Canadian Journal of Law and Technology

Volume 5 | Number 1 Article 2

1-1-2006

Liability for Botnet Attacks

Jennifer A. Chandler
University of Ottawa

Follow this and additional works at: https://digitalcommons.schulichlaw.dal.ca/cjlt

Part of the Computer Law Commons, Intellectual Property Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Jennifer A. Chandler, "Liability for Botnet Attacks" (2006) 5:1 CJLT.

This Article is brought to you for free and open access by the Journals at Schulich Law Scholars. It has been accepted for inclusion in Canadian Journal of Law and Technology by an authorized editor of Schulich Law Scholars. For more information, please contact hannah.steeves@dal.ca.

Liability for Botnet Attacks

Jennifer A. Chandler†

Introduction

A troubling change has taken place recently in malicious attacks over the Internet.[1] The motives of attackers have shifted from the pursuit of thrills and the acquisition of bragging rights to mercenary goals. The attacks and attackers have become more organized and professional. In particular, attackers have begun to develop "botnets" or networks of infected computers that they are able to control remotely. These botnets are used to send spam, to circulate malware (such as viruses), to steal confidential information, to launch distributed denial of service ("DDoS") attacks,[2] and to extort protection money from Web sites by threatening such attacks, among other harmful uses. The key problem with botnets is their ability to make use of large numbers of computers at once. This makes profitable a broader range of attacks, including those that would otherwise not be worthwhile.[3] In addition, botnets can be sold or rented out, and easily updated with new attack tools to suit the needs of buyers in the underground botnet market.

Vast quantities of resources are being devoted to cyber security, fuelled by concern about our increasing reliance on Internet communications as well as the desire to ensure that the social and economic benefits of the Internet are realized. However, despite investment, the cyber insecurity problem remains. The current approach to cyber security is often reactive rather than preventative. Flawed software is remedied by the expensive patching process rather than by releasing robust software in the first place.[4] Malware proliferates at a rate that makes it difficult to produce new patches and new virus signatures, and to deploy them at a sufficient pace to avoid infections.[5] Harmful communications such as spam or denial of service attacks are met with filtration systems that consume financial and computing resources, and slow legitimate traffic.

With the exception of personal firewalls, these solutions become available only after a vulnerability or attack is identified, often after damage has already been caused. Furthermore, these solutions are expensive and inconvenient given that they must be deployed on many computers.[6] Deployment is not the end of the matter because the "arms race" between hackers and the security industry means that many of these solutions require continuous updates.

It is likely that some or all of these problems are not being resolved in the most efficient manner possible. The weak points, particularly in the case of botnets, are the inadequately secured personal computers of average users. These users do not face the full costs of their lack of computer security. This is particularly the case now that bot software is being designed to be minimally disruptive to the computer owner, so that bots may avoid detection and removal. Accordingly, average users fail to invest in security. They do not become educated about security, they do not ensure that flaws in their software are appropriately patched, nor do they demand secure software from vendors in the first place. They either fail to apply security measures such as anti-virus software or firewalls or, if they do apply them, they do not maintain them conscientiously. In economic terms, they impose significant negative externalities on cyberspace. Although a user's personal investments in security will offer him or her protection against some threats (such as spyware), the user is otherwise dependent on the security investments of others to avoid spam and DDoS attacks.

This paper will consider the possibility of using tort liability to address cyber insecurity. In previous work, I have proposed a hypothetical lawsuit by the victim of a DDoS attack against the vendor of unreasonably insecure software, the flaws of which are exploited to create the DDoS attack army.[7] Indeed, software vendors are facing increasing public disapproval for their contributions to cyber insecurity.[8] However, not all DDoS attack armies are assembled by exploiting flaws in software. Computers are also infected when users voluntarily open infected email attachments or download infected files from file-sharing networks. Accordingly, the cyber insecurity resulting from the large numbers of average end-users with infected computers cannot be entirely addressed by reducing the number of exploitable flaws in widely-deployed software. It may be useful to find additional ways to address other avenues of infection.

Some have argued that we should focus on modifying end-user behaviour or catching the criminals

†© J.A. Chandler. Assistant Professor, Faculty of Law, University of Ottawa. The author thanks the anonymous peer reviewers as well as the participants at the Oxford Internet Institute's Conference "Safety and Security in a Networked World", September 8–10, 2005 for helpful comments on this paper.

directly responsible for malware and cyber-attacks. As discussed below, I suggest that effort of this sort is useful but insufficient. Another possibility is to induce ISPs to take a far more active role in (1) ensuring end-users' computers are appropriately maintained in order to reduce the risk of malware infection, and (2) monitoring end-users' computers so that infected computers can be quarantined before they cause harm. An increase in ISP control over subscribers' computers would have some negative consequences, and it would be necessary to consider whether the anticipated increase in cyber security is a sufficient benefit to outweigh the potential harms. Should it be decided that ISP liability is a useful approach, the hypothetical lawsuit by the victim of a DDoS attack that I described in earlier work could also be brought against the ISP that hosted all or part of the attacking botnet.

Part I of this paper will discuss the emerging problem of bots and botnets. Part II will explore what ISPs can do about botnets, and will briefly outline the possible argument in tort that could be made by the victim of a DDoS attack launched from an ISP's network.

Part I — Overview of Bots and Botnets

In the computer world, a bot (short for "robot") is a software program that performs an automated process. While some bots are useful (such as those used by search engines to browse through Web sites collecting information to include in the search engine database), malicious bots have also emerged and are a serious threat to cyber security. The key components of a malicious bot (to which I refer simply as a "bot" in this paper) are normally the following: a propagation mechanism, a remote control function, and several actions that can be taken by the bot at the direction of the controller.[9] The feature that distinguishes bots from other forms of malicious code, or malware, is the use of a remote control mechanism that permits them to be effectively networked. These networks can be very large, consisting of tens of thousands of linked systems,[10] which together offer considerable computing power.

Propagation

A computer can become infected with a bot in numerous ways, and the creativity of malware writers suggests that additional methods will arise. Bots can spread through network connections by exploiting vulnerabilities in software (normally the Windows operating system),[11] by using backdoors installed on a computer during an earlier malware infection, and by cracking weak passwords on network shares.[12] They can also spread through peer-to-peer file-sharing networks by adopting alluring filenames that induce other users to download them.[13] They spread through email both as attachments that users must open in order to trigger the infection, and also as malicious HTML code that runs automatically when an email is viewed using certain email client programs.[14] Bots can also infect users who view maliciously designed Web sites using vulnerable Internet browser software.[15] Many bots, such as the Gaobot/Agobot, Mytob and Spybot families, use multiple methods to propagate.[16]

Although many of the current bots contain their own propagation mechanisms, not all bots do. Instead, some simply connect to the botnet's remote control channel to await instructions after they are installed on a computer.[17]

Remote Control

Bots are distinguished from other forms of malware due to their ability to form coordinated networks, or "botnets", under the command of the botnet controller.[18] This is achieved in a variety of ways.

One common method is to design bots that, once installed on an infected computer, attempt to join specific Internet Relay Chat ("IRC") communication channels. IRC is a system that enables multiple member discussions in forums called IRC channels under the control of channel operators.[19] Once connected to the designated IRC channel, the bots await further commands from the controller.[20] A botnet controller can efficiently control numerous bots in this way.[21]

Botnets are vulnerable to disruption if they are detected and their IRC channels are disabled.[22] Bot designers have attempted to protect their botnets by planting the IRC servers they use on compromised computers,[23] by encrypting communications with the botnet, and by protecting access to the IRC channel by a password.[24] Another technique adopted by botnet controllers is to use a dynamic domain name service to identify the location of the IRC server. In this way, if a botnet's IRC channel is shut down, the controller can move to another location. The bots are designed to join a channel on a server at a particular domain name that is registered with the dynamic domain name service. If the IRC server must move to a new IP address, the dynamic domain name service takes care of the redirection and the bots can find the new IRC server even though they continue to look for the same domain name.[25]

In addition, bot designers are moving to new methods of communication. Symantec has observed two bots that use their own encrypted peer-to-peer networks.[26] The advantage of a peer-to-peer network model is that the detection and removal of one node will not disrupt the network, thus avoiding the vulnerability associated with a centralized communication system like IRC.[27] An example of a bot that uses peer-to-peer communication is Phatbot. The bots register themselves as peers on the Gnutella network but use an atypical port for communication, which serves to distinguish them from normal participants in the Gnutella network.[28]

Symantec also describes bots that use an email-related protocol (POP3) to communicate.[29] The bots connect to a predefined mail server to retrieve email messages that contain commands in email attachments. The bots can also respond to commands through the same channel. Symantec notes that "[s]ince POP3 communication is not uncommon on most networks, this traffic would be more likely to go undetected than a connection to an IRC server. Additionally, ports used for POP3 communication are less likely to be filtered or blocked at the network perimeter".[30]

The Uses of Botnets

Botnet controllers can deliver instructions to the bots through the IRC channel or other communication channel. If a bot is not already designed to perform a particular function, the bots are easy to update by instructing them to download software from a specified location.[31] Among the activities performed by botnets are sending spam (including phishing email), gathering and returning sensitive data to the controller, launching DDoS attacks, and speeding the spread of other malware, among other uses. [32]

Spam and phishing

Spam, or unsolicited bulk email, has become a tremendous online annoyance.[33] Estimates from early 2005 of the proportion of email that is spam range from 68% to 83%. Some of this email is more than merely annoying. A "phishing" attempt is an email message that attempts to trick the recipient into parting with confidential information by masquerading as a message from a legitimate business such as a bank or eBay, and requiring the victim to log in to confirm account details.

In an attempt to shut down spammers, multiple "block lists"[34] are available to assist email servers to reject messages coming from IP addresses known to send spam. Spammers have reacted to this defensive strategy by relaying spam through compromised computers, including those linked into botnets. In this way, spammers are able to avoid being blocked by spam block lists. Symantec reports that within its list of the top 50 instances of malware, the proportion that contains email-relaying capacity has been steadily increasing from 37% in the last six months of 2003, to 47% in the first six months of 2004, and 53% in the last six months of 2004.[35]

Spying and theft of confidential information

Many of the common bots are designed to look for confidential information in stored memory such as CD keys for games, software product ID numbers, or passwords.[36] In addition, they may contain "packet sniffers" and "keystroke loggers" to look for sensitive information.[37] The increase in the prevalence of malicious code designed to steal sensitive confidential information is attributed to the growth of botnets, which facilitate the remote retrieval of this information.[38] In addition to the theft of confidential information, bots can be used for general privacy invasion. For example, the Spybot family has been observed not only to log keystrokes and look for stored passwords, but also to capture screenshots or webcam footage.[39]

Distributed denial of service attacks

Botnets are often used to launch DDoS attacks. Statistics on the level of DDoS activity vary, with Symantec reporting a steady increase in DDoS attacks in the last half of 2004.[40] The number of DDoS attacks reported in the 2004 CSI/FBI Computer Crime and Security Survey, on the other hand, showed a decline when compared to the 2003 data. In any event, DDoS attacks continued to impose heavy costs, estimated at about $26 million in 2004 for the 269 respondents to the 2004 CSI/FBI survey.[41]

The motives for DDoS attacks are varied. One of the troubling uses that has emerged recently, and which is closely associated with botnets, is extortion. Starting in about 2003, criminals began to threaten to disable online betting companies with DDoS attacks during peak gambling times unless the companies paid thousands of dollars.[42] Other businesses that generate significant revenue online are equally vulnerable to DDoS-related extortion.[43]

Another example illustrates the use of botnets "for hire". In 2004, Jay Echouafni and his co-conspirators were indicted in California after Echouafni paid a business partner to arrange for hackers to launch DDoS attacks against his online business competitors.[44] The attacks, which took place in 2003, cost the victims over $2 million and disrupted services for their ISPs and other sites.[45] Echouafni, however, paid $1,000 for the attacks, which were launched from the hackers' botnets.[46] He claimed that his competitors had stolen some of his Web site content and were themselves launching DDoS attacks against his Web site.[47]

DDoS attacks are occasionally used for political purposes. Examples include attacks by Indian hackers against Pakistani government Web sites,[48] attacks on Web sites associated with the Chechen rebel movement,[49] and a spate of attacks originating in China and Korea against Japanese sites at a time of heightened tension between the countries.[50] DDoS attacks have also been used, most likely by spammers, to attack spam block-lists.[51]

Accelerating the propagation of malware

Botnets can also be used to "pre-seed" computers with malware in order to increase the speed of propagation and thus ensure an effective epidemic. It has been suggested that the Witty worm was likely launched by a botnet, as the worm broke out roughly at the same time from a large number of computers distributed all over the world.[52] Symantec discovered that the Witty worm was launched from computers that did not run the vulnerable software that Witty exploited, further suggesting that it had been launched from a botnet.[53] Botnet owners have also profited from their botnets by installing adware, for which they are paid by online advertising companies on a "per install" basis.[54]

Other uses for botnets

Botnets can be used for online advertising fraud. Where an advertiser contracts with a Web site to carry its advertisement and the fee varies according to the number of visitors clicking on the ad, a botnet can be used to click on the ads to inflate the traffic in order to defraud the advertiser.[55] Botnets can be used to manipulate online polls, since each bot has a distinct IP address and appears to be a unique vote.[56] They are also used to manipulate certain online games.[57]

The Future of Botnets

As the foregoing illustrates, botnets already present a considerable danger. Unfortunately, this danger is increasing. Reports of bot code increased steadily through 2004, and the number of documented variants of the three major bots (Randex, Gaobot and Spybot) reached nearly 6,000 at the end of 2004.[58] McAfee reports a three-fold increase in bot detection over the first two quarters of 2005.[59]

The future of botnets is quite worrisome. Botnets will become increasingly effective as broadband access spreads.[60] Furthermore, mounting evidence suggests that botnets are increasingly used for financial gain, that the newer bots are more sophisticated, and that their networks are increasingly difficult to disrupt.[61] Already many of the established bot families take steps to evade detection by terminating the processes of anti-virus software on infected computers.[62] Some bots, such as Polybot, possess polymorphic ability, or the ability to "mutate" to impede detection by anti-virus software that depends upon specific virus signatures.[63] Polybot is modified each time it runs on an infected computer.[64]

There is evidence that botnets are available for rent. Botnets and zombies are reportedly available at prices of 5 to 10 cents per computer.[65] The market in botnets is reasonably sophisticated, with dealers offering higher quality bots (i.e., high-bandwidth machines and machines located in jurisdictions where authorities are perceived to be less likely to shut down bots[66]) at a premium, as well as making sales promotional offers.[67] The "business" of malware was revealed in a public battle between rival gangs of malware writers in 2004. When one group launched a worm designed to remove a rival group's worms from infected computers, the retaliatory worm contained insults and taunts along the following lines: "Hey, NetSky . . . don't ruine our bussiness, wanna start a war? [*sic*]"[68] The ability to generate money by selling or renting out botnets or by offering attacks "for hire" offers a powerful incentive to criminals who would not be motivated by the thrills or the pursuit of boasting rights that appear to have motivated hackers in the past.

Part II — Liability of ISPs for the harms caused by botnets

Many parties contribute in some way to the botnet problem. The obvious culprits are the writers of malware, the botnet controllers, and the parties who rent or pay for attacks by botnets. The criminal law exists to deter and sanction this behaviour, but is clearly not sufficient. The scale of the problem and the forensic and jurisdictional challenges of enforcement seem to have greatly reduced the deterrent impact of the criminal law.[69] These difficulties should not prevent the state from continuing to pursue cyber-criminals to the extent possible given limited resources, but it cannot be the sole approach. It is also necessary to ensure that others who are well-positioned to detect and prevent attacks take reasonable steps to do so.[70]

The end-users who fail to maintain the security of their systems supply the computers that form botnets.[71] Increasingly, however, even conscientious end-users can become infected. Systems are vulnerable due to the delay between the discovery of a software flaw or a new piece of malware and the implementation of a remedial patch or anti-virus update. The US CERT notes three occasions in 2005 of major system infections resulting from newly discovered worm variants not included in the then-current anti-virus signatures.[72] Firewalls cannot protect against infections delivered via normal processes such as email or inadvertently browsing web sites infected with malicious code.[73]

The apparent lack of interest in the security of their computers that is shown by average end-users is not surprising. The average end-user does not have a good understanding of computer and network security. Even those end-users who do have a reasonable understanding of security face the costs in time and money of installing and maintaining security software, and patching software flaws. Although programs such as Microsoft's automatic update system have eased the patching burden for the average end-user, patches continue to cause problems. They are expensive to manage in the context of enterprises,[74] and they periodically contain new flaws.[75] Another danger is that the patching system may be hacked and users induced to download a compromised patch.[76]

The key problem, however, is that end-users do not suffer most of the costs associated with the insecurity of their computers. Furthermore, their investments in security benefit others as much or more than they benefit the end-users. In other words, end-users suffer very little when their computers are used to send spam or launch DDoS attacks, and any investment in securing their own computers will not protect them against the spam or DDoS attacks launched from the insecure computers of others. This is increasingly the case as writers of malware become interested in assembling botnets to use for financial gain. Bot software is designed not to disrupt the infected computer, but to quietly participate in the spam or attack activity directed by the botnet controller against another party. A noisy or disruptive bot would risk detection and removal by the owner of the infected computer.

To the extent that end-users do suffer from their own computer insecurity, as is the case with the theft of confidential information by spyware, most appear to be unaware of the threat, so it does little to encourage them to secure their systems. While this suggests that there is room for efforts to educate end-users, they will still not face the costs of spam and DDoS, and this suggests that they will under-invest in security. Some have suggested that end-users could be fined or sued in order to cause them to maintain system security.[77] This would, however, be expensive and would run into the difficulty that many infected computers may be located in other jurisdictions.

Responsibility of Internet Service Providers

What can ISPs do?

ISPs, including providers of home Internet access, universities and other network operators, are facing increasing pressure to deal with the harms emanating from bots on their networks. The Canadian government released the report of its task force on spam in May of 2005.[78] The report recommends that ISPs and other network operators implement a set of best practices[79] to combat spam. The U.S. Federal Trade Commission announced "Operation Spam Zombies" in May 2005, which encourages ISPs to take steps to protect their subscribers' computers from being used to relay spam. Should these exhortations be ignored, one suspects that regulation might follow.

There are signs that the pressure on ISPs is starting to come from private sector sources as well, including the victims of DDoS attacks. A consortium of British online gambling companies (which are often targeted by DDoS extortion attempts) has started to lobby ISPs to apply better security to combat DDoS attacks.[80] They are asking ISPs to distribute firewalls to customers to monitor for, and shut down the flood of attack traffic emanating from, infected computers. Although they are currently asking for help, it is possible that they might eventually attempt a lawsuit.

Some network operators are simply starting to block email received from ranges of IP addresses assigned to particular ISPs that harbour spammers. The targeting appears to be somewhat imprecise, affecting both infected computers that are relaying spam as well as other subscribers.[81] The threat of having to deal with subscribers upset by service interruption may cause ISPs to take action to control bots on their networks.

There appear to be a variety of measures that ISPs could take that would help to impede the propagation of bot software (and thus suppress botnet creation) or to throttle botnet activity on their networks. ISPs could (1) enforce the application of software patches and anti-virus updates on subscriber computers, (2) scan subscribers' computers for known infections,[82] (3) periodically scan subscribers' computers to check the integrity of operating system, firewall and antivirus software,[83] (4) block email attachments with file extensions commonly associated with infections or scan email attachments, (5) quarantine infected subscribers,[84] (6) block ports that are associated with known software vulnerabilities,[85] (7) block applications often used to transmit malware such as peer-to-peer file-sharing, or (8) block all ports not needed for a set of approved applications (e.g., e-mail, web browsing). Some of these measures may have significant negative consequences, and constitute an unacceptable exchange of freedom and privacy for cyber security improvements.

There are also many measures that ISPs could take to reduce some of the key harms inflicted by botnets. In addition to some of the measures mentioned above, the Canadian spam report lists a set of ISP best practices,[86] including blocking port 25 on subscribers' computers,[87] monitoring the volume of subscribers' email traffic, and rate-limiting their email. Additional recommendations are aimed at encouraging communication and cooperation amongst network operators, as well as suppressing address spoofing, and enhancing the traceability of spam.[88] The U.S. FTC makes similar recommendations.[89]

With respect to DDoS attacks, ISPs can enforce "egress filtering", which monitors IP packets sent from their subscribers to detect false source addresses (a characteristic of some DDoS attacks). Other mechanisms based on monitoring for traffic anomalies have also been proposed to deal with DDoS.[90] Most ISPs seem to choose not to invest in source-based preventative mechanisms to forestall DDoS attacks on others.[91]

What should ISPs do?

As noted above, there are many measures that ISPs could adopt that would reduce the spread of bot software and the damage done by botnets. Some ISPs are reportedly already blocking port 25, limiting the number of emails that a subscriber can send through the ISP's email server, and quarantining infected machines.[92] Some ISPs already block email attachments with certain file extensions,[93] and others offer virus-scanning of attachments before they are delivered to customers.[94]

The number of ISPs taking preventative measures and/or the type of measures adopted so far appear to be insufficient to deal with botnets. Botnets are proliferating, even on the networks of ISPs that offer security services to subscribers. Prolexic, a provider of anti-DDoS filtering services, provides a summary of attack traffic from the first two quarters of 2005, showing the top twenty infected networks worldwide.[95] The list includes numerous ISPs who provide free anti-virus software, personal firewalls and other security protections.[96]

Stronger measures such as enforced system monitoring, patching and updating, and the application at source of anti-DDoS measures may be advisable, but such measures may raise costs and annoy subscribers. If an ISP invests too much in security, to the benefit of everyone connected to the Internet, while competing ISPs do not, it may lose price-sensitive subscribers.[97] Subscriber reaction to intrusive safety measures would likely depend upon the sophistication of the subscribers as well as the measures taken. It is possible that ISPs will be unwilling to take the stronger measures, such as monitoring for and suspending individual accounts, as they would have to deal with telephone calls from confused and angry subscribers.[98]

ISPs will undoubtedly have some incentive to try to deal with botnets on their networks. These motivations include reducing complaints from the recipients of harmful traffic (some of whom may be their own subscribers), limiting the consumption of network resources by spam and DDoS sent by botnets, and avoiding the possibility of having some traffic blocked by other ISPs. However, they will not face the full costs of botnets since many of the harms will be borne by others. As a result, one might suspect that ISPs will take some measures, but may not take the optimal level of care to shut down botnets.

Two ways in which ISPs could be encouraged to deal with botnets are regulation or liability for the harms caused by botnets on their networks. I will not consider regulation further in this paper, except to note that ISPs are strongly opposed to the idea of regulation, arguing that rapid technological change and the need to permit flexibility in implementing security measures militate against codifying requirements by regulation.[99] The other possibility is liability in negligence to the victim of a botnet attack emanating, in whole or in part, from an ISP's network. Before discussing some of the arguments involved in such a lawsuit, I will turn now to the reasons why we might not wish to encourage ISPs to increase their control of subscriber activities.

A number of arguments could be raised against holding ISPs liable for botnet attacks. First, ISPs could take measures that would unacceptably invade subscriber privacy. Second, ISPs could impose so many limitations on subscriber activity that individual freedom and innovation would be curtailed. Third, once ISPs are required to increase their ability to control traffic flows for security purposes, they may more easily use this power for illegitimate purposes. Fourth, smaller ISPs will not be able bear the costs of precautions as they do not have the economies of scale open to larger ISPs.[100] Fifth, the increase in prices associated with additional security measures will squeeze out marginal subscribers.[101] Sixth, the pressure on others, such as end-users, to take reasonable steps to address cyber security will be reduced, and the pursuit of innovative ways to assist end-users to protect themselves will be abandoned in favour of innovation aimed at assisting ISPs to monitor and control their networks.[102] Seventh, imposing liability on domestic ISPs will not be effective in preventing the harms of botnets, as they will merely relocate to other jurisdictions.

These are valid concerns, and it is difficult to answer many of them. In deciding whether or not it is wise to encourage or permit the courts to impose liability on ISPs for botnets, it will be necessary to consider whether the improvements in cyber security to be expected are worth tolerating the negative consequences.

There are dangers in shifting to an increasingly active role for ISPs in the control of information flowing through their systems. ISPs may begin to censor or control traffic for their own purposes. In a recent incident, a Canadian ISP blocked access by its subscribers to a Web site run by a labour union of its employees that was attempting to publicize its views about a labour dispute.[103] Clark Ray notes the danger that ISPs might be tempted to collect information for resale to vendors or advertisers, to apply software updates unrelated to security, or to examine files unrelated to software maintenance (e.g., searching for unlicensed software or unlicensed music files).[104] Users might be able to protect their privacy to some extent by encrypting files.[105]

There is also a danger that holding ISPs liable for botnet attacks will cause them to limit excessively the nature of the service they offer, perhaps blocking all but a list of approved ports and applications. A more moderate response would be to block only those ports known to be associated with problems. The example of the blocking of port 25 suggests that the market may respond to meet the needs of more sophisticated users who find themselves stymied by the port block. When ISPs began to block port 25, new services emerged to meet the requirements of users who wished to continue to run their own mail servers.[106] This type of circumvention is likely not to be a problem because sophisticated users can be expected to maintain the security of their systems.

Another difficulty is that the infected computers may reside on the networks of foreign ISPs. In fact, if ISP liability is successful in reducing the ease with which botnets can be assembled, one would expect that botnets would migrate to other jurisdictions. Parties seeking to pursue foreign ISPs would find it more challenging to sue as a practical matter due to the issue of legal jurisdiction. The concern that botnets might migrate to more congenial jurisdictions is buttressed by the observation that, in the underground zombie trade, the price of zombies hosted in certain countries is higher because they are considered less likely to be shut down.[107] To the extent that foreign ISPs permit this to occur, they could be black-listed and communications from them refused or limited. There are precedents for black-listing foreign servers that are significant sources of spam.[108]

ISP Liability for Botnet Attacks

The suggestion that ISPs be held liable in negligence if they fail to take reasonable steps to prevent attacks by botnets on their networks runs counter to the widespread tendency to treat ISPs as immune from liability for the content of traffic on their networks. For example, the *Canadian Human Rights Act*,[109] the Canadian *Copyright Act*[110] as discussed by the Supreme Court of Canada in *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*,[111] and the recently tabled amendments to the Canadian *Copyright Act*[112] provide some immunity to network operators who merely provide a transmission conduit for communications. In the United States, courts have interpreted very broadly the legislation immunizing ISPs from liability, to the increasing consternation of several American commentators.[113] For example, Rustad and Koenig argue that ISP immunity should be pared back in order to make ISPs "more accountable to the public for excessive preventable dangers in cyberspace".[114] The authors point out that "ISPs … are no longer delicate infants that need absolute immunity in order to survive".[115]

It is possible that this tendency to treat ISPs as immune from responsibility for activities on their networks might impede the legal argument advanced in this paper. Nevertheless, I will now turn to the hypothetical lawsuit by the victim of a DDoS attack against the defendant ISP(s) that hosted the attacking botnet.

The victim of the DDoS attack is well-suited to be a plaintiff in the proposed lawsuit. The DDoS victim might suffer the scale of loss that would motivate a lawsuit. The DDoS "for hire" case described earlier inflicted over $2 million in losses on the three businesses attacked.[116] The 2004 CSI/FBI survey reported that the 269 respondents estimated their losses from DDoS in 2004 at $26 million.[117] Groups of DDoS victims have already identified ISPs as capable of stemming the attacks.[118]

Tort law does permit liability to be imposed on a defendant in situations in which the harm to the plaintiff is caused most directly by a third party. The defendant may be held responsible where he or she creates a situation of unreasonable risk such that a plaintiff will be harmed by a third party.[119] For example, Canadian courts have held landlords responsible where their inadequate security measures expose tenants to attack by unknown third parties. Similarly, those having care of vehicles may be liable if they leave keys behind when it is reasonably foreseeable that the vehicles may be stolen and cause injury to others.[120] These cases reveal that a defendant may be liable to a plaintiff in negligence for creating an unreasonable risk of attack by an intervening third party. As a result, there is precedent for an argument that ISPs, by failing to prevent or disable botnets on their networks, are creating a situation of risk of harm to DDoS victims at the hands of the botnet controllers.

The lawsuit by the victim of DDoS does face some hurdles under current tort law. First, the defendant ISP might argue that it does not owe a duty of care to the plaintiff. Second, the ISP might argue that the plaintiff's losses are "pure economic losses", the recovery of which is restricted in negligence cases. Finally, the ISP might argue that the plaintiff is contributorily negligent for failing to employ anti-DDOS services.

A plaintiff in a negligence case must establish that the defendant owes the plaintiff a duty of care. The Canadian legal test to determine the existence of a duty of care in a novel situation involves two steps.[121] First the court must determine if there is a "relationship of proximity" between the plaintiff and the defendant, and whether the harm to the plaintiff was a reasonably foreseeable consequence of the defendant's acts. Second, the court must consider if there are residual policy considerations that suggest that a duty of care should not be recognized in the circumstances. The meaning of "proximity" has caused great perplexity, but it appears to exist where the relationship between plaintiff and defendant is sufficiently "close and direct" that the defendant ought to foresee that its carelessness might harm the plaintiff and that it is just and fair that the defendant be required to take care to avoid harming the plaintiff.[122]

I have argued in an earlier paper that vendors of software that has achieved near complete market share are in a sufficient relationship of proximity with all users of cyberspace because their software in large measure determines the structure and security of cyberspace for everyone.[123] ISPs do not have the same sort of necessary connection to the users of cyberspace as the vendor of widely-deployed software, since the ISP market is more fragmented, and the available statistics suggest that the most infected network (aol.com) is responsible for about 5% of bots in the world, and 11% of bots in the U.S.[124] This suggests a lesser connection to everyone in cyberspace than a software vendor with near complete market share.

It may be necessary to consider a form of "cyberproximity", or proximity that is tailored to cyberspace. It is clear that the Internet presents a seemingly intractable challenge to law enforcement and security by virtue of the unprecedented level of worldwide interconnection involvrd, and the volume of communication. We may need to move to a more broadly distributed model of responsibility in which everyone is responsible for the harms that his or her corner of the network may cause to everyone else on the network.

This would result in a more expansive conception of duty than traditional tort law might otherwise have imposed, but I do not feel it is an unreasonable or revolutionary step. The principle being invoked in the cyberspace context, namely that of taking care not to create situations of risk that might foreseeably be exploited by criminals to attack others, is the same as that applied in the physical world in the case of keys left in a vehicle.[125] The number of parties to which one owes a duty of care is greater in the cyberspace context by virtue of the high level of interconnection between people made possible by the Internet. The increased degree of interdependence (particularly with respect to security) among those participating in cyberspace is also a feature of this environment, such that it is arguably "just and fair" to require participants to look out for each other. Leaving keys in a vehicle in one city is unlikely to injure anyone on the other side of the globe, but maintaining an insecure network could easily injure many people. An overly limited vision of proximity and thus of duty of care would fail to recognize this fact.

Assuming the proximity hurdle can be passed, it is reasonably simple to pass the foreseeability hurdle. As trade groups such as the consortium of British online gambling companies mentioned earlier begin to lobby ISPs to apply better security to combat DDoS attacks,[126] the harm to e-commerce enterprises resulting from botnet-driven DDoS activity is becoming impossible to ignore.

The losses suffered by the DDoS victim are most likely to be "pure economic losses" (i.e., economic losses that arise independent of any physical injury to person or to property) flowing from the interruption in the use of the victim's computer services. The victim might suffer loss of business, harm to goodwill and wasted employee time and effort. The victim is unlikely to have lost data, which would have made it possible to argue that data ought to be treated as property.[127] The DDoS victim could sue the perpetrator of the attack for the economic losses using one of the intentional business torts such as interference with contractual relations, or interference with economic relations by unlawful means.[128] However, because the defendant ISP is being pursued using a negligence theory rather than a vicarious liability theory, the plaintiff faces the problem that the recovery of pure economic loss through a negligence lawsuit has been restricted by common law courts.

Common law courts have been reluctant to permit the recovery of pure economic loss due to the risk of indeterminate liability,[129] the fear that lawsuits will proliferate and absorb too many scarce judicial resources,[130] the need to respect and protect contractual allocations of loss, and the desire to preserve the vigorous free market competition that might be discouraged by the prospect of liability for the negligently inflicted pure economic loss of a competitor.[131] In addition, pure economic losses are viewed as "less compelling of protection than bodily security or proprietary interests".[132] Despite all of these concerns, however, Canadian and U.S. courts permit the recovery of negligently inflicted pure economic loss in certain circumstances.[133]

One useful analogy to the present problem is provided by the American case, *Union Oil Co. v. Oppen*.[134] In that case, fishermen successfully sought compensation for lost commercial fishing profits from oil companies that caused a major oil spill. Feldthusen suggests that this was the correct result given that the oil companies were best situated to avoid the harm, and because there is no private party available to sue for property damage in the case of a public resource. There was, accordingly, a strong deterrence argument for permitting the plaintiffs to recover for economic losses resulting from damage to a public resource.[135] This reasoning is applicable in the context of DDoS attacks. The Internet has arguably attained the status of a public resource, which is endangered because the parties best-positioned to address cyber insecurity (including ISPs and vendors of software) do not face the full costs of insecurity and accordingly do not invest the optimal level of effort in remedying the problem.

Another counter-argument that the defendant ISP might raise is that the victim of the DDoS attack was contributorily negligent in failing to take self-defensive steps. Plaintiffs who fail to use safety devices, particularly car seatbelts, are often considered to have been contributorily negligent.[136] "The essence of the argument is that the plaintiff's failure to employ the device was unreasonable, and that this unreasonable conduct was a contributing cause of the plaintiff's injuries."[137] In another Canadian case, the plaintiff poultry farmer's failure to plug in a power failure alarm system on the night that the defendant negligently cut the power lines was considered contributory negligence. The evidence was inconsistent on how many other farmers employed these systems, but 25%–50% likely did.[138]

It appears that the failure to take reasonable self-protective measures might leave a plaintiff open to a charge of contributory negligence. In the case of DDoS, the self-defensive options are limited. Anti-DDoS services are reported to cost $12,000 per month when supplied by large US ISPs.[139] It is uncertain whether these services can handle all forms of DDoS and it is difficult to determine the accuracy of the claims made by such service providers.[140] These services seem sufficiently immature, expensive and inconsistently deployed that it would be unlikely that the failure to use them would be construed as contributory negligence. Nevertheless, the possibility remains that parties who are at considerable risk of DDoS and stand to lose large sums might be expected to take such steps.

Should a duty of care be found to be owed by a defendant ISP to the victim of a DDoS attack, a court would have to determine the requisite standard of care. In other words, what actions would the law consider reasonably required of ISPs to prevent harms emanating from botnets on their networks? As noted earlier in this paper, there appear to be a variety of measures that ISPs could take that would help to impede the propagation of bot software (and thus suppress botnet creation), or to throttle botnet activity on their networks. Many of the measures designed to prevent the creation of botnets and the spread of bot software have negative consequences for subscriber privacy and freedom. It might be preferable to encourage ISPs to focus on effective source-based preventive tools. Using these techniques, ISPs can monitor traffic emanating from their own networks and throttle attacks launched against third parties. Experts studying the problem of DDoS note the desirability of such approaches and suggest that incentives for ISPs to deploy them are currently insufficient.[141] Potential liability may encourage ISPs to develop and apply such tools effectively.

Conclusion

Cyber insecurity continues to create significant and increasing concern, particularly with respect to the national security implications. Although vast quantities of resources are employed to address the cyber security problem, the steps taken so far are proving inefficient and insufficient. The parties best placed to take steps to address cyber insecurity, including software vendors, ISPs, and end-users do not face the full consequences of their contributions to cyber insecurity. Accordingly, they do not invest time and money to the socially optimal level of improved security.

In previous work, I have suggested that software vendors should face liability in negligence for unreasonably insecure software. This would help to reduce malware that is spread by exploiting software vulnerabilities. However, malware is also spread due to the careless behaviour of end-users in opening infected files. It is likely to be inefficient to pursue individual end-users to induce them to maintain the security of their systems. Instead, ISPs and other network operators are well-positioned to enforce security in subscribers' computers. A range of security measures that vary in their degree of intrusiveness are open to ISPs. Some of these measures may be so harmful to individual liberty and privacy that they are not worth the security improvement to be gained. Nevertheless, it is likely that some measures, such as enforced software patching and anti-virus software maintenance, as well as source-based DDoS attack prevention should be taken.

Should ISPs not take reasonable steps to prevent DDoS attacks launched by botnets harboured on their networks, they ought to be liable in negligence to the DDoS attack victims. While groups of DDoS attack victims are so far restricting themselves to lobbying ISPs to take security measures, they may soon find it worthwhile to sue.

Notes:

1 John Leyden, "Botnets, phishing and spyware" *The Register* (21 December 2004) <http://www.theregister.co.uk/2004/12/21/security_review_2004/>.

2 An Internet-based denial of service attack is one that seeks to disable the target system by overwhelming it with a large volume of communications traffic. A distributed denial of service attack is one that is launched simultaneously from a large number of sources.

3 Laurianne McLaughlin, "Bot Software Spreads, Causes New Worries" (2004) 5(6) IEEE Distributed Systems Online, <http://csdl2.computer.org/comp/mags/ds/2004/06/o6001.pdf> at 4., quoting Bruce Schneier, "What worries me the most is that [bots] make marginal attacks profitable".

4 Mark G. Graff and Kenneth R. van Wyk, *Secure Coding: Principles & Practices*, (Sebastopol, CA: O'Reilly & Associates, 2003) at 56. Graff and van Wyk cite estimates that the cost of fixing an error with a patch once the software is widely deployed is sixty times as expensive as fixing it at the design stage.

5 Simon Avery, "Virus made in 7 days" *Globe and Mail* (17 August 2005), <http://www.globetechnology.com/servlet/story/RTGAM.20050817.wirusess0817/BNStory/Technology/>.

6 The anti-virus software market is worth billions of dollars, and is expected to reach $5.5 billion in 2005; the anti-spam filter market reached just under $1 billion in 2004: Matthew D. Sarrel, "Lock down your e-mail" *PCMag.com* (26 January 2005), <http://www.pcmag.com/article2/0,1895,1755125,00.asp>. Anti-DDoS services can be very expensive, reportedly $12,000 per month when supplied by large US ISPs: Denise Pappalardo and Ellen Messmer, "Extortion via DDoS on the Rise" *Computerworld* (16 May 2005), <http://www.computerworld.com/printthis/2005/0,4814,101761,00.html>.

7 Jennifer A. Chandler, "Improving Software Security: A Discussion of Liability for Unreasonably Insecure Software" forthcoming 2005, Stanford University Press; Jennifer A. Chandler, "Security in Cyberspace: Combatting Distributed Denial of Service Attacks" (2003-2004) Univ. Ott. L. & Tech. J. 231.

8 Jack Kapica, "Business Users Blast Microsoft" *Globe and Mail* (18 August 2005), <http://www.globetechnology.com/servlet/story/RTGAM.20050818.gtwormaug18/BNStory/Technology/>.

9 Thorsten Holz, "A Short Visit to the Bot Zoo" (May/June 2005) *IEEE Security & Privacy*, p. 76; Honeynet Project & Research Alliance, "Know your Enemy: Tracking Botnets" (13 March 2005), <http://honeynet.org/papers/bots/>.

10 Honeynet Project, *supra* note 9; McLaughlin, *supra* note 3, reporting Symantec's suggestion that botnets comprise 2000–10,000 computers on average, although botnets as large as 400,000 have been found.

11 Holz, *supra* note 9 at 77: "[M]ost bots also include a mechanism to spread further, usually by automatically scanning whole network ranges and propagating themselves via vulnerabilities. These vulnerabilities usually appear in the Windows operating system, the most common being DCOM (MS03-026, buffer overrun in RPC interface could allow code execution) and LSASS (MS04-011, security update for Microsoft Windows). Attackers also integrate recently published exploits into their bots to react quickly to new trends."

12 Holz, *ibid.*

13 Holz, *ibid.* Peer-to-peer file-sharing networks are a very dangerous source of malware, in general. One study in early 2004 reported that nearly half of the executable files on Kazaa contained malware: Kim Zetter, "Kazaa Delivers More Than Tunes" *Wired.com* (9 January 2004), online: <http://www.wired.com/news/business/0,1367,61852,00.html>.

14 Larry Seltzer, "New Bagle Worm Variant Can Run Without Launching Attachment" *eWeek* (18 March 2004), online: <http://www.eweek.com/article2/0,1759,1656339,00.asp>.

[15] The Bofra worm illustrates just one of the methods used to take advantage of vulnerable browser software. The Bofra worm sets up a malicious web server on an infected computer and emails the link to victims using its own SMTP engine. The victim is infected when it follows the link to the malicious website. Once the victim is infected, the worm opens a backdoor and also instructs the computer to connect to one of a series of IRC servers to listen to further commands directed to the botnet. See John Leyden, "Bofra worm sets trap for unwary" *The Register* (10 November 2004)<http://www.theregister.de/2004/11/10/bofra_worm/>; "Sophos explains how the Bofra worm spreads" *Sophos* (9 November 2004), <http://www.sophos.com/virusinfo/articles/howbofrawork.html>.

[16] Symantec, "Symantec Internet Security Threat Report: Trends for July 04–December 04" Volume VII (March 2005) (hereinafter "Symantec, Internet Threat Report''), online: <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539/> at 56; McAfee Inc.,"Virus Profile, W32.Gaobot.worm.gen" (update 24 May 2004), online: <http://vil.nai.com/vil/content/v_100785.htm>. According to McAfee, the Gaobot family contained 1350 variants as of May 2004; Symantec, "W32.HLLW.Gaobot", online: <http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.html>; Symantec, "W32.Spybot.worm", online: <http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html>; Symantec, "W32.Mytob@mm,", online: <http://www.symantec.com/avcenter/venc/data/w32.mytob@mm.html>.

[17] Examples include the Litmus bot (Symantec, "Backdoor.Litmus", <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.litmus.html>) or SlackBot (Symantec, "Backdoor.Slackbot.B", <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.slackbot.b.html>).

[18] Symantec, "Internet Threat Report" *supra* note 16 at 56.

[19] See IRCHelp.org's tutorial and primer on IRC <http://www.irchelp.org/>. Users who install an IRC client program can access an IRC network (a series of linked IRC servers) by connecting to one of the IRC servers. Communications sent by one user to the channel are relayed to all other users in the same channel throughout the network.

[20] Honeynet Project, *supra* note 9.

[21] *Ibid.*

[22] Ryan Naraine, "Botnet Hunters Search for 'Command and Control' Servers" *eWeek Enterprise News & Reviews* (17 June 2005), online: <http://www.eweek.com/article2/0,1895,1829347,00.asp>; Symantec, "Internet Threat Report" *supra* note 16 at 58: "The dependence on a centralized communication channel makes the bot network fragile, since taking down the IRC server will effectively disable communication between the bots and their master"; Bill McCarty, "Automated Identity Theft" (*2003) IEEE Security & Privacy* 89 at 90, describing the closure of botnet control channels on the DALnet IRC network after they were identified using a Windows 2000 honeynet.

[23] Honeynet project, *supra* note 9 at 8.

[24] *Ibid.* at 6.

[25] Multi-State Information Sharing and Analysis Center and United States Computer Emergency Readiness Team, "Current Malware Threats and Mitigation Strategies" *US CERT Informational Whitepaper* (16 May 2005), online: <http://www.cscic.state.ny.us/msisac/webcasts/05_05/info/mal_%20thrt_mit_strat.pdf> at 3.

[26] Symantec, "Internet Threat Report" *supra* note 16 at 58.

[27] *Ibid.*

[28] Luhrq Threat Intelligence Group, "Phatbot Trojan Analysis", *Lurhq Managed Security Solutions* (15 March 2004), online: <http://www.lurhq.com/phatbot.html>.

[29] Symantec, "Internet Threat Report", *supra* note 16 at 58.

[30] *Ibid.*

[31] Holz, *supra* note 9 at 77; Honeynet Project, *supra* note 9 at 7, 12; Symantec, "Internet Threat Report" *supra* note 16 at 76.

[32] Holz, *supra* note 9 at 77; Honeynet Project, *supra* note 9 at 7, 12.

[33] Dawn Anfuso, "Spam is more stressful than traffic" *iMedia Connection* (8 July 2004), online: <http://imediaconnection.com/content/3774.asp>, reporting on a humorous but telling Yahoo! Mail survey in which respondents compared the irritation and stress engendered by spam with that produced by traffic jams, visits to the dentist, moving house, etc.

[34] See the description of SPEWS (Spam Prevention Early Warning System) at <http://www.spews.org>.

[35] Symantec, "Internet Threat Report" *supra* note 16 at 59.

[36] Honeynet Project, *supra* note 9: "Another use for botnets is stealing sensitive information or identity theft . . . Searching some thousands [of] home PCs for *password.txt*, or sniffing their traffic, can be effective."

[37] *Ibid.* at 4.

[38] Symantec, "Internet Threat Report" *supra* note 16 at 7: "This rise in information exposure threats is partially due to the presence of bots and bot networks, which can expose confidential information on compromised computers because of their remote access capabilities."

[39] Symantec, "W32.Spybot.worm", *supra* note 16.

[40] Symantec, "Internet Threat Report" *supra* note 16 at 25.

[41] Lawrence A. Gordon *et al.*, *Ninth Annual 2004 CSI/FBI Computer Crime and Security Survey* (2004: Computer Security Institute), online: <http://www.gocsi.com> at 10: DDoS attacks were ranked second after viruses in terms of costliness.

[42] Graeme Wearden and Andy McCue, "British cybercops nab alleged blackmailers" *CNET News.com* (21 July 2004), online: <http://news.com.com/British+cybercops+nab+alleged+blackmailers/2100-7348_3-5278046.html>; John Leyden, "Cybercops seize Russian extortion masterminds" *The Register* (21 July 2004), online: <http://www.theregister.co.uk/2004/07/21/cyber_shakedown_taken_down/>; John Leyden, "Scot in court on DDoS charges" *The Register* (18 January 2005), online: <http://www.theregister.co.uk/2005/01/18/operation_casper_court/>.

[43] Will Knight, "Attack on game raises prospect of online extortion" *New Scientist* (21 April 2005), online: <http://www.newscientist.com/channel/info-tech/electronic-threats/dn7293>; Will Sturgeon, "Extortion scams 'heading your way'" *Silicon.com* (21 April 2004), online: <www.silicon.com/software/security/0,39024655,39120157,00.htm>; Robert Lemos, "Attacks disrupt some credit card transactions" *CNET News.com* (22 September 2004), online: <http://news.com.com/Attacks+disrupt+some+credit+card+transactions/2100-7349_3-5378217.html?tag=cd.top>, describing an attack against an online credit card processor, Authorize.net. The company was attacked around the time it laid off 12% of its employees, but ruled out retribution for the lay-offs as a motive due to the earlier receipt of an extortion letter.

[44] U.S. Department of Justice, "Background on Operation Web Snare: Examples of Prosecutions" (27 August 2004), online: <http://www.usdoj.gov/criminal/fraud/websnare.pdf>.

[45] *Ibid.*

[46] Kevin Poulsen, "FBI busts alleged DDoS Mafia" *Security Focus* (26 August 2004), online: <http://www.securityfocus.com/news/9411>.

[47] *Ibid.*

[48] Brian McWilliams, "Yaha Worm Takes Out Pakistan Government's Site" *Security Focus* (26 June 2002), online: <http://online.securityfocus.com/news/501>.

[49] "Playgirl email virus gets political and attacks Chechen rebel Web sites, Sophos reports" *Sophos* (9 December 2004), online: <http://www.sophos.com/virusinfo/articles/maslanc.html>.

[50] Anthony Faiola, "Anti-Japanese Hostilities Move to the Internet" *Washington Post.com* (10 May 2005), online: <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/09/AR2005050901119.html>.

[51] Reuters, "Worm Aims to Disarm Spam Fighters" *Wired News* (2 December 2003), online: <http://www.wired.com/news/technology/0,1282,61434,00.html>; Hiawatha Bray, "Saboteurs hit spam's blockers" *The Boston Globe* (28 August 2003), online: <http://www.boston.com/news/nation/articles/2003/08/28/saboteurs_hit_spams_blockers/>.

[52] David Geer, "Malicious Bots Threaten Network Security", (January 2005) IEEE Computer 18 at p. 20, citing Alfred Huger of the Symantec Security Response Team.

[53] Robert Lemos, "Alarm growing over bot software" *CNET News.com* (30 April 2004), online: <http://news.com.com/2100-7349_3-5202236.html>.

[54] Brian Krebs, "Adware Firm Accuses 7 Distributors of Using 'Botnets'" *Washington Post* (16 August 2005), online: <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/16/AR2005081600727.html>.

[55] Honeynet project, *supra* note 9 at 4.

[56] *Ibid.*.

[57] John Leyden, "Botnet used to boost online gaming scores" *The Register* (21 December 2004), online: <http://www.theregister.co.uk/2004/12/21/randex_botnet_fun_and_games/>.

58 Symantec, "Internet Threat Report," *supra* note 16 at 58.

59 McAfee Inc., "McAfee AVERT Reports That Top Threats for Q2 2005 Include Money Making Schemes and a Rise in BOTS and Spyware" (11 June 2005), online: <http://www.mcafeesecurity.com/us/about/press/mcafee_enterprise/2005/20050711_182503.htm>.

60 Dinesh C. Sharma, "Study: Broadband penetration to surge by 2010" *CNet News.com* (2 August 2005), online: <http://news.com.com/2100-1034_3-5815756.html>, reporting a Forrester Research study predicting a jump from 29% to 62% household broadband access by 2010 in the United States.

61 Symantec, "Internet Threat Report," *supra* note 16 at 76.

62 Holz, *supra* note 9 at 77-78; Honeynet Project, *supra* note 9 at 5.

63 The Symantec Glossary includes the following entry for "polymorphic": "A virus that can change its byte pattern when it replicates, thereby avoiding detection by simple string-scanning techniques", online: <http://securityresponse.symantec.com/avcenter/glossary/index.html#p>.

64 McAfee Inc., "Virus Profile, W32/polybot.gen!IRC,?" (10 March 2004), online: <http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101090>.

65 John Leyden, "Phatbot arrest throws open trade in zombie PCs" *The Register* (12 May 2004), online: <http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/>; John Leyden, "The illicit trade in compromised PCs" *The Register* (30 April 2004), online: <http://www.theregister.co.uk/2004/04/30/spam_biz/>; John Leyden, "Hackers plot to create massive botnet" *The Register* (3 June 2005), online: <http://www.theregister.co.uk/2005/06/03/malware_blitz/>; Joris Evers, "Hacking for Dollars" *News.com* (6 July 2005), online: <http://news.com.com/Hacking+for+dollars/2100-7349_3-5772238.html?tag=st.rn>, reporting that "[s]pammers, phishers and others who want to rent out a network of about 5,500 zombies typically pay about $350 a week, according to security company Symantec".

66 Brian Krebs, "For Spammers, Worm Turns a Profit" *Washington Post.com* (7 February 2005), online: <http://www.washingtonpost.com/wp-dyn/articles/A4873-2005Feb7.html>, quoting Johannes Ullrich of SANS Internet Storm Center, who reports seeing asking prices as high as $25 per infected home computer.

67 *Supra* note 65.

68 Bob Sullivan, "Virus Writers Trade Insults as E-mail Users Suffer" *MSNBC News* (3 March 2004), online: <http://www.msnbc.msn.com/id/4422372/>; "E-mail users caught in virus feud" *BBC News* (4 March 2004), online: <http://news.bbc.co.uk/2/hi/technology/3532009.stm>.

69 See the discussion of the challenges of addressing cybercrime using traditional models of criminal law in Susan Brenner, "Toward a Criminal Law for Cyberspace: Product Liability and Other Issues" (2005) 8 Pgh J. Tech. L. & Pol'y 1 at 14–18.

70 Chandler, "Security in Cyberspace", *supra* note 7 at 242.

71 "Ultimately, huge numbers of poorly secured PCs degrade the reliability, capacity, and trustworthiness of the entire network to the detriment of all. The presence of large numbers of easy targets motivates more effort in discovering and applying attacks, increasing the likelihood that one's own machine will be compromised." Clark Ray, "A Modest Proposal: Licensing Personal Computers and Internet Service Providers" *Proceedings of the 2003 IEEE Workshop on Information Assurance*, (June 2003), at 151.

72 MS-ISAC and US-CERT, *supra* note 25 at 2.

73 *Ibid.*

74 A Microsoft-sponsored study comparing the software patch management costs of Windows systems versus open source systems reveals the astounding cost of the patch management system. Enterprises spend hundreds of dollars each year per computer system. The figures do not include the resources expended on detecting the vulnerabilities and engineering the patches: Theo Forbath, Patrick Kalaher and Thomas O'Grady, "The total cost of security patch management: A comparison of Microsoft Windows and open source software" *Wipro Technologies Ltd.* (April 2005), online: <http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf>.

75 *Supra* note 4 at 5-6: Graff and van Wyk estimate that 10–15% of security patches introduce new security vulnerabilities.

76 Paul Roberts, "New Trojan masquerades as Windows XP update" *Computerworld.com* (9 January 2004), online: <http://computerworld.com/securitytopics/security/story/0,10801,88940,00.html>.

77 Stephen E. Henderson & Matthew E. Yarbrough, "Frontiers of Law: The Internet and Cyberspace: Suing the Insecure?: A Duty of Care in Cyberspace" (2002) 32 N.M.L. Rev. 11 at 23.

78 Government of Canada, "Stopping Spam: Creating a Stronger, Safer Internet" (May 2005), online: <http://e-com.ic.gc.ca/epic/Internet/inecic-ceac.nsf/en/h_gv00317e.html>.

79 *Ibid.* The best practices are outlined in Appendix B to the Report. The Report also notes at page 4 that "[t]he adoption of these [best] practices will also address spam-related security issues, since spam is often the vehicle for more harmful activities".

80 Dan Ilett, "Web bookies demand higher security standards" *ZDNet UK* (5 April 2005), online: <http://news.zdnet.co.uk/internet/security/0,39020375,39193981,00.htm>.

81 Alorie Gilbert, "Developing nations losing spam battle, report says" *CNET News.com* (27 May 2005), online: <http://news.com.com/2100-7348_3-5723435.html>; Spamhaus, "Should ISPs be profiting from knowingly hosting spam gangs?" (4 February 2005), online: <http://www.spamhaus.org/news.lasso?article=158>; Mark Ward, "Spam blacklist targets Telewest" *BBC News* (9 May 2005), online: <http://news.bbc.co.uk/1/hi/technology/4528927.stm>; Joris Evers, "ISPs versus the zombies" *ZDNet Australia* (21 July 2005), online: <http://zdnet.com.au/insight/security/soa/ISPs_versus_the_zombies/0,39023764,39203478-1,00.htm>, suggesting that "Ultimately, if an ISP's network becomes infested with zombies, other providers will block traffic from that network ...".

82 Ray, *supra* note 71 at 152.

83 *Ibid.*

84 Some universities disable the accounts of infected users or fine those who inadvertently spread viruses. Others require signed statements that security patches are up to date. See Associated Press, "Colleges Crack Down on Viruses" *Wired News* (4 September 2003), online: <http://www.wired.com/news/technology/0,1282,60299,00.html>; Brian Krebs, "Universities Rush to Protect Networks" *Washington Post* (4 September 2003), online: <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A25845-2003Sep4&notFound=true>.

85 Johannes Ullrich, "Internet Service Providers: The Little Man's Firewall?" *SANS Institute*, online: <http://www.sans.org/rr/special/index.php?id=isp_blocking>.

86 "Stopping Spam", *supra* note 78: The best practices are outlined in Appendix B to the Report. The Report also notes at page 4 that "[t]he adoption of these [best] practices will also address spam-related security issues, since spam is often the vehicle for more harmful activities".

87 *Ibid.* at 38: Port 25 is used by the SMTP protocol to send and receive email. If port 25 is blocked, users will be required to send email through the ISP's email server, and will be unable to run their own email servers. In that way, ISPs can monitor for unusually high email traffic coming from a user. For further discussion see Jim Hu, "Comcast takes hard line against spam" *ZDNet News* (10 June 2004), online: <http://news.zdnet.com/2100-3513_22-5230615.html>.

88 "Stopping Spam", *supra* note 78.

89 U.S. Federal Trade Commission, "FTC, Partners Launch Campaign Against Spam 'Zombies'" (24 May 2005), online: <http://www.ftc.gov/opa/2005/05/zombies.htm>.

90 See e.g., Jelena Mirkovic, Gregory Prier and Peter Reiher, "Attacking DDoS at the Source" (2002) *Proceedings of 10th IEEE International Conference on Network Protocols*, online: <http://www.cis.udel.edu/~sunshine/publications/404_mirkovic_j.pdf>.

91 Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms" (2004) 34(2) *ACM SIGCOMM Computer Communications Review* 39, online: <http://www.cis.udel.edu/~sunshine/publications/ccr.pdf> at 13: "The goal of DDoS defense mechanisms deployed at the source network is to prevent network customers from generating DDoS attacks. Such mechanisms are desirable, but motivation for their deployment is low since it is unclear who would pay the expenses associated with this service."

92 Joris Evers, "ISPs versus the zombies" *ZDNet Australia* (21 July 2005), online: <http://zdnet.com.au/insight/security/soa/ISPs_versus_the_zombies/0,39023764,39203478-1,00.htm>.

93 See, e.g., the filtering policies described at the following universities: Seattle Pacific University, online: <http://www.spu.edu/CISHelpDesk/email/filtering.asp>; University of Cambridge, Engineering Department, online: <http://www-h.eng.cam.ac.uk/help/mail/filters.html>.

94 See, e.g., the UK ISP Fastnet, <http://www.fastnet.co.uk/index.php?path=services/mail_filtering_suite/virus_filtering_faq.php>.

95 Prolexic Technologies, "The Prolexic Zombie Report: Q1-Q2 2005", online: <http://www.prolexic.com/zr/>. Larger ISPs may be at a disadvantage as they may have lower rates of infection but greater absolute numbers of compromised PCs. See John E. Dunn, "Study: AOL leads ISPs in 'zombie' computer infections" *Computerworld* (20 June 2005), online: <http://www.computerworld.com.au/index.php/id;2048638993;relcomp;1>; John Leyden, "AOL rebuts zombie network slur" *The Register* (16 June 2005), online: <http://www.theregister.co.uk/2005/06/16/aol_rebuffs_prolexic_zombie_report>.

96 Comcast.net, which hosted the second highest number of zombies in the U.S. according to Prolexic, offers a range of security services free to subscribers: <http://www.comcast.net/security/>.

97 Byron Acohido and Jon Swartz, "Tech industry presents less-than-unified defense" *USA Today* (9 September 2004), online: <http://www.usatoday.com/tech/news/computersecurity/2004-09-09-zombie-response_x.htm>, quoting John Dreiling VP of Charter Communications, "How do I put enough resources in front of this problem without creating a cost model so high that I price myself out of business?"

98 *Ibid.*

99 "Stopping Spam", *supra* note 78, Appendix B, at 37. The Working Group that developed the best practices recommendations for ISPs was anxious that its recommendations not become mandatory requirements or be perceived as anything other than strictly voluntary. The Working Group was largely made up of representatives of network operators.

100 Ray, *supra* note 71 at 155: Ray notes the possibility that the extra burdens he recommends might be beyond the capacities of smaller ISPs, but suggests that smaller ISPs could outsource "software maintenance" functions.

101 Lichtman and Posner suggest at p. 23–26 that the exclusion of users as a result of higher prices would have costs in the form of the loss of the positive externalities that new users generate by joining cyberspace. Nevertheless, they point out that the response ought not to be tort immunity. Instead, they suggest government subsidies might be provided to ensure that Internet access remains affordable, while preserving the incentives for security that ISP liability offers. Douglas Lichtman and Eric Posner, "Holding Internet Service Providers Accountable" (2004) University of Chicago; John M. Olin, "Law & Economics Working Paper No. 217 (2nd Series)", available on the Social Science Research Network, online: <http://ssrn.com>.

102 It is desirable that the "least cost avoider" be charged with solving the problem. However, it is not clear that end-users, in the aggregate, are the least cost avoiders. While their individual avoidance costs may be low, there are many of them. It may be more efficient to have a smaller group of ISPs addressing the problem.

103 OpenNet Initiative, "Telus Blocking of Labor Union Web Site Filters 766 Unrelated Sites", online: <http://www.opennetinitiative.net/bulletins/010/ONI-010-telus.pdf>: The blocking took place from July 25, 2005 until July 28, 2005 when Telus reinstated access. Telus maintained that its action was justified because the site contained confidential information, encouraged people to tie up the call centre phone lines, and endangered those crossing the picket line by posting their photographs.

104 Ray, *supra* note 71 at 153. He suggests that users be shielded from liability for copyright infringement that comes to light as a result of the software maintenance scanning, in order to overcome the anticipated public resistance to his proposal.

105 *Ibid.* at 156.

106 For example, they may pay for a mail reflector service. An example of a mail reflector service is at <http://www.no-ip.com/services/managed_mail/inbound_port_25_unblock.html>.

107 Brian Krebs, "For Spammers, Worm Turns a Profit" *Washington Post.com* (7 February 2005), online: <http://www.washingtonpost.com/wp-dyn/articles/A4873-2005Feb7.html>, quoting Johannes Ullrich of SANS Internet Storm Center who reports seeing asking prices as high as $25 per infected home computer.

108 Nick Farrell, "Chinese in a stir-fry over spam: Country is routinely used to relay spam" *Computing* (5 March 2002), online: <http://www.computing.co.uk/vnunet/news/2117860/chinese-stir-fry-spam>.

109 R.S.C. 1985, c. H-6. subsection 13(3) provides: "For the purposes of this section, no owner or operator of a telecommunication undertaking communicates or causes to be communicated any matter described in subsection (1) by reason only that the facilities of a telecommunication undertaking owned or operated by that person are used by other persons for the transmission of that matter."

110 *Copyright Act*, R.S.C. 1985, c. C-42, paragraph 2.4(1)(*b*) provides that "for the purposes of communication to the public by telecommunication . . . a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public. . . ."

111 [2004] 2 S.C.R. 427.

112 Canada, Bill C-60, *An Act to amend the Copyright Act*, First Session, Thirty-eighth Parliament, 53-54 Elizabeth II, 2004-2005, First Reading June 20, 2005, <http://www.parl.gc.ca/PDF/38/1/parlbus/chambus/house/bills/government/C-60_1.PDF>.

113 See e.g., Michael L. Rustad and Thomas H. Koenig, "Rebooting Cybertort Law" (2005) 80 Wash. L. Rev. 335, and Lichtman and Posner, *supra* note 101. Even in the case of the transmission of malicious code, and despite the significant differences between defamatory content and harmful computer code, a court held that the *Communications Decency Act* insulated an ISP (*Green v. America Online* 318 F. 3d 465 (3rd Cir. 2003)).

114 Rustad and Koenig, *ibid.* at 382.

115 *Ibid.* at 412.

116 *United States v. Jay Echouafni et al.*, (Operation Cyberslam), online: <http://www.usdoj.gov/criminal/fraud/websnare.pdf>.

117 Lawrence A. Gordon *et al.*, *Ninth Annual 2004 CSI/FBI Computer Crime and Security Survey* (2004: Computer Security Institute), <http://www.gocsi.com> at 10: DDoS attacks were ranked second after viruses in terms of costliness.

118 Ilett, *supra* note 80.

119 This form of liability is not a form of vicarious liability. Vicarious liability exists where a defendant is responsible for the wrong committed by a third party, even though the defendant has not directly committed a tort. This is distinct from a situation in which a defendant is held personally negligent for having created an unreasonable risk of harm by a third party.

120 Robert M. Solomon, R.W. Kostal and Mitchell McInnes, *Cases and Materials on the Law of Torts*, 6th ed., (Scarborough Ont.: Thomson, Carswell, 2003) at p. 288–290.

121 *Cooper v. Hobart*, [2001] 3 S.C.R. 537.

122 *Ibid.*

123 Chandler, "Security in Cyberspace" *supra* note 7 at 257.

124 *Supra* note 95.

125 See, e.g., *Hewson v. Red Deer* (1976), 63 D.L.R. (3d) 168 (Alta. T.D.)

126 Ilett, *supra* note 80.

127 The characterization of intangible property is problematic, particularly in our present electronic information age. Some authors have argued that the destruction of electronic data should be treated as property damage (e.g., Robert D. Sprague, "Software Products Liability: Has Its Time Arrived?" (1991) W. St. U.L. Rev. 137 at 159–162), although there is contrary judicial authority (*Seaboard Life Insurance Co. v. Babich*, [1995] B.C.J. No. 1868 (B.C.S.C.)).

128 G.H.L. Fridman, *The Law of Torts in Canada* (Toronto: Carswell, 2002) at 813.

129 This concern was expressed by Justice Cardozo in *Ultramares Corp. v. Touche* (1931), 174 N.E. 441, 255 N.Y. 170 (C.A.), where he noted the risk of ruinous and open-ended liability ". . . in an indeterminate amount for an indeterminate time to an indeterminate class". The Supreme Court of Canada considers the "spectre of unlimited liability to an unlimited class" when deciding whether to recognize a novel duty of care in negligence (*Cooper v. Hobart* (2001), 206 D.L.R. (4th) 193 (S.C.C.)), and when deciding whether to permit the recovery of pure economic loss in a novel context ("the scope of indeterminate liability remains a significant concern underlying any analysis of whether to extend the sphere of recovery for economic loss" (*Martel Building Ltd. v. Canada* (2000), 193 D.L.R. (4th) 1 (S.C.C.)).

130 Bruce Feldthusen, *Economic Negligence*, 4th ed., (Scarborough, Ontario: Thomson Canada Ltd., 2000) at 11.

131 John G. Fleming, *The Law of Torts*, 9th ed., (Sydney: Law Book Co. Ltd., 1998) at 193.

[132] *Martel Building Ltd. v. Canada* (2000), 193 D.L.R. (4th) 1 (S.C.C.).

[133] Dan B. Dobbs, *The Law of Torts* (St. Paul: West Group, 2000), at 1030, and Feldthusen, *supra* note 130 at 1-2.

[134] (1974) 501 F. 2d 558 (9th Cir.).

[135] Feldthusen, *supra* note 130 at 252.

[136] Lewis Klar, *Tort Law*, 3rd ed., (Toronto: Thomson Carswell, 2003), at 472.

[137] *Ibid.*

[138] *Heeney v. Best* (1979), 108 D.L.R. (3d) 366 (Ont.C.A.).

[139] Anti-DDoS services can be very expensive, reportedly $12,000 per month when supplied by large US ISPs. Denise Pappalardo and Ellen Messmer, "Extortion via DDoS on the Rise" *Computerworld* (16 May 2005), online: <http://www.computerworld.com/printthis/2005/0,4814,101761,00.html>.

[140] Mirkovic and Reiher, *supra* note 91 at 9: "[T]here are many possible DDoS attacks, very few of which can be handled only by the victim. It is frequently necessary to have a distributed, possibly coordinated response system . . . . Many vendors and researchers make bold claims that their solution completely handles the DDoS problem. There is currently no benchmark suite of attack scenarios or established evaluation methodology that would enable comparison between defense systems. Such a situation is likely to discourage networks from investing in DDoS protection, since they cannot be assured of the quality of the product being purchased."

[141] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms" (2004) 34(2) *ACM SIGCOMM Computer Communications Review* 39, online: <http://www.cis.udel.edu/~sunshine/publications/ccr.pdf> at 13: "The goal of DDoS defense mechanisms deployed at the source network is to prevent network customers from generating DDoS attacks. Such mechanisms are desirable, but motivation for their deployment is low since it is unclear who would pay the expenses associated with this service."