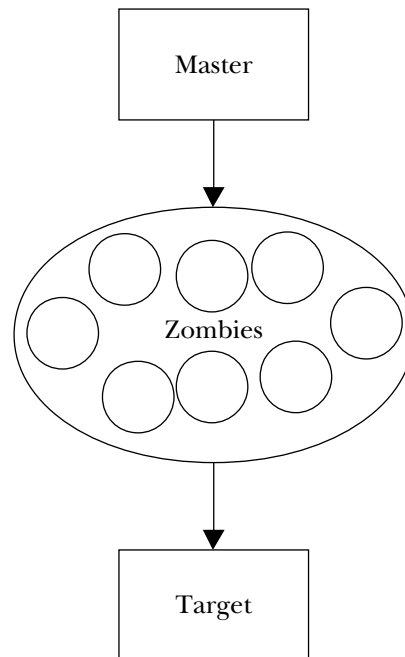
⁷ *Id.*

⁸ *Id.*

different. It is not illegal—indeed, it is encouraged—to send email, request a page, or download a publicly-available file from a website or computer. As we shall see, this makes DoS a difficult act to criminalize, since the acts in question become criminal (a) only in bulk, and (b) only when motivated by malice. In this sense, the problems of criminalization of DoS are akin to those of spam, where the ordinary act of sending an email is transformed by bulk and disregard for social order into something commonly regarded as worthy of criminalization.

The second key point is that a DoS attack clearly requires a large amount of resources to mount. A single hacker, however determined, cannot easily make enough page requests, or send enough emails, to knock down the server of, say, Worldpay, or the FBI, or CNN. The computational resources that such organizations can command will be very large, as are, possibly, their back-up resources to deal with surges in traffic.⁹ Hence, DoS attacks are almost always mounted as *distributed denial of service (DDOS) attacks* (see diagram below).

FIGURE 1: DISTRIBUTED DENIAL OF SERVICE—DDOS



DDOS attacks work by using remotely controlled computers to

⁹ See Cert Coordination Centre, *supra* note 2.

generate more requests of a device than it can serve.¹⁰ The remotely controlled machines are typically, though not always, insecure home or university computers, and are invariably controlled without the knowledge of their owner.¹¹ The owner will usually notice no, or almost no, degradation of his own computer's performance.¹² It is the DDOS target that eventually suffers. These controlled machines are known as *bots*, *slaves*, or *zombies*.¹³ The attacker (or hacker, or mastermind, or *zombie-master*) gains remote control over these machines via zombie clients implanted in them.¹⁴ These are usually implanted either by viruses or worms propagated via the Internet.¹⁵ *Viruses* are in essence programs that replicate themselves.¹⁶ They may be contained in email attachments opened by the computer owner, or in programs the owner is induced to click on while surfing (for example, by disguising the virus as a nude picture of a well known starlet).¹⁷ Zombie clients are now mainly spread by a species of viruses known as *worms*, such as the MyDoom or Agobot worms.¹⁸ *Worms* typically install "backdoors" in the infected computer, enabling the computer to be remotely controlled.¹⁹ The backdoors can also be exploited by other worms, such as Doomjuice, which spread using the backdoor opened by MyDoom.²⁰ *Trojan viruses* are a delivery mechanism for viruses and worms.²¹ They lurk in otherwise legitimate executable files (programs); and when the infected programs are run, the machines are infected or pass the infection to other connected machines.²² The characteristics of all three categories of virus, worm and Trojan are becoming intertwined and may now be found in one piece of software.²³

¹⁰ *Id.*

¹¹ See Wikipedia, *Denial-of-service attack*, *supra* note 1.

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ See Wikipedia, *Computer Virus*, http://en.wikipedia.org/wiki/Computer_virus.

¹⁷ See Kelly Martin, *Security meltdown: who's to blame?*, THE REGISTER, Jul. 6, 2005, http://www.theregister.co.uk/2005/07/06/security_blame (last visited Feb. 26, 2006) (stating that "[t]hey [hackers] would deserve all the blame if it wasn't so darn easy to convince a user to click on the attacked picture: 'it's one of Angelina Jolie and she's nude' pretty much guarantees success.").

¹⁸ John Leyden, *MyDoom Returns*, THE REGISTER, Jan. 17, 2005, http://www.theregister.co.uk/2005/01/17/mydoom_returns (last visited Feb. 26, 2006).

¹⁹ See Wikipedia, *Computer Worm*, http://en.wikipedia.org/wiki/Computer_worm (last visited Feb. 26, 2006).

²⁰ *Id.*

²¹ See Wikipedia, *Trojan Horse*, http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29.

²² *Id.*

²³ See, e.g., <http://www.ircbeginner.com/opvinfo/trojan-virus.html> (last visited Feb. 26,

DDOS involves the use of huge networks of zombie machines (10,000 or more in some cases) which have been so infected.²⁴ The infected machines are then remotely instructed to attack the target site simultaneously.²⁵ Each zombie can generate thousands of requests of a server, an effect then multiplied by the size of the zombie network.²⁶ With enough zombies, even the biggest and most secure web sites or Internet pipes can be overwhelmed. Common types of DDOS attack software optimized for different types of system include “smurf”, “trinoo” and “Tribal Flood Network.”²⁷ The technical details of these forms are unnecessary for this paper, since all essentially take the form of a master/zombies attack.

Besides providing enough resources to bring down a serious commercial or governmental site, the use of zombie networks makes the zombie-master—the actual criminal behind the attack—almost untraceable.²⁸ The IP addresses of machines sending requests that initiate the DDOS will be those of the innocent zombies, not the zombie-master.²⁹ In the infamous “Mafiaboy” case in August 2000, a sixteen year old Canadian, convicted of initiating DDOS attacks on major sites such as CNN, Amazon.com, eBay, and Dell was caught only because he bragged of his exploits on an Internet Relay Chat (IRC) channel, not because of computer forensics.³⁰

Finally, zombie networks are by no means used only for DDOS attacks. They are now the main means of delivering spam email,³¹ since almost all legitimate ISPs refuse accounts to known spammers, and automatically limit the capacity of new spammers to send millions of emails at once from their own email address.³² Sending spam via zombies, as well as enabling unfiltered access to the target market, practically guarantees untraceability, and also

2006) (stating that “[t]he ‘LoveBug’ . . . is a perfect example of all of the above. It’s a Trojan because it came disguised as a ‘Love Letter’ when really it was carrying a harmful program. It is a virus because, once executed, it infected files on your computer, turning them into new Trojans. It’s a worm because it propagated itself by sending itself out to everyone listed in your email address book or IRC client.”).

²⁴ See <http://en.wikipedia.org/wiki/DDOS>.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *W3C Briefing on Securing Against DoS Attacks FAQ*, <http://www.w3.org/Security/Faq/WWWsf6.html> (last visited Feb. 26, 2006).

²⁸ See Cert Coordination Centre, *supra* note 2.

²⁹ See <http://www.grc.com/dos/drDOS.htm>.

³⁰ *16 year old boy charged with web site attacks*, OUT-LAW.COM, Aug. 4, 2000, <http://www.out-law.com/page-875>.

³¹ John Leyden, *Zombie PCs spew out 80% of spam*, THE REGISTER, Apr. 4, 2004, http://www.theregister.co.uk/2004/06/04/trojan_spam_study.

³² See Wikipedia, *Denial-of-service attack*, *supra* note 1.

prevents mail from being bounced back to the true address of the spammer.³³ Older methods by which spammers evaded ISP control, such as using “open mail relays”—mail server machines with inadequate authentication security—are now ceasing to be operative, both because security among mail server administrators is tighter, and because lists of the IP addresses of such open relays are now regularly circulated and updated by “blackhole lists,” and then in turn blocked by network administrators.³⁴ The HoneyNet project³⁵ found that in addition to their role in DDOS and spam, zombie networks are now extensively used to sniff network traffic for unencrypted passwords, for key logging, to install spyware, and for click-fraud involving Google’s AdWords program. These latter activities enable online fraud. “Phishing” emails, which seek to obtain personal financial and account data by fraud, are also known to be mainly sent out from zombies.³⁶ Control of zombie networks would thus solve not just the DDOS problem but also many other major Internet social blights.

A. *Prevalence and Effects of DDOS*

DDOS has been recognized as a major security and business concern on the Internet since at least 2000, when the first major wave of DDOS attacks hit the headlines.³⁷ Whereas early virus, worm and hack attacks required skilled programming knowledge and an enormous input of time and energy, modern automated tools make it staggeringly easy to create, modify and disseminate viruses and worms, and to scan for and infect insecure machines. The new wave of DDOS zombie-masters are thus as likely to be computer illiterate Russian mafiosi as they are to be the classic

³³ See Wikipedia, *Zombie computer*, http://en.wikipedia.org/wiki/Zombie_computer.

³⁴ Lilian Edwards, *Canning the Spam and Cutting the Cookies: Consumer Privacy On-Line and EU Regulation*, in *THE NEW LEGAL FRAMEWORK FOR E-COMMERCE IN EUROPE* (Lilian Edwards ed., 2005).

³⁵ See HoneyNet Project, <http://honeynet.org/> (last visited Feb. 26, 2006); see also Bruce Schneier, *Attack Trends: 2004 and 2005* (June 2, 2005), <http://www.schneier.com/essay-085.html>.

³⁶ See *CipherTrust Proves Worldwide Phishing Attacks Originate From Less Than Five Zombie Network Operators*, IT OBSERVER, Oct. 19, 2004, <http://www.ebcvg.com/press.php?id=521> (last visited Feb. 26, 2006). CipherTrust found that less than 1% of all email was “phishing” email, but that fewer than five zombie network operators were responsible for all Internet phishing attacks worldwide. Of these zombies, 32% were based in the U.S., 16% in Korea and the rest spread across 98 countries.

³⁷ In fact, the first well-documented DDOS attack appears to have occurred in August 1999, when a DDOS tool called Trinoo (described below) was deployed in at least 227 systems, of which at least 114 were on Internet2, to flood a single University of Minnesota computer; this system was knocked off the air for more than two days. See <http://www.anml.iu.edu/ddos/history.html>.

teenage male genius geek.³⁸ The spiraling adoption of broadband, which tends to encourage users to leave machines permanently connected to the Internet, especially home PCs owned by consumers who know little or nothing of firewalls and security, has also made infection a matter of simplicity and concomitant universality. To add insult to injury, it is no longer necessary for a criminal to have extensive technical know-how to establish his own zombie network. Zombie networks are now known to be regularly traded by virus writers as commodities to criminals, spammers and gangsters.³⁹ The price is not high: *The Register* in April 2004 cited a sale of a 10,000 host zombie network for \$500 in the summer 2003, with the proviso that the price might rise, since infected hosts are now more often cleaned of spyware and secured.⁴⁰ In fact, Symantec recently cited the price as around \$350 for 5,500 hosts.⁴¹ So many hosts are now infected with worms and “back doors” that it is also now quite possible to “steal” a zombie network rather than set one up from scratch,⁴² and the Honeynet project has reported observing such “thefts.”⁴³

Chandler cites research in 2001 by CERT, which observed nearly 13,000 attacks on over 5,000 different machines belonging to 2,000 different organizations within a three week period in 2001.⁴⁴ These figures would now look reassuring compared to the insecurity exploitable in 2005. The anti-virus firm Sophos claimed in July 2005 that any unprotected home PC connected to broadband in the UK has a 50% chance of being infected within 12

³⁸ See *supra* text accompanying note 30 (even the notorious “Mafiaboy” did not really fit this profile in 2000); see also D. Ian Hopper, *Canadian teen charged in Web site attack released:*

Boy arrested for CNN.com ‘denial of service’ hack has tough limits on Internet contact, (Apr. 19, 2000), <http://archives.cnn.com/2000/TECH/computing/04/19/dos.investigation/> (“Hackers like to brag about their capability,” said Inspector Yves Roussel, officer-in-charge of the RCMP’s Commercial Crime unit. ‘Mafiaboy was not that good, actually. He wasn’t what we could call a genius in that field.’ Roussel said others could easily make the types of attacks made by ‘Mafiaboy.’ Several simple and easy-to-find tools are available for inflicting a distributed denial of service attack, including Tribal Flood Net and Trinoo.”).

³⁹ See John Leyden, *The illicit trade in compromised PCs*, THE REGISTER, Apr. 30, 2004, http://www.theregister.co.uk/2004/04/30/spam_biz/ (last visited Feb. 19, 2006); see also Wikipedia, *supra* note 1.

⁴⁰ See John Leyden, *Phatbot arrest throws open trade in zombie PCs*, THE REGISTER, May 12, 2005, http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/.

⁴¹ See *Hackers Aim Now Is Fortune Over Fame*, CANBERRA TIMES (Jul. 11, 2005) at 13.

⁴² See John Leyden, *The strange death of the mass mailing virus*, THE REGISTER, Dec. 19, 2004, http://www.theregister.co.uk/2004/12/09/symantec_virus_forecast_2005/.

⁴³ Honeynet Project, *supra* note 35.

⁴⁴ Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 231 (2003-2004).

R

R

R

minutes.⁴⁵ Schneier, summarizing in 2004 the results of the ongoing HoneyNet Project,⁴⁶ which leaves typically set up machines on-line and unprotected to assess the prevalence of random attacks, reports that:

[a] random computer on the Internet is scanned dozens of times a day. The life expectancy, or the time before someone successfully hacks, a default installation of Red Hat 6.2 server is less than 72 hours. A common home user setup, with Windows 98 and file sharing enabled, was hacked five times in four days. Systems are subjected to NetBIOS scans an average of 17 times a day. And the fastest time for a server being hacked: 15 minutes after plugging it into the network.⁴⁷

Using its sample of exposed machines, the HoneyNet Project reported in March 2005 that in three months from November 2004 to January 2005, 226 DDOS attacks were launched on 99 different targets.⁴⁸ The Project estimates that around one million infected hosts are under the control of zombie-masters.⁴⁹

Because of the speed of recent adoption of broadband, and the failure of consumers to keep up with security requirements, the EU and especially the UK⁵⁰ have become hot spots for the creation of “zombie hordes.” Symantec, the Internet security firm, reported in March 2005 that Britain had the largest zombie PC population of any country on the planet.⁵¹ The UK had more than a quarter of all zombies (25.2%), with the US closely behind (24.6%), and China (7.8%) in third place.⁵² Another report in May 2005 declared that 26% of all worldwide infected zombie PCs were to be found in the EU, compared with 20% in the US and 15% in

⁴⁵ See John Leyden, *Malware authors up the ante*, CHANNEL REGISTER, Jul. 1, 2005, http://www.channelregister.co.uk/2005/07/01/sophos_1h05_malware_report/.

⁴⁶ HoneyNet Project, *supra* note 35.

⁴⁷ Bruce Schneier, *Foreword*, in KNOW YOUR ENEMY: LEARNING ABOUT SECURITY THREATS (The HoneyNet Project ed. 2d ed., 2004).

⁴⁸ HoneyNet, *supra* note 35.

⁴⁹ See John Leyden, *Rise of the Botnets*, THE REGISTER, Mar. 15, 2005, http://www.theregister.co.uk/2004/09/20/rise_of_the_botnets/.

⁵⁰ See UK ‘embraces digital technology’: *Increasing numbers of people in the UK are moving to digital and broadband technology, according to the latest report from media regulator Ofcom*, (July 13, 2005), http://news.bbc.co.uk/1/hi/entertainment/tv_and_radio/4679023.stm. Ofcom report that as of July 2005, for the first time more households in the UK (over 8 million) have broadband access to the Net rather than dial up (7.5 million). Almost 2 million households went broadband in the 6 months between December 2004 and June 2005.

⁵¹ See John Leyden, *Britain tops zombie PC charts*, THE REGISTER, Mar. 21, 2005, http://www.theregister.co.uk/2005/03/21/botnet_charts/.

⁵² See *id.* (citing Symantec’s *Global Internet Threat Report* which notes the statistics were based on the period July to December 2004 for the number of PCs worldwide known to be infected with bot agents such as the Agobot worm).

R

R

China.⁵³

The net effect of all this has been that DDOS has arrived since 2004 as one of the top three computer security threats most feared by European businesses.⁵⁴ Both U.K. and U.S. empirical evidence demonstrate growing concern among commercial and law enforcement bodies. The 2005 NOP/National Hi-tech Crime Unit study on Hi-Tech Crime found that denial of service was taken seriously by 79% of respondents, drawn from a range of companies with a bias towards those with over 100 employees.⁵⁵ Only 17% of all respondents had actually experienced a DoS attack, compared to the 83% who had experience of the most common computer crime, infestation by viruses, worms, or Trojans.⁵⁶ This figure had nonetheless doubled since the same survey in 2004.⁵⁷ Those who had experience of DoS each reported only around two attacks experienced in 2004.⁵⁸ These figures do not make DoS seem a major concern, and for smaller companies it is probably not. However, the total economic damage inflicted by each DoS attack for companies over 1000 employees *is* significant, when loss of 24/7 client service delivery, loss to brand, loss of productivity by employees and loss of goodwill are all factored in.⁵⁹ These respondents estimated that DoS had cost them in 2004 almost £555 million—an estimate of cost which ran second only to that inflicted by viruses, worms and Trojans (£677 million) and financial computer fraud (£622 million).⁶⁰ The threat of DoS is summed up by what was said when respondents were asked what the single most important impact of computer enabled crime was: 69% said it was whether the company's ability to continue to do business with its customers was endangered.⁶¹ Since this is the exact purpose of a DoS attack, it is no wonder it is so costly when it succeeds.

U.S. figures drawn from the 2005 CSI/FBI Computer Crime and Security Survey show a similar pattern.⁶² Of recorded computer crimes reported by respondents, 17% involved DoS—

⁵³ See Iain Thomson, *EU zombie army leads the world*, VNUNET.COM, May 27, 2005, <http://www.vnunet.com/vnunet/news/2135706/eu-zombie-army-leads-world>.

⁵⁴ See NOP/National Hi-Tech Crime Unit Study on Hi-Tech Crime 12 (2005), http://www.nhtcu.org/media/documents/publications/8817_Survey.pdf (last visited Feb. 20, 2006).

⁵⁵ *Id.*

⁵⁶ *Id.* at 25.

⁵⁷ *Id.* at 16.

⁵⁸ *Id.*

⁵⁹ *Id.* at 24.

⁶⁰ *Id.*

⁶¹ *Id.* at 12.

⁶² COMPUTER SECURITY INSTITUTE, 2005 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY (2005).

exactly the same proportion as in the UK.⁶³ In terms of dollar amount of loss due to the crime in question, however, DoS came fourth with an estimated \$7.3 million loss to the respondents.⁶⁴ The survey notes, however, that estimates of costs of computer crime were only reluctantly and loosely provided by respondents, if at all; and that the costs of virus damage are becoming (for reasons outlined above) irresistibly intertwined with those caused by DoS, so that these figures are unreliable in separation.⁶⁵ What is very different in the U.S. report from the UK report is a clear trend of decline in reported hi-tech computer crime in general, and its cost implications, including DoS.⁶⁶ Whether this will be replicated in Europe, or whether it is merely the product of selective non-reporting by certain companies worried about adverse publicity (a trend evident in the survey), remains to be seen.⁶⁷ It is possible that while certain crimes, such as theft of confidential data, are declining because of better security and authentication practices, threats such as DoS which arise from a lack of security on the part of consumer-owned zombies, rather than corporate targets, will continue to rise.

B. *Who Suffers DoS/DDOS and Why*

Denial of service attacks have a variety of targets and purposes. The earliest DoS attacks, as with much early hacking, may have been carried out simply to demonstrate prowess in hacking, or out of sheer malice or spite. Attacks carried out on ad servers such as those operated by DoubleClick, attacked in July 2004, or on on-line payments companies, such as the attacks on WorldPay in November 2003, and again in 2004, often bear this kind of character.⁶⁸ Attacks on payment systems have collateral effect on other industries which are highly disruptive. When WorldPay was attacked in October 2004, for example, 30,000 clients around the world using its payment services were potentially affected.⁶⁹

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.* Viruses topped the table for losses due to computer crime, with \$42 million losses resulting reported in 2005.

⁶⁶ *Id.* at 13.

⁶⁷ *Id.*

⁶⁸ *DDoS Attack On Ad Company Shuts Down Sections Of Internet's Most Popular Sites*, DMEUROPE, July 28, 2004 (DDoS attack on DoubleClick); Chris Nuttall, *Complacency At Targets Helps Hackers Make Mischief*, FIN. TIMES, Nov. 12, 2003, at 4 (DDoS attack on WorldPay in 2003); *Worldpay Hit By "Malicious" Denial Of Service Attack*, FIN. TIMES (VNU NEWSWIRE), Oct. 4, 2004 (DDoS attack on WorldPay in 2004).

⁶⁹ See *Worldpay Struck By Online Attack*, BBC NEWS, Oct. 4, 2004, <http://news.bbc.co.uk/2/hi/business/3713174.stm>.

Another non-economic reason for DoS attacks is to make a political or ethical point. Activists frequently organize DoS attacks to shut down the website of an offending corporation for a short period, with attendant publicity.⁷⁰ An interesting recent variation on this is the use of DDOS to try to shut down spammer sites, allegedly in the public interest. In November 2004, Lycos Europe made a “Make Love, Not Spam” screensaver available for free download which also launched DDOS attacks on spam sites manually selected by Lycos from the list supplied by Spamcop.⁷¹ The tool could, according to Lycos, flood target sites with around 33 terabytes of useless traffic generated by 10 million screensavers downloaded.⁷² After some public concern as to the legality of the tool in various European jurisdictions, and hostility from leading anti-spam groups, the screensaver was withdrawn.⁷³ Another variation on “public interest” DDOS was floated during recent U.S. debates on how to control illegal downloading of music and movie files.⁷⁴ Representative Howard Berman suggested that DDOS attacks on sites trading in illegally copied files, especially peer-to-peer (“P2P”) sites, should be exempted from criminal liability.⁷⁵ Although the suggestion was welcomed by the RIAA, P2P companies were less enthused, describing it as a call for “a posse of copyright vigilantes.”⁷⁶

More recently, concern about DDOS has revolved mainly around its use for two purposes: commercial blackmail, and threat to critical infrastructure. There has been an explosion since 2004 in the use of DDOS to blackmail companies by criminals threatening to hack and bring down their sites unless pay-offs are

⁷⁰ See Armin Medosch, *Hactivism—Political Activism on the Net or: Why we have to protect the net as a public sphere—Draft speech for 10th of July conference by the Transnational Radical Party*, at <http://servizi.radicalparty.org/documents/index.php?func=detail&par=54> (“For example in the context of the Seattle protests by the global anti-capitalist movement, an English hacktivist group emerged who called themselves electrohippies and launched a netstrike on the servers of the World Trade Organisation and the IMF. German activists who support asylum seekers and tried to stop forced deportations on Lufthansa flights organised a netstrike against the flight booking service of Lufthansa on the internet.”).

⁷¹ See Paul Roberts, *Lycos, spammers trade blows over screensaver*, THE INDUSTRY STANDARD (Dec. 2, 2004), <http://www.thestandard.com/internetnews/000689.php>.

⁷² *Id.*

⁷³ *Id.* Interestingly, Lycos claimed they were not committing any illegal act because they were always careful to slow down the target site but not to actually shut it down. In terms of UK law, it is doubtful if this would have made a crucial distinction as both would involve (or, arguably, not involve) a “modification” of the target or “unauthorized access” to the target.

⁷⁴ *Lawmaker Tries to Foil Illegal File Sharing*, WASH. POST (June 25, 2004) (on file with author).

⁷⁵ *Id.*

⁷⁶ *Id.* (quoting Ellen Stroud of Morpheus noting that Berman’s suggestion appears to have fallen along with the Bill he was introducing).

made.⁷⁷ In the UK, this has been particularly directed at the online gambling industry, whose members, according to the All Party Parliamentary Internet Group (“A.P.I.G.”) report,⁷⁸ frequently receive demands for between \$10,000 and \$40,000. In the United States demands of up to \$100,000 have been reported.⁷⁹ Law enforcement activity is impeded not only by dubiety about the legal framework,⁸⁰ but also by systematic non-reporting of extortion by companies worried about bad publicity and exposure of security vulnerabilities.⁸¹ Law enforcement is further impeded by DDOS becoming mainstreamed as part of Mafia and gangster activity, which is often controlled from remote jurisdictions, notably Russia and Eastern Europe.⁸² The United Kingdom National Hi Tech Crime Unit officers made high profile arrests of several Russian DDOS gangsters in July 2004.⁸³ Anti-DDOS software costs around \$12,000 per month, which puts it out of the range of many small companies and is not always effective.⁸⁴ An interesting wrinkle in the use of DoS for commercial gain is its use as an anti-competitive practice. One case reported in March 2005 featured a company in New Jersey which hired a seventeen year old to DDOS attack a competitor website, www.jersey-joe.com.⁸⁵ The target site suffered losses in excess of \$1 million as a result. Remarkably, the FBI was able to track the viruses

⁷⁷ See Schneier, *supra* note 35 (“Another 2004 trend that we expect to continue in 2005 is crime. Hacking has moved from a hobbyist pursuit with a goal of notoriety to a criminal pursuit with a goal of money. Hackers can sell unknown vulnerabilities—‘zero-day exploits’—on the black market to criminals who use them to break into computers. Hackers with networks of hacked machines can make money by selling them to spammers or phishers. They can use them to attack networks. We have started seeing criminal extortion over the Internet: hackers with networks of hacked machines threatening to launch DoS attacks against companies. Most of these attacks are against fringe industries—online gambling, online computer gaming, online pornography—and against offshore networks. The more these extortions are successful, the more emboldened the criminals will become.”).

R

⁷⁸ See Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group, (June 2004), <http://www.apig.org.uk/archive/activities-2004/computer-misuse-inquiry/CMARreportFinalVersion1.pdf> [hereinafter APiG Report].

⁷⁹ See Denise Pappalardo & Ellen Messmer, *Extortion via DDOS on the rise*, COMPUTERWORLD (May 16, 2005), <http://www.computerworld.com/printthis/2005/0,4814,101761,00.html>.

⁸⁰ See *infra*, text accompanying notes 93-126.

⁸¹ See Pappalardo & Messmer, *supra* note 79.

⁸² See *id.*

⁸³ See Stephen Baker & Brian Grow, *Gambling Sites, This Is A Holdup: Organized Criminal Hackers Threaten To Paralyze Their Networks If They Don't Pay Up*, BUS. WEEK, Aug. 9, 2004, at 60.

⁸⁴ See Pappalardo & Messmer, *supra* note 79.

⁸⁵ See Kevin Poulsen, *Feds bust DDOS “Mafia”*, THE REGISTER, Aug. 27, 2004, http://www.theregister.co.uk/2004/08/27/ddos_mafia_busted/ (Echouafni paid members of the “criminal underground” to launch attacks on three online competitor stores in Los Angeles, resulting in an estimated \$2 million in losses to them.).

R
R

R

distributed back to the teen hacker.⁸⁶

But perhaps the most disquieting threat posed by DDOS is to the information systems of critical infrastructure: hospitals, defense, transport, air traffic control, nuclear power stations, government, justice, and essential public utility companies such as electricity and water. It has been intimated that cyber warfare including DDOS has been used in conflicts such as Bosnia.⁸⁷ The threat DDOS might pose to national security is probably the most proximate reason why a requirement to create a distinct offense of “rendering inaccessible computer data . . . without right” has been imposed throughout Europe by the recent European Union Framework Decision on Attacks Against Information Systems.⁸⁸ The Council of Europe Cybercrime Convention, which is open to signatories outside Europe, also criminalizes “the serious hindering without right of the functioning of a computer system by inputting . . . data.”⁸⁹

II. LEGAL RESPONSES TO DoS AND DDOS

It is old news that there is a common pattern to how new threats associated with information technology are received by society. We have seen it with Internet pornography, with hacking, with the grooming of children in chat rooms, with spam, and now with DoS. It is rather like the psychological processes of grieving which are said to be denial, anger, despair, bargaining and acceptance.⁹⁰ The first reaction tends to be disbelief that the threat can really be this significant, or smug assertions that existing law is adequate to meet the challenge.⁹¹ The second reaction is dawning acceptance induced by growing evidence that something very bad really is happening, at which point a moral panic breaks out, accompanied by cries for new criminal offences and new laws to be passed (or heavier sentences added to those in existence).⁹² The third reaction is despair. Domestic criminal law in the UK and elsewhere is invariably inadequate to deal with Internet malfeasance launched from other jurisdictions and is, in any case, almost impossible to track down to their source. This is very much

⁸⁶ Stephen Labaton, *An Army of Soulless 1's and 0's*, N.Y. TIMES, June 24, 2005, at C1.

⁸⁷ For an example of one such unsubstantiated allegation, see Posting of CW to Balkan / Haimos Cafe Forums, <http://p208.ezboard.com/fbbalkansfrm20.showMessage?topicID=2.topic>.

⁸⁸ Council Framework Decision 222/JHA, art.5, 2005 O.J (L 69/69).

⁸⁹ Council of Europe, Convention on Cybercrime, art. 5, Nov. 23, 2001, 185 E.T.S. 5.

⁹⁰ See generally ELISABETH KÜBLER-ROSS, *ON DEATH AND DYING* (1969).

⁹¹ *Id.*

⁹² *Id.*

where we are with DoS and DDOS in the UK and Europe right now.

The contention of this paper will be that we need to move on from denial, anger and despair, though perhaps not as far as acceptance. We need to move past the inevitable knee-jerk call for new criminal offences to see if there are more effective ways to deal with the problem of DoS. In this section, we will first look at how UK law does and could deal with DDOS, looking at both criminal and civil law.

A. *Criminal Law*

Existing UK law specifically tailored to deal with computer crime is largely to be found in the Computer Misuse Act of 1990 (CMA).⁹³ As one of the earliest global legislative attempts to deal with computer crime, it was self-evidently not drafted for the Internet era.⁹⁴ As a result, although the Act deals fairly effectively with hacking and dissemination of viruses, doubts have arisen as to whether the CMA adequately covers DoS.⁹⁵

Two obvious routes exist within the CMA, which might be explored by those seeking to criminalize DoS. The first is section 1, originally designed to punish hacking, which prohibits “unauthorized” access to “any program or data”.⁹⁶ The other is section 3, designed to counteract the spreading of viruses, which prohibits any “unauthorized modification of the contents of any computer” which is intended “to impair the operation of any computer.”⁹⁷

As the APIG report notes, one of the problems with deciding if the CMA covers DoS is that the analysis of the differences between DoS and DDOS attacks has in many cases been muddy.⁹⁸ In “plain” or “vanilla” DoS, the only computer system affected is usually the target. The most obvious offense committed might seem to be unauthorized access. Yet as various commentators have pointed out, it is difficult to see the *access* that is perpetrated in DoS, harmful though it is in bulk, as “unauthorized”.⁹⁹ Websites that are not protected by passwords or other types of authentication are invariably regarded as impliedly authorizing,

⁹³ See generally Computer Misuse Act, 1990, c. 18. (Eng.).

⁹⁴ APIG Report, *supra* note 78, § 59 at 5.

⁹⁵ See *id.* § 22 at 5 (regarding hacking and viruses); see *id.* §§ 59-75 at 11-12 (discussing the efficacy of the CMA in prosecutions of DoS and DDOS attacks).

⁹⁶ Computer Misuse Act, 1990, c. 18, § 1 (1). (Eng.).

⁹⁷ See *id.* § 3 (2).

⁹⁸ APIG Report, *supra* note 78 at 9-12.

⁹⁹ Cf. *id.* at 9-10, ¶58.

indeed encouraging, third parties to “visit”—that is, make page and file requests.¹⁰⁰

One possible way out of this conundrum might be via the leading House of Lords case on authorization and the CMA, *R v. Bow St. Stipendiary Mag. ex parte Gov't of the United States* (“Allison’s Case”).¹⁰¹ In this case, Allison conspired with an employee of American Express to access confidential information in customer accounts for fraudulent purposes.¹⁰² The employee was authorized to view certain accounts assigned to her as part of her job, but also gave Allison information gleaned from other, similar, accounts to which she had not been assigned.¹⁰³ In a preceding case, *Director of Public Prosecutions v. Bignell*, a policeman who had legitimate access to the Police National Computer (PNC), but used that access to look up its records for a non-work-related purpose (to find out about his wife’s new lover) was found *not* to have committed an offense under section 1 of CMA as he had authorization to access the PNC, albeit for different purposes.¹⁰⁴ *Allison’s Case* was distinguished on the basis that the employee in question was authorized only to access certain accounts, not other similar data, even though her password facilities physically allowed her to do so.¹⁰⁵ This does not however go as far as saying that authorization extends only to the *purposes* for which it was given under section 1 of the CMA.¹⁰⁶ *Allison’s Case* therefore does not really solve the problem of whether Web sites might be seen as giving implied license to access for legitimate users but not to those attempting DoS attacks. T.J. McIntyre argues that an analogy might be drawn with English case law where a burglar can be accused of criminal trespass, if they enter to steal, even though they have permission to enter the building.¹⁰⁷ Such tentative analogies however are not likely to produce uniform results across different legal systems and

¹⁰⁰ In the U.S., attempts have been made to deal with the problem of third parties accessing Web sites for purposes undesirable to the Web site owner—for example, to collect prices on that Web site and put them into a competitive price-comparison site—via the common law concept of trespass. However these cases are in a state of flux, and many writers feel that the extension of trespass to cover access to intangible moveable property is undesirable and might effectively create monopolistic information rights by the back door which would not ordinarily be available via the intellectual property system.

¹⁰¹ [1999] 3 W.L.R. 620 (Eng.).

¹⁰² *Id.* at 622.

¹⁰³ *Id.* at 623.

¹⁰⁴ [1998] 1 Cr. App. Rep. 1 (Eng.).

¹⁰⁵ [1999] 3 W.L.R. 620, 628-30 (Eng.).

¹⁰⁶ *Id.* at 629.

¹⁰⁷ T.J. McIntyre, Computer Crime in Ireland: A Critical Assessment of the Substantive Law, http://www.tjmcintyre.com/resources/computer_crime.pdf (last visited Feb. 24, 2006); see also *Smith v. Jones* [1976] 63 Cr. App. Rep. 47 (Eng.) (the leading English criminal trespass case).

as such are not a very firm basis on which to build a criminal law of DoS.

What about section 3? Again, the commentators on the Act are split.¹⁰⁸ Section 3 as noted above requires unauthorized “*modification*” of the contents of the computer targeted for criminal liability to be imposed.¹⁰⁹ So first of all the issue of “authorization” arises again, and we will return to this below. But, secondly, is the server or system knocked down or slowed by DoS really “modified”? Section 3 was clearly drafted envisaging modification in terms of the type of damage a virus wreaks: deletion, over-writing and repetitive copying of data and programs. In DoS on the other hand, no alteration is made to the target computer system in *type* that would not be part of the ordinary legitimate expectations of the target; the difference is in volume, and in underlying motivation. The United Kingdom Internet Crime Forum legal subgroup reported to Parliament in 1993 that they thought that the test of “modification” could be satisfied where the attack had rendered the data stored on a computer unreliable or impaired its operation.¹¹⁰ Yet this seems a heavily purposive interpretation. A server that has suffered a DoS attack can be restored in a short period of time to full functionality, with no permanent damage or loss of data.¹¹¹ In the real world, the analogous offense might be locking a person in a room so they cannot get to work for a short while, compared with assaulting that person in a way that would leave lasting bruises or scars. Both should be crimes, but they are not the same crime and should not be so labeled.

Similar problems arise if we abandon the CMA and look to statutes relating to criminal damage in England or Ireland¹¹² or the common law of malicious mischief in Scotland.¹¹³ All seem to require some element of permanent damage to apply.¹¹⁴ The

¹⁰⁸ APiG Report, *supra* note 78 §§ 20-21 at 5.

¹⁰⁹ Computer Misuse Act, 1990, c. 18, § 3 (1) (a) (Eng.).

¹¹⁰ UK Internet Crime Forum legal subgroup.

¹¹¹ *Id.*

¹¹² See generally Criminal Damage Act, 1971 (Eng. and Wales); Criminal Damage Act, 1991, § 2(1) (Ireland); see also IAN J. LLOYD INFORMATION TECHNOLOGY LAW (4th ed. 2004).

¹¹³ See GERALD H. GORDON, GORDON'S CRIMINAL LAW ¶ 22-01 (Michael G.A. Christie ed., 2001), which glosses Hume to assert that malicious mischief can involve economic as well as physical damage to property. However, according to the case law, this seems only true where there is “unauthorized interference” involved, for example deflating a tire. So we are back to the problem of what is authorization? See also LLOYD, *supra* note 112. Lloyd seems to be of the opinion that the Scots law of malicious mischief is adequate to prosecute computer misuse.

¹¹⁴ See Burden and Palmer, *Cyber-crime—A New Breed of Criminal?* 19 C. L. S. R. 222 at 223 (2003); see also Shelley Hill, *Driving a Trojan Horse and Cart Through the Computer Misuse Act*, 14 J. SOC'Y COMPUTERS & L. 31 (2004).

R

R

recent introduction of a Private Member's Bill, which formulates an offense of denial of service without using the word "modification," lends weight to doubts that the current phrasing would securely support a prosecution.¹¹⁵ In the only UK prosecution for DoS thus reported, *R v Caffey*,¹¹⁶ the action prosecuted was charged as "unauthorized modification" under section 3 of the CMA, but there was no opportunity for argument as to the applicability of section 3 as the case fell on a "Trojan virus" defense, to be discussed below.¹¹⁷

The problems of defining "modification," and of transience of damage have both recently been addressed with some success in the latest reforms to section 3 of the CMA, made in the Police and Justice Bill of 2005 and still in Parliament at the time of writing.¹¹⁸ Clause 34 of the Bill amends section 3 by replacing the word "modification" with "act", which word is undefined save for including "a series of acts." In addition, section 3(2) of the CMA, as amended, will specify that the intent necessary to commit the crime exists whether the intention is to produce temporary or permanent impairment, or hindering or prevention of access to a computer, program or data.

But this still leaves the weasel word "unauthorized" to be considered. As noted above, it is difficult to assert that access to an open, non-secured website is "unauthorized" when the whole point of a website is to invite traffic and visitors. In section 3, is "modification", or even the new formulation of an "act" (such as the sending of email traffic or data or page requests) suddenly "unauthorized" simply because it is made in such volume, or in such aggressive ways, that the site suffers a DoS attack? If such traffic *is* to be deemed unauthorized, how is the law to separate "good" traffic from "bad" traffic when both look identical in type if not in volume?

This problem arose starkly in UK case law in the case of a teenage hacker charged with sending five million emails to cause a DoS attack against a former employer, in December 2005 at Wimbledon Magistrate's Court.¹¹⁹ The judge refused to find there

¹¹⁵ Computer Misuse Act 1990 (Amendment) Bill, 2005, Bill [102] (Eng.).

¹¹⁶ (Southwark Crown Court Oct. 17, 2003) (unreported, but discussed in Hill, *supra* note 114).

¹¹⁷ See *infra* text accompanying notes 132-142.

¹¹⁸ See Police and Justice Bill, cl. 33-36 (2006), at <http://www.publications.parliament.uk/pa/cm200506/cmbills/119/06119.27-33.html>.

¹¹⁹ See *Denial of Service Prosecution Fails*, OUT-Law.com News, Mar. 11, 2005, <http://www.out-law.com/page-6298> (last visited Apr. 18, 2006). The boy could not be named for reasons of age, and no formal report of the opinion exists.

was an offense under section 3, not because of any doubts about the applicability of the word “modification” but because, “In this case, the individual emails caused to be sent each caused a modification which was in each case an ‘authorised’ modification. Although they were sent in bulk resulting in the overwhelming of the server, the effect on the server is not a modification addressed by [the Act].”¹²⁰

The key issue, in other words, was the judge’s acceptance of the theory that an unsecured website impliedly authorizes the sending of emails to itself. Sadly, however, this result does not seem to have been apprehended by the drafters of the amendments in the 2006 Bill, which does nothing to clarify the question of “authorization” and indeed, makes matters worse, by stressing that the “knowledge” also required by section 3 is “knowledge that the act in question is unauthorized.”¹²¹

So far we have looked only at “vanilla” DoS. What of Distributed DoS? The problems above in general apply *mutatis mutandum* to the eventual attack on the target. Creating a zombie machine by infecting it with a virus or worm more clearly involves unauthorized modification in terms of section 3 since the contents of the zombie computer are clearly altered without knowledge or authorization.¹²² Arguably, there is also unauthorized *access* under section 1¹²³ made by the zombie-master to the zombie; but here we, again, run into problems of whether access can ever be either “authorized” or “unauthorized” when the infected computer in question has been left unsecured by firewall or other means (as will often be the case with zombified machines). The question is akin to asking if someone has broken into a house when they walk through an open door, but for the purposes of theft. The CMA says nothing of any requirement on victims to put security in place before “unauthorized access” can take place; and it is interesting to note that the EU Framework Decision on Attacks on Information Systems¹²⁴ merely allows, not requires, member states to put in place such requirements of minimum security before an offense is committed. In any case, since section 3 does not require proof of unauthorized access, a prosecution under section 3 for creating zombies should be sound even if the section 1 offense is mildly problematic.

¹²⁰ *Id.*

¹²¹ Police and Justice Bill, *supra* note 118, cl. 34 amending § 3(4) of the CMA.

¹²² Computer Misuse Act, 1990, c. 18, § 3 (2) (Eng.).

¹²³ *Id.*, § 1 (1).

¹²⁴ Council Framework Decision, *supra* note 88, at 11.

Which leaves UK law in the unsatisfactory state of apparently providing a route to prosecute zombie masters who perpetrate DDOS under section 3 and perhaps section 1—but not, it seems, villains who launch plain DoS attacks.¹²⁵ Even though DDOS attacks are likely to be the most crippling ones, as the APiG report suggests, “it is clearly undesirable to have the illegality of an attack depend upon the exact mechanism used.”¹²⁶ More annoyingly still, the amendments made by the Police and Justice Bill to secure a water-tight offense that could be prosecuted in cases of DDoS has failed to touch the main source of problems, the issue of when an act under section 3 is “authorized” or not.

More generally, the analysis above illustrates how difficult it is to criminalize an activity such as plain DoS whose *actus reus* is *prima facie* legal. But if intent is the crucial *sine qua non* of DoS, then particular problems relating to intent arise which may make DoS almost impossible to satisfactorily prosecute.

B. DoS and Intent: the “Possessed by Aliens” Defense

First, as the APiG report recognized, a sloppily drafted DoS statute might easily criminalize innocent actors who non-maliciously provoke a DoS attack.¹²⁷ It is not uncommon for a popular source to publicize a particular website or phone number as containing interesting content; several thousand people then typically visit it quickly, and that site or phone line crashes.¹²⁸ These innocent crashes are commonly known as “slashdots” after the on-line computer-culture journal of the same name. The 2002 Private Member’s Bill introduced by Lord Northesk to add a specific DoS offense to the existing CMA provided that a person was guilty who had committed the *actus reus* even if the act was “not intended to cause such an effect, provided a reasonable person could have anticipated [it] could cause such an effect.”¹²⁹ Such an objective formulation of intent was intended to deal with the

¹²⁵ It is noticeable that the only UK prosecution so far which has been publicized as a prosecution of DoS, *R v Caffrey*, (see Hill, *supra* note 114, at 13), was, according to the testimony of Professor Neil Barrett, the computer forensic expert involved, no such thing. Barrett wrote to APiG to make this clear. According to Barrett, Caffrey, the accused, allegedly took control of the Port of Houston computer system with intent to launch a DDOS attack on an unknown third party target. As a result of this, the Port of Houston computer system crashed. Thus as Barrett says, “we have not yet had a case of DoS argued under section 3 of the 1990 Act.” See *Feedback on CMA Inquiry and Report*, at <http://www.apig.org.uk/archive/activities-2004/feedback-on-cma-inquiry-and-report.html>.

¹²⁶ APiG Report, *supra* note 78, § 66 at 11.

¹²⁷ *Id.* § 67-70 at 11.

¹²⁸ *Id.* § 69 at 11.

¹²⁹ See text of Bill (which fell) at <http://www.parliament.the-stationery-office.co.uk/pa/ld200102/ldbills/079/2002079.htm>.

R

R

scenario where it cannot be easily proven that the zombie master actually intended to cause harm, as opposed to mere “innocent” hacking. But such an objective intent element may catch innocent slashdotters as well as manipulative zombie masters.¹³⁰

A purely subjective approach to intention also however has problems. If DoS is a crime largely performed by innocent zombies, how easy is it to tell in court the difference between the zombies and the zombie master?

Suppose A is accused of DoS. It is very easy to claim that the seemingly malicious acts perpetrated by A’s machine were actually not done under the control of A, but of malicious code which had infected that machine and which had initially been spread by B, who is thus the true offender. Code such as “Trojan viruses” effectively take control of a computer and cause it to perform unexpectedly when certain ordinary programs such as the email program are operated. This was exactly the defense raised in the only reported UK denial of service prosecution thus far, *R v Caffrey*.¹³¹ Caffrey apparently launched an attack against the Port of Houston computer system, which had the effect of preventing access to that port’s information by shipping, mooring and support services.¹³² Caffrey alleged that a Trojan virus was responsible and it was not his intent to cause such damage.¹³³ The jury accepted this plea, despite the fact that there was no trace of the Trojan virus left on his computer when it was searched by police.¹³⁴ Caffrey however claimed that the Trojan was self-deleting after it had performed its task, and though the prosecution claimed such technology did not exist, it presumably raised enough of a reasonable doubt for the jury to reject the charge.¹³⁵

Realistically, Caffrey’s claim is somewhat analogous to a murder case where the accused claims that he performed the act but only while possessed by aliens, or perhaps more likely, while sleepwalking. Such cases do come up, and tend to be dealt with sensibly, by a mixture of assessment of credibility, medical evidence and, where appropriate, some degree of substitution of an objective for subjective intention test.¹³⁶ Yet when we move from

¹³⁰ APIG Report, *supra* note 78, § 69 at 11.

¹³¹ Southwark, *supra* note 116.

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ *Id.*

¹³⁶ See ANDREW ASHWORTH, PRINCIPLES OF CRIMINAL LAW 99 (4th ed. 2003), for a discussion of automatism including somnambulism. Somnambulism currently seems to be treated as founding the defense of insanity in English law. See *R v Burgess* [1991] 2 Q.B. 92.

the discourse of medicine to that of computer science, it seems the average jury is likely to be sufficiently out of its depth to give the accused the benefit of the doubt. In another UK computer hacking prosecution, *R v Bedworth*,¹³⁷ a jury refused to convict a student hacker on the grounds that he was “addicted to hacking”. Since the UK legal systems do not in general allow intoxication by drugs or alcohol to invalidate a charge (as opposed to mitigate sentencing), the jury’s readiness to accept this defense seems illogical. At the time of *Bedworth*, in 1993, there was some speculation that the jury did not take hacking seriously and were reluctant to convict a young person for what was seen as “high jinks”.¹³⁸ Neither factor would seem to hold in the case of *Caffrey*, heard in 2005.¹³⁹ It may be as Hill suggests, that successful prosecution of subjective intent-based computer crimes may be incompatible with jury trials, and may even demand the introduction of specialized computer courts or expert judges.¹⁴⁰ Alternately, sufficient expert evidence may resolve the issue; in *R v Caffrey* it has been suggested that the judge was not allowed access to all the expert evidence early enough in the proceedings, and that an early expert’s meeting might have led to the “Trojan virus” defense not being put before the jury at all.¹⁴¹

Several Private Member’s Bills designed to refine the law of DoS, introduced by Derek Wyatt in 2005, and the Earl of Northesk in 2002¹⁴² failed, perhaps understandably, to address the problems of intent raised by *Caffrey*. It is less comprehensible why the Police and Justice Bill amendments drafted *since* the *Caffrey* case also fail to do anything to deal with this issue.

C. Civil Law

As we have seen above, the nature of DoS and DDOS as intent-based crimes will always make it difficult both to prosecute them and to draft effective laws criminalizing them. A wider problem is whether the criminal law is the best approach to challenging the social problems caused by DoS. High tech crime investigation

¹³⁷ 1993, England and Wales, unreported. See a journalistic account at http://www.eff.org/Net_culture/Hackers/uk_court_acquits_teenage_hacker.article.

¹³⁸ See Andrew Charlesworth, *Legislating against computer misuse*, J.L. & INFO. SCI. 80 (1993).

¹³⁹ *R v. Caffrey*, (Southwark Crown Court Oct. 17, 2003) (unreported, but discussed in Hill, *supra* note 114).

¹⁴⁰ Hill, *supra* note 114.

¹⁴¹ See Clive Carmichael-Jones, *Trojan Horses Complexities*, COMPUTERS & LAW 33 (Dec. 2003/Jan. 2004).

¹⁴² Computer Misuse Act 1990 (Amendment) Bill, 2005, Bill [102] (Eng.). Computer Misuse (Amendment) Bill, 2002, H.L. Bill [79] (Eng.).

resources are highly limited in the UK,¹⁴³ and the resources needed for technical training of ordinary policemen are vast. As the APIG report and many other commentaries note, DoS attacks are most often controlled from foreign jurisdictions not the domicile of the target, most commonly Russia, so investigation, prosecution and enforcement become even more difficult.¹⁴⁴ Finally, there has long been anecdotal evidence that most large corporate targets would in any case prefer to deal with DoS attacks in-house than expose themselves to bad publicity for poor security by bringing in the police.¹⁴⁵

A law and economics perspective might suggest that if public resources to crack down on computer crime are thinly stretched, and if the criminal law is in any case ineffective and inappropriate, perhaps a solution—or supplementary solution—should be found in the civil law instead.¹⁴⁶ Arguably the market can help control DoS if individual targets—usually corporations with considerable legal and financial resources—are given rights to sue those who create the hazard of DoS in the first place. The costs of enforcement and suppression are thus transferred from the public to the private sector, which has a serious interest in stamping out DoS.

But the question of who to sue remains. As noted in the introduction, DoS and especially DDOS involve a complicated mesh of actors, not just the target and perpetrators. Chandler identifies five parties who might be considered as partly responsible for, or complicit in, every DDOS attack:¹⁴⁷

- the targets or victims themselves;

¹⁴³ As an example, the Scottish High Tech Crime Unit, which is part of the Scottish Drugs Enforcement Agency, was designed on set up in 2003 to number ten staff. Even this required a budget of £700,000 in 4/2003.

¹⁴⁴ See APIG Report, *supra* note 78, at 10.

¹⁴⁵ The UK NHTCU/NOP e-crime survey of 2005 found that 64% of those interviewed said they would involve the police if affected by hi-tech crime. However other questions in the survey suggest that they would mainly involve the police only in cases of financial fraud or physical theft of equipment, not denial of service. 69% of respondents said they were worried about the effect a hack attack might have on their business, while only 17% said they were worried about the damage it might have on their reputation. However one might cynically suggest that these responses were disingenuous. Computer security experts suggest that the major corporate motivation to report high tech crime to the police is not a sense of public duty or a hope the perpetrators will be caught, but the need for police involvement to be shown before an insurance claim can be made. However only 14% of the respondents in the NHTCU survey said this was their main motivation, as opposed to 43% who said they primarily wanted an investigation to take place. See NHTCU Survey, *supra* note 55.

¹⁴⁶ See Paul Barton & Viv Nissanka, *Cyber-crime—criminal offence or civil wrong?*, 19 COMPUTER LAW & SEC. REPORT 401 (2003).

¹⁴⁷ Chandler, *supra* note 44, at 240. This is the leading scholarly contribution on legal regulation of DDOS thus far.

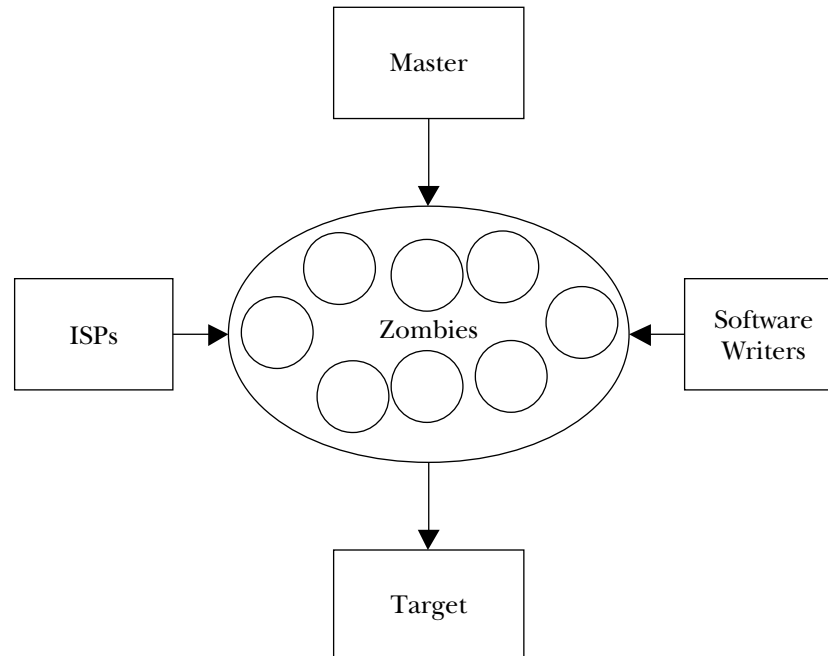
R

R

R

- the criminal or “zombie master;”
- the “zombies” or potential zombies, i.e., “ordinary” Internet-connected computer users;
- the Internet Service Providers (ISPs) who provide Internet access to potential zombies and to the target;
- the software developers who provide the software whose insecurities are exploited both in the creation of “zombies” and in the ultimate DoS attack on the target.¹⁴⁸

FIGURE 2: ACTORS IN DDOS



The obvious party for the target to sue is the zombie master. Yet in many or most cases this party will be difficult to identify using computer forensic evidence, and even if proof of identity can be found, effective legal action may be extremely difficult to take against either criminals lurking in foreign jurisdictions or teen hackers with few or no resources. Just as it is difficult to prosecute zombie masters under criminal law, civil law actions are also likely to be ineffective in curbing their activities. As in many other areas of commercial law, targets will be tempted to write off the actual rogue as a lost cause, and go looking for other, hopefully deeper and more accessible, pockets to sue.

¹⁴⁸ *Id.*

1. Sue the Zombies?

To this end, a number of commentators have suggested that, in an evocative phrase, the targets of DDOS should “blame the victims.”¹⁴⁹ As we have seen, DDOS cannot be carried out without networks of zombie drones. Can a case be made for the targets of DDOS to sue the zombies, even though the zombies are themselves innocent and unknowing victims? The basis of such a claim would have to be that the zombie-machine owners owed a duty of care to the ultimate targets to keep their computers safe from zombification. In other words, can a civil duty of adequate security be imposed upon every Internet user whose computer is connected to the Internet some or all of the time? So far there are no reported or even publicized legal cases of this kind, though anecdotal accounts do circulate of tentative moves in this direction.

In policy terms, reducing the insecurity of the general Internet-using public would clearly be a decisively helpful step to stamping out DDOS. Internet security can be seen as a community problem. As the influential Computer Emergency Response Team (CERT) Advisory CA-2000-01 states, “security on the Internet is a community effort.”¹⁵⁰ It is well known that many home Internet users, especially those connected “always-on” to broadband, fail to take elementary security measures due to a mixture of inertia, technophobia and ignorance. It is not just home users who are guilty here—university computers have also in the past often been used as zombie networks due to a lack of corporate-level security and easy public access, as have machines belonging to small companies. The NHTCU/NOP survey for 2005 found that even its corporate respondents failed on the whole to take important security precautions: only 33% carried out regular security audits and only 34% did audits that complied with recognized British or ISO standards for information security.¹⁵¹ As noted earlier, a zombie drone usually experiences very little degradation of service when used in a DDOS attack, so there is little incentive for the user

¹⁴⁹ See Stephen E. Henderson & Matthew E. Yarbrough, *Frontiers of Law: The Internet and Cyberspace: Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11 (2002); see also Carl S. Kaplan, *Can Hacking Victims Be Held Legally Liable?*, N.Y. TIMES, Aug. 24, 2001, *Cyber Law Journal* (citing Margaret Jane Radin, *Distributed Denial of Service Attacks: Who Pays?* (pts. 1 & 2), *CYBERSPACE LAWYER* (Dec. 2001/Jan. 2002)).

¹⁵⁰ Jerry Wegman & Alexander D. Korzyk, *Internet Denial of Service Attacks: Legal, Technical and Regulatory Issues*, 7 J. LEGAL, ETHICAL AND REG. ISSUES (2004), <http://www.cbe.uidaho.edu/wegman/blaw265/DOS%20paper%20AA%202003%20web.htm> (citing the CERT advisory.)

¹⁵¹ NHTCU Survey, *supra* note 55.

to take security measures in their own interests, as opposed to in the public good.¹⁵² An imposition of legal liability might provide that incentive. Furthermore, suing zombies is appealing for the targets of DDOS attacks since the zombies used to mount the DDOS attack are likely to be in the same jurisdiction and legal system as the victim; while the zombie master is more than likely not to be. The IP addresses of the zombies used in the DDOS attack should be easily loggable on the target computer system, while the zombie master will be extremely difficult to identify. The zombies are likely to be law abiding citizens who will respond to legal action and pay up if found liable in damages, while the zombie is rather more likely to evade such civil duties; some zombies may even prove conveniently to have “deep pockets.”¹⁵³

Yet it is difficult to find an ethical basis for blaming the zombies for the sins of the zombie masters. Individual users are unsophisticated and ill resourced to keep up with the requirements of maintaining home PC security. It is unlikely that even the possible danger of legal liability would encourage some, such as the very young, the very elderly, the very busy and the unskilled, to maintain their machines in good secure order. For many users, a home computer is now the equivalent of a TV rolled in with a DVD player and a home music center. Such users no more expect to have to keep their PC secure than they do their TV. To impose liability on these and not on their better resourced or technologically more able brethren would be, currently at least, to create a tax on ignorance and technophobia. As we have seen, even SMEs have trouble maintaining the security of their machines, let alone individuals.

As Chandler notes, the problem lies not just with home users, but also with the software they run—which is overwhelmingly supplied by the quasi-monopolistic market leader, Microsoft.¹⁵⁴ Commonly used programs such as Microsoft Windows, Internet

¹⁵² See *supra* note 12 and accompanying text.

¹⁵³ This raises the question of what recourse zombies sued for breach of duty of care might have *inter se*. Suppose target X is the subject of a DDOS attack launched by a network of 10,000 zombies. One zombie, A, is identified as a corporate server whose company has substantial assets. Should target X be entitled to sue A for the whole of the substantial losses it has incurred as a result of DDOS just because A was contributory to the loss and is a “deep pocket?” This would certainly be easier for X than suing 10,000 zombies. Should A’s damages be restricted to 1/10,000th of X’s losses? Should all zombies have some kind of joint and several liability, with A forced to sue other zombies for their contributory negligence to recoup the part of the damages for which they are liable? The answers to these questions will vary from jurisdiction to jurisdiction according to their rules on contributory negligence and class actions, which is an unfortunate answer given that DDOS will almost always involve trans-border issues.

¹⁵⁴ Chandler, *supra* note 44, at 244.

Explorer, and Microsoft Outlook are frequently infected by malware via security holes.¹⁵⁵ The problem is that these programs were, historically, not designed with security as an integrated element, prioritized during the design process, but have had it added by “bolt-on” patches as security holes have been discovered and exploited by hackers and criminals.¹⁵⁶ Constant “patching” is necessary via the download and installation of software patches. Not only is this process of “patching” confusing and burdensome for many home users, but patches themselves sometimes interfere with the workings of the programs already on the machine. For this reason many more sophisticated users are wary of installing patches, and especially the periodically issued large-scale fixes known as “service packs.” One of the solutions to home user machine insecurity would be to automate patching, so that a new patch is installed over the Internet connection to the home user whenever issued; and this is indeed exactly what the latest version of Windows, Windows XP, does. The newest version of Windows, due for release in late 2006 and provisionally now entitled Vista, promises still more: according to Microsoft, it will represent “a completely new approach to computing, with security not an add-on but an integral part of the operating system.”¹⁵⁷ The details of how this will be done remain unclear at date of writing, but it seems likely that the way Vista will work will be to introduce a more effective and UNIX-like security protocol which will, however, decrease ease of use for unsophisticated users. The problem remains that many users are not up to date with Windows XP, and are either ignorant of its existence or unwilling to spend the money and effort to upgrade. These problems are likely to persist when Microsoft Windows Vista is released. The loss of convenience will also not entice newer users.

Legally, imposing a duty of security on home users raises more problems than it solves. Under the common law of negligence, a novel duty of care is only usually imposed by the courts where it is reasonably foreseeable that a failure in that duty would cause damage to the person to whom the duty is owed, and where there is no good policy reason to reduce or limit that duty. This can also be seen as a “proximity” test.¹⁵⁸ Does a home PC user really foresee

¹⁵⁵ *Id.*

¹⁵⁶ *Id.* at 248.

¹⁵⁷ See BBC News, *Vista opens on Microsoft Windows*, July 22, 2005, <http://news.bbc.co.uk/1/hi/business/4708177.stm>.

¹⁵⁸ The general law of negligence cannot conceivably be summarized in this paper but the leading case discussing when the courts will recognize a new type of negligence throughout most Commonwealth jurisdictions and formerly England and Scotland is *Anns*

that their failure to install Microsoft patches will lead to WorldPay being taken out by a DDOS attack? Should they reasonably be expected to do so? Is there really a proximate relationship between every Internet home user and every other Internet-connected machine? What about causation? If a home user's computer is insecure, but the machine is then infected by a worm distributed by a third party, is there a break in the chain of causation? Or alternately, given the statistic quoted earlier that an unprotected home machine in the UK will have a 50% chance of infection within 12 minutes, is infection also reasonably to be foreseen?¹⁵⁹

Even if the problem of reasonable foreseeability is overcome, there are still policy reasons why the courts might not wish to impose a duty of care on the home user. The loss suffered by the target is likely to be characterized as pure economic loss (remembering again that servers hit by DDOS suffer no permanent damage and the loss is thus merely to profits and not to property). The common law courts have generally been loath to expand the categories of negligence by imposing duties to prevent pure economic loss, for obvious reasons that this might "open the floodgates" to claims.¹⁶⁰ In the U.S., the recent case of *Bell v Michigan Council*¹⁶¹ did indeed for the first time impose liability at common law for inadequate security in relation to information. The facts were however significantly *sui generis*.¹⁶² The defendant was a trade union of which the plaintiffs were mandatory members.¹⁶³ Due to lack of security by the trade union, personal information was stolen regarding members by a third party, which led eventually to financial and emotional losses to members due to identity fraud.¹⁶⁴ In this particular case, the court was willing to hold that the harm of someone misusing the plaintiff's personal

v. Merton London Borough Council, [1978] A.C. 728. *Anns* is seen in England as a high water point of the extension of liability for negligence. A later formulation in *Murphy v. Brentwood District Council*, [1991] 1 A.C. 398, held that it had to be fair, just, and reasonable to impose a novel duty. This author's view is that this would be a very difficult test to meet in the case of zombies and targets.

¹⁵⁹ By no means will every *novus actus interveniens* between tortfeasor and ultimate victim break the chain of causation. See *The Oropesa* (1943) 1943 1 All ER 211 (CA) at 32.

¹⁶⁰ This is also an extremely complex topic. See *Hedley Byrne & Co. Ltd. v. Heller & Partners, Ltd.* [1964] A.C. 465, and more recently, *White v. Jones* [1995] 2 A.C. 207.

¹⁶¹ *Bell v. Mich. Council 25 of the AFSCME*, No. 246684, 2005 Mich. App. LEXIS 353 at *1 (Feb. 15 2005).

¹⁶² *Id.* at *2-3.

¹⁶³ *Id.* at *2.

¹⁶⁴ *Id.* It should be noted that the information taken was in the form of data written in a notebook, which was stolen by the daughter of the treasurer of the Union, who then used it for criminal purposes. There was no electronic information storage in this case.

information was foreseeable by the union, and that the union did thus owe a duty of adequate security to its members.¹⁶⁵ But this duty arose because of the “special relationship” of proximity between the plaintiffs and the defendant, and the fact that the defendants were compelled to release their personal details to the union.¹⁶⁶ Such a duty would not hold in every case where a third party obtains personal data from an information holder due to insecurity by that host, and subsequently uses it to commit the crime of identity theft.¹⁶⁷

Even if the courts are willing to impose a duty of care, how much must an individual do to fulfill it? It is surely unreasonable to expect any user to provide absolute security given the insecure state of both the Internet and the dominant software most machines run, so the most likely formulation would be some duty of reasonable or adequate security. So what is “adequate security”? Here, the technology industry may be able to assist, since international ISO standards do exist for computer and information security. Barton and Nissanka reported in 2003 that the DTI was considering whether to impose a requirement to implement ISO/IEC17799:2000, an entry-level framework for information security, upon UK business.¹⁶⁸ The fact that the DTI has apparently not pursued this for commercial users makes it seem unlikely that it is plausible to impose such conditions upon *home* users, both in terms of costs of compliance for users, and costs of enforcement by (for example) the Information Commissioner.

A better alternative to a common law duty of security might be to look to existing special statutory duties. The EC Data Protection Directive (DPD)¹⁶⁹ already imposes a duty of security on data controllers processing personal data, under the Seventh Data Protection Principle. Not every home computer will however contain personal data, and thus not every home user will be a data controller and fall under the DPD umbrella. In any case, the duty of security is owed to the persons whose personal data is made insecure and who consequentially suffer harm,¹⁷⁰ not to the victims of DDOS imperiled by the information holding computer *itself*. The DPD route thus is of little help. A more radical alternative might be to impose some kind of “home MoT” test on computer

¹⁶⁵ *Id.* at *12.

¹⁶⁶ *Id.* at *16.

¹⁶⁷ Bell v. Mich. Council, at *16-17.

¹⁶⁸ Barton & Nissanka, *supra* note 146.

¹⁶⁹ Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

¹⁷⁰ See Data Protection Act, 1998, c. 29, s. 13 (Eng.).

owners.¹⁷¹ Just as UK car owners must have their car certified every year as fit to be on the road after a certain period, home PC owners with broadband connections might be required to have their PC checked out as secure—say, every six months. “Computer MOT inspectors” could visit homes, just as television license inspectors do currently. But whereas the MoT system is well enforced by the need to show MoT to get an annual tax disc, which is itself monitored by computer records as well as public inspection of cars on the road, and television reception can be monitored from external vehicles, it is hard to see how compliance with “home security tests” for computers could be enforced without gross violation of normal standards of household privacy. It is also unlikely anyway that even if provided with VAT Inspector-like powers of ingress, home computer “MoTs” could be carried out frequently enough to keep up with exploitation of security holes by malware writers. Imposing legal duties of care on home users thus seems *in toto* to be impractical and unenforceable as well as unjust.

2. Sue the Software Writers?

Chandler’s preferred solution to DDOS is to place a duty of care on the companies that produce the insecure software used by the majority of users.¹⁷² She argues that the leading software which dominates the consumer and business markets is systemically insecure, because the software industry is fixated on providing complex features (“feature creep”) and getting the product to market on deadline, at the expense of security as a priority.¹⁷³ Imposing legal liability for insecurity owed to the victims of that insecurity might force the software writers to re-assess these priorities. She has considerable support on this point from the software industry itself, and computer security experts, notably the leading cryptographer Bruce Schneier, who has argued repeatedly that just as manufacturers are liable for flaws in their products, so software writers should similarly, be liable for “buggy software.”¹⁷⁴ Schneier complained in 2003, “It’s crazy that Firestone can produce this tire with a systemic flaw and they’re liable, whereas Microsoft produces an operating system with two systemic flaws per week and they’re not liable.”¹⁷⁵

¹⁷¹ I am indebted for this suggestion to Richard Jones of Liverpool John Moores University.

¹⁷² Chandler, *supra* note 44, at 243.

¹⁷³ *Id.* at 248.

¹⁷⁴ *Id.*

¹⁷⁵ See Todd Bishop, *Should Microsoft be liable for bugs?*, SEATTLE POST-INTELLIGENCER, Sep. 12, 2003, http://seattlepi.nwsourc.com/business/139286_msftliability12.html.

Software writers can in theory be liable either in contract or in tort for their products. In terms of contractual liability, software companies habitually protect themselves from liability via exclusion clauses, which are invariably accepted by buyers (or more accurately, licensees) of the software as part of shrink-wrap or click-wrap contracts.¹⁷⁶ Such exclusion clauses may however be subject to challenge in some jurisdictions on grounds such as consumer unfair term protection,¹⁷⁷ or general doctrines of unconscionability. Most actions in contract or negligence for software defects do tend to revolve around the validity or non-incorporation of exclusion clauses.¹⁷⁸ However, even without benefit of exclusion clauses, software writers will tend to put in place enough testing, design and specification routines in relation to security to defend themselves against charges of breach of express or implied terms of quality under contract; such routine measures of due diligence will also protect against actions under common law negligence. By contrast however, those who produce manufactured products are in some jurisdictions subject to *strict* liability, which cannot be excluded by contract, albeit with defenses available such as the argument that the product was “state of the art” and therefore could not be 100% guaranteed safe.¹⁷⁹

Yet imposing some kind of strict liability on software writers, as Schneier and his supporters might prefer,¹⁸⁰ also seems an inequitable and impractical solution. Software development is a highly complex, massively distributed and incremental process. Software can be, and is, tested for bugs and flaws, but operates in so many different environments, with so many different combinations of other programs, data and users that 100% safety is simply impossible to guarantee. Put simply, a software program is not a car tire and cannot be guaranteed to be 100% or even 95% safe as a car tire can be in normal use on every imaginable type of road. Furthermore, there is no industry of third parties attempting to reduce the safety of tires once they have left the factory—whereas a panoply of hackers exist whose main *raison d’être* is to

¹⁷⁶ See, e.g., *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

¹⁷⁷ See The EC Unfair Terms in Consumer Contracts Directive, Council Directive 93/13, 1993 O.J. (L 095) 29; Unfair Contract Terms Act, 1977, c. 50 (Eng.), and Unfair Terms in Consumer Contracts Regulations, 1994, S.I. 3159 (Eng.).

¹⁷⁸ See *St. Albans City and District Council v. Int’l Computers Ltd.* [1995] F.S.R. 686 (Q.B.); *Beta Computers (Europe) Ltd. v. Adobe Sys. (Europe) Ltd.* [1996] S.L.T. 604 (O.H.).

¹⁷⁹ See the EC Liability for Defective Products Directive, Council Directive 85/374, 1985 O.J. (L 210) 29 (EEC), implemented in the UK by the Consumer Protection Act, 1987, c. 43.

¹⁸⁰ Chandler, *supra* note 44.

discover security holes in software. Schneier argues that if liability did rest at least in part with software companies, then just like firms in other industries, they would turn to buying product liability insurance.¹⁸¹ Insurance companies would in turn respond by pricing the risk, in effect voting on the security of each product.¹⁸² In theory, this sounds good. However, given the current monopolistic market for software, what this would mean is that effectively around 90% of the risk of network insecurity would fall on Microsoft. At that level of risk, would insurance be available, and if so, at what premium? If the cost of that premium was then passed on to the public, what would happen to the price of a copy of Windows XP, currently £61 / \$199 for a home user? Effectively the costs of software insecurity, currently shared between a large number of vulnerable targets and users, would be loaded on to a few major software writing companies, which might indeed in the long term provide considerable incentives for safer software, but in the short term might lead to rapid destabilization of the economics of producing software, with catastrophic consequences for Internet access and commerce.¹⁸³

In Europe, it is controversial whether software *per se* as opposed to software which is incorporated within a tangible “product” such as a car, a refrigerator or an air traffic control system, falls within the existing strict liability regime of the EC Product Liability Directive.¹⁸⁴ “Product” is defined in Art. 2 of the Directive as including all moveables, and electricity, but in the UK Consumer Protection Act 1987, implementing the Directive in the UK, this is interpreted rather differently as “goods and electricity.”¹⁸⁵ Even if included, software writers might well escape liability under what is known as the “development risk” defense, which allows a producer to claim that “. . . the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered.”¹⁸⁶ Given the energy with which hackers seek security holes once a major software product is released, this would seem a plausible defense for software writers, and may explain the lack of any cases brought against software under the Directive thus

¹⁸¹ Schneier, *infra* note 198, at 19.

¹⁸² See *Fighting the worms of mass destruction*, ECONOMIST, Nov. 27, 2003, http://www.economist.com/displayStory.cfm?story_ID=2246018.

¹⁸³ One might also ask, parenthetically, what effect such liability might have on the fledgling open source software industry.

¹⁸⁴ See IAN J. LLOYD, INFORMATION TECHNOLOGY LAW § 27.46, (4th ed., 2004).

¹⁸⁵ Consumer Protection Act, 1987, c. 43, s. 1 (Eng.).

¹⁸⁶ Council Directive 85/374, art. 7(e), 1985 O.J. (L 210) 29 (EEC).

far.¹⁸⁷ Crucially, also, the Directive is a piece of consumer protection legislation;¹⁸⁸ the only damage that can be claimed for is personal injury, or damage to property of a kind ordinarily intended for private use or consumption, and so used. Product liability law as currently constituted thus will never provide a remedy in the overwhelming majority of cases of denial of service which are launched at commercial or public sector websites and computer systems.

Even if the Product Liability Directive were to be broadened, the economic policy behind the argument to place liability on software writers also seems flawed. Chandler argues that the market has failed to persuade Microsoft to prioritize security, or rather to design products with “the optimal balance of price and quality (including security characteristics.)”¹⁸⁹ She cites three reasons for imperfect market operation: a non-competitive monopolistic market for software; purchasers are often too ignorant to accurately assess themselves the price/security balance in software products; and purchasers, especially consumers, do not themselves suffer the costs of insecurity—for as was already noted, it is largely not the zombies that suffer in DDOS attacks but merely the targets.¹⁹⁰

But there is considerable evidence that at least the first two of these three reasons no longer hold. Microsoft itself, as noted above, has been forced by considerable public backlash and outcry to prioritize network security in *Vista*, its new version of Windows. Although the technical details are not yet available, the pre-launch publicity clearly indicates that the market is forcing Microsoft to sell *Vista* as above all, a secure product.¹⁹¹ Furthermore, this public and corporate awareness of Microsoft as a purveyor of network insecurity is affecting the monopoly characteristics of the market. For example, the overwhelming majority of users may still use Internet Explorer, but more sophisticated users are noticeably moving to competing browsers like Safari and Firefox, running on competing hardware such as Macintoshes, specifically to avoid the bugs, viruses and spyware which tend to be tailored only to Microsoft products.¹⁹² Similarly, uptake on open source products

¹⁸⁷ Council Directive 85/374, 1985 O.J. (L 210) 29 (EEC).

¹⁸⁸ *Id.*

¹⁸⁹ Chandler, *supra* note 44.

¹⁹⁰ *Id.*

¹⁹¹ See BBC News, *supra* note 157.

¹⁹² *Browser News* reports that as of July 23, 2005, the percentage of users using Internet Explorer in its variants is down from a high of around 94% to 84%. The number of Internet Explorer users dropped for the first time in June 2004, with a switch to rival

such as Linux is being driven by perceived quality advantages as well as price, and not least the fact that these products tend to be perceived as bug-free compared to Microsoft packages. The HoneyNet Project, for example, found that an unpatched Linux system left open to attack would be compromised in around three months whereas a similar Microsoft system would be attacked within hours.¹⁹³ Furthermore, while Microsoft product security declined over time, as hacking efforts were concentrated on the most popular software products, Linux security had contrarily improved enormously over the last two to three years due to efforts made to improve it.¹⁹⁴

The final and key point as to why imposing liability on software writers for insecure software would not solve the zombie horde problem is that, as already mentioned above, if home users are slow to install free patches on their systems, they will certainly be even slower to upgrade to new, more secure versions of Windows (and other key applications) which cost actual money. Windows XP, as we have seen,¹⁹⁵ already solves some security problems via automated patching, but many users—not only consumers, but universities, public sector bodies and SMEs—are unwilling to go through the effort and cost of full scale upgrade to XP. The same pattern will undoubtedly be seen with Windows Vista. Even if Microsoft was, unlikely as it would seem, to be persuaded to offer free upgrades to all existing legitimate Windows customers, there would still be many users unwilling or unable to manage the logistics of an upgrade, plus many users running illegal or pirate copies, who would not be eligible for upgrades.¹⁹⁶

The problem, as Schneier and other colleagues have also identified, is not simply that the market drives Microsoft towards preferring speed and content features to security, but that Microsoft's dominance of the software market has produced a software monoculture where viruses and worms can be easily bred

browsers such as Safari, Mozilla and other "Gecko-based" browsers most visible among more sophisticated users. See http://www.upsdell.com/BrowserNews/stat_trends.htm (last visited Feb. 15, 2006).

¹⁹³ See HoneyNet Project, *supra* note 35.

¹⁹⁴ See Greg Keizer, HoneyNet Project Finds Updated Linux PCs Stay Secure Online for Months, Dec. 23, 2004, <http://www.techweb.com/wire/security/56200327>.

¹⁹⁵ See *supra* note 161 and accompanying text.

¹⁹⁶ It can be interestingly noted that Microsoft announced on July 26, 2005, that they would no longer provide free updates to Windows XP to users who could not prove the copy they were running was not a pirated copy. This was announced as part of Microsoft's ongoing anti-piracy campaign. Lucy Sherriff, *Fakers Beware: No More MS Updates for You*, July 26, 2005, http://www.theregister.co.uk/2005/07/26/ms_updates_wga_launch/.

R

R

and have enormous global impact.¹⁹⁷ A recent report on cyber-insecurity and the costs of software monopoly argues that:

Most of the world's computers run Microsoft's operating systems, thus most of the world's computers are vulnerable to the same viruses and worms at the same time. The only way to stop this is to avoid monoculture in computer operating systems, and for reasons just as reasonable and obvious as avoiding monoculture in farming. Microsoft exacerbates this problem via a wide range of practices that lock users to its platform Because Microsoft's near-monopoly status itself magnifies security risk, it is essential that society become less dependent on a single operating system from a single vendor if our critical infrastructure is not to be disrupted in a single blow. The goal must be to break the monoculture. Efforts by Microsoft to improve security will fail if their side effect is to increase user-level lock-in.¹⁹⁸

These kinds of problems have of course already emerged in more immediately commercial contexts than that of computer security. Attempts have been made in both the U.S. and the EU to tackle what are seen as Microsoft's monopolistic "lock-in" practices, such as bundling application with operating system software, with some but rather limited success.¹⁹⁹ Even the monoculture report cited above does not recommend breaking up Microsoft, as was much discussed before the U.S. and EU antitrust cases, but rather seeks to allow rival developers greater access to Microsoft's platforms and programs so as to create a software "biodiversity."²⁰⁰ Such attempts, from a legal perspective, are the domain of competition law, not negligence or product liability law and are outside the scope of this paper. What is germane, however, is that as an isolated legal move, imposing liability for insecure software on the leading software writers is unlikely to solve the problems of viruses, worms and zombies, while the software world remains an effective monoculture. This brings us to our final section.

III. SECURITY IS FOR EVERYONE, NOT JUST FOR CHRISTMAS

So where do we go from here? The key point we have so far established is that DoS and DDOS are phenomena generated by

¹⁹⁷ Chandler, *supra* note 44.

¹⁹⁸ Geer et. al., *Cyberinsecurity: The Cost Of Monopoly—How The Dominance Of Microsoft's Products Poses A Risk To Security*, Sept. 24, 2003, <http://www.ccianet.org/papers/cyberinsecurity.pdf>.

¹⁹⁹ In Europe see the Commission Decision of March 23, 2004 relating to a proceeding under Article 82 of the EC Treaty. Case COMP/C-3/37.792 Microsoft.

²⁰⁰ See Geer, *supra* note 198, especially section 3 of text.

computer insecurity.²⁰¹ That in its turn is at present generated by two main factors: the tendency of the software industry to produce software which trades off security against speed of development, feature expansion, and user convenience;²⁰² and user failure to make their own machines or systems secure, usually driven by a mixture of ignorance, inertia and lack of incentive to consider risks.²⁰³ We have looked at how criminal law will tend not to deter the hackers and other rogues who launch DoS attacks anonymously or from foreign jurisdictions; and how placing civil liability on either software writers, or users who may potentially become zombies, will *alone* not provide a complete solution.²⁰⁴ The answer must lie in the taking of collective responsibility for security on the Internet by all parties concerned.

When we consider ways of preventing the capture of “zombie hordes” by zombie masters, we need also to recall that zombie networks are used not only to perpetrate DDOS attacks, but also the overwhelming majority of spam, phishing and other types of fraudulent email traffic.²⁰⁵ We are thus considering a major source of social and commercial problems on the Internet, not a few isolated cases of “high jinks” or a few enterprising East European blackmailers. In the case of DDOS, in looking for a regulatory solution, we have to consider if we are mainly trying to discourage teenage hackers from disrupting the Internet for kicks—in which case well drafted criminal laws backed by more punitive custodial sentences might be the way forward²⁰⁶—or whether we are mainly concerned with cutting down the risk of future DDOS attacks which might crucially compromise the critical infrastructure of a country. In the first case, the rhetorical power of the criminal law might seem the most appropriate sanction to employ; but in the second scenario, what we want is actually to find some way of preventing DDOS in the first place. Of course, as usual, the soundest advice will be to go for a mixed paradigm of governance—and indeed, it is likely that we will see in future years a mixture of criminal laws, civil liability cases, and technical fixes being used to regulate DDOS, and more widely, zombie creation.

²⁰¹ See *supra* notes 150-153 and accompanying text.

²⁰² See *supra* notes 154-156 and accompanying text.

²⁰³ See *supra* note 150-151 and accompanying text.

²⁰⁴ See discussion *supra*, sections “Criminal Law” and “Civil Law.”

²⁰⁵ See Leyden, *supra* note 31.

²⁰⁶ Heavy sanctions combined with several high profile cases, for example, seem to have had a significant effect on the willingness of young people to take the risk of illegal MP3 downloading. See, e.g., Tony Smith, *RIAA legal threat cuts P2P downloads by 23%*, THE REGISTER, Aug. 21, 2003. http://www.theregister.co.uk/2003/08/21/riaa_legal_threat_cuts_p2p/.

But in reality, as far as state control goes, the question will be where to put the finite number of resources that can be devoted to enforcing computer security. The argument thus far would be that although criminal laws have a strong exhortatory effect, the resources that would need to be employed to effectively enforce criminal law in this area, might well be better put to backing educational and industry efforts to improve computer security across all players concerned: home users, corporate targets, and ISPs.

This brings in the final two parties Chandler cites as complicit in the creation of DoS attacks: the targets themselves, and the intermediaries who provide Internet access to targets and zombies—that is, ISPs.²⁰⁷

A. *Targets*

Targets should clearly be aware of basic security procedures appropriate to their size and services offered, patch their software regularly, use firewalls and anti-virus software, maintain data backups, keep up with international information security standards, make emergency agreements for support from their own ISPs if under attack, and be prepared to involve the police as needed. As we noted earlier, many smaller companies and some larger ones are deficient in some of these duties. The NHTCU/NOP survey found that only a third of its survey of corporations carried out regular security audits and the same number carried out audits compliant with international ISO standards.²⁰⁸ These figures have room to improve. In terms of DDOS, however, the problem is that there is fairly little a target can do to protect themselves from becoming a victim. State of the art security practices will help protect them against viruses and worms, and prevent corporate targets themselves being used as zombies, but will not protect against a DDOS attack.²⁰⁹ Filtering out traffic may stop servers crashing, but involves a huge risk of filtering out “good” traffic along with bad, alienating existing customers and possibly exposing the target to legal liability.²¹⁰ The only real defense is to have an unlimited stand-by supply of computational resources,

²⁰⁷ Chandler, *supra* note 44; *see also* Commission Decision (EC), Relating to a Proceeding Under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft), Mar. 24, 2004. R

²⁰⁸ *See* NHTCU Survey, *supra* note 55. R

²⁰⁹ *See* JELENA MIRKOVIC, ET AL., INTERNET DENIAL OF SERVICE: ATTACK AND DEFENCE MECHANISMS (2005).

²¹⁰ *See* Wegman & Korzyk, *supra* note 150. R

which for most companies is simply financially untenable.²¹¹

B. ISPs

In terms of criminal and civil law, there is no principled justification for placing responsibility for user computer security on ISPs, which neither initiate nor profit from DDOS attacks (not spamming or phishing). Yet ISPs in their role as the intermediaries who supply broadband Internet to home users could do much to improve the security of home computers. Take the example for a moment, not of DDOS, but of spam launched from zombie machines. Most home users send out their email via their ISP's mail server facilities and have no desire or ability to run their own machine as a mail server. In such cases, a particular "port" (ports are channels for the ingress and egress of data traffic to particular programs on the machine), namely port 25, on the home machine serves little useful function. However home machines can use this port once they are infected by malware—viruses or worms—to covertly send out spam email on behalf of spammers. As discussed earlier, this is how around 80-90% of spam and phishing email is sent.²¹² One function an ISP could perform, which is much talked of in computer security circles, is to "block port 25."²¹³ This would effectively block the use of zombified home machines to send out spam. If ISPs closed port 25 on all home user machines as a matter of default, rather than as a matter of default leaving it open and available for use, the amount of spam currently clogging the Internet could be massively reduced.²¹⁴

In terms of preventing DDOS, there is no single obvious solution of this kind. DDOS traffic is ordinary traffic and thus cannot be detected or shut off by ISPs *per se* without destroying the usability of that machine. But ISPs do have the ability, skills and resources to scan home machines attached to their network to ascertain if they have become zombie machines, and in such cases,

²¹¹ See MIRKOVIC, *supra* note 209.

²¹² See Leyden, *supra* note 31.

²¹³ See *Blocking Port 25 Traffic*, BROADBAND REPORTS, Jan. 29, 2004, <http://www.broadbandreports.com/shownews/38004>.

²¹⁴ Of course, for more sophisticated users, this would irritatingly reduce the flexibility of the use of their home machines. For example, mobile users who wish to log into their email from a variety of locations and via a number of ISPs would find their ability to do so limited. Therefore, it has been suggested that ISPs should offer the option (perhaps via a web form) for users to request that their port 25 be re-opened. The default, however, should be closure. I am indebted for information on port 25 to personal correspondence with Mike Scott, Simon Bisson and Andrew Ducker. See also Operation Spam Zombie, *infra* note 224.

can cut them off from the Internet until they are cleansed of viruses and malware. ISPs could also become part of the process of remote automatic “patching” of machines so they stay “state of the art” secure. As we noted earlier, one of the major reasons for insecurity of home machines is that patches issued by software writers to fill security holes are often not downloaded or not installed by home users.²¹⁵ Installing patches remotely by ISPs would in some ways be very easy, but in other ways raise many problems, as patches might conflict with the rest of the setup on the home machine, causing unexpected bugs and leading to disputes between the home user and the ISP.²¹⁶ Tools would have to be developed which would allow ISPs to take on this task with some degree of safety, and ISPs would also have to be given exemption from legal liability for tampering without authorization with the designated setup of the home machine. This would not be an easy set of tools to develop, but as noted above, it is a question of where money could be best spent to produce a safe computer network environment.

There is generally no reason why ISPs should agree to voluntarily take on this role of “Internet security guards.” Indeed, the whole history of online intermediary law has been of ISPs insisting that they are “mere conduits,” and not responsible either for the traffic they distribute or host, nor the acts of the users to whom they provide access.²¹⁷ Financially, ISPs do not benefit in any compelling way from preventing DDOS attacks across the Internet as a whole, and indeed would rather actively place themselves at risk of legal liability if, for example, they cut off an infected zombie user from their network in breach of the service agreement.²¹⁸ ISPs *do* benefit proximately from reducing the amount of spam in the world, as one of the major costs to ISPs is providing excess bandwidth for spam email, and filtering it out, and so some ISPs already voluntarily undertake to cut off infected home machines from the network which are being used to distribute spam.²¹⁹ Being identified as hosting a source of spam may also lead to an ISP network being “black-listed” and ostracized

²¹⁵ See *supra* note 150 and accompanying text.

²¹⁶ See personal correspondence with sysadmins, noted *supra* note 214.

²¹⁷ See Lilian Edwards, *The Problem of Intermediary Service Provider Liability*, in *THE NEW LEGAL FRAMEWORK FOR E-COMMERCE IN EUROPE* (Lilian Edwards ed., 2005).

²¹⁸ Of course, this risk could be avoided *ex ante* in the user agreement by inserting a clause that would allow an ISP to act whenever they have reasonable cause.

²¹⁹ See e.g., Earthlink, cited in <http://www.cbsnews.com/stories/2004/02/17/tech/main600618.shtml>.

from other networks.²²⁰ In general, ISPs need some kind of regulatory incentive to take on this kind of supervisory role in the general context of improving Internet security standards as a whole. It is not clear how this could best be done but both the civil and the criminal law here seem like very blunt instruments. A better approach might be the development of “soft law” industry standards or code practices via co-regulatory processes involving the ISP and software industries, commerce and governments.²²¹ Wegman and Korzyk suggest that left to self regulate, ISPs will not invest in Internet security, as it is not only an extra business cost, but also “because increasing security slows system performance, customer satisfaction might suffer compared to the competitor [ISP]. The responsible ISP is thus penalized for its responsible behavior.”²²²

Accordingly, they propose that a regulatory code of conduct needs to be introduced, which would *inter alia* require that:

- all ISPs and large networks employ frequently updated anti-virus protection;
- all software on the Internet passes minimum security standards;
- all computers sold come pre-loaded with firewall protection; and
- all ISPs and large networks promptly terminate service to users who are detected sending malicious code, and legal immunity should be given for such action.²²³

Operation Spam Zombie, an action mounted by the U.S. Federal Trade Commission with European assistance to reduce the amount of spam generated by spam zombie machines, also recommends a multi-faceted attack strategy to reduce zombie traffic.²²⁴ ISPs should:

- block port 25;
- identify PCs sending out abnormal amounts of email and identify if they are infected spam zombies;
- if so, these machines should be isolated from the network till clean of infection;

²²⁰ See Edwards, *supra* note 34.

²²¹ Since the Broadcasting Offenses (Amendment) Act of 1999 was passed, Australia has experimented with similar co-regulatory industry codes in an effort to promote the filtering out of obscene material by ISPs.

²²² Wegman & Korzyk, *supra* note 150.

²²³ *Id.*

²²⁴ See Press Release, Federal Trade Commission, Operation Spam Zombies (May 24, 2005), available at <http://www.ftc.gov/opa/2005/05/zombies.htm>; John Leyden, *ISPs Urged to Throttle Spam Zombies*, THE REGISTER, May 24, 2005, http://www.theregister.co.uk/2005/05/24/operation_spam_zombie/.

- customers should be given plain language advice on how to avoid viruses, worms, Trojans etc.; and
- customers should be given easy-to-use tools to remove zombie code if identified, or assistance to remove it.²²⁵

Such suggestions seem to be the beginning of a holistic attitude to computer security which will be necessary if the Internet is to remain useable under the combined assault of spam, phishing, viruses, worms, spyware and DDOS attacks. Hacking ceased to be a joking matter long ago. Computer security is now possibly all that stands between us and the collapse of the critical infrastructure that keeps our society going. In such circumstances, how to regulate zombies is not an abstruse consideration for Internet lawyers but one of the most vital questions we currently face.

²²⁵ *Id.*