

# **DISTRIBUTED DENIAL OF SERVICE**

## **LAW, TECHNOLOGY & POLICY**

**MEIRING de VILLIERS**

**John Landerer Faculty Fellow**

**University of New South Wales, School of Law**

**Sydney, NSW 2052**

**AUSTRALIA**

**[mdv@unsw.edu.au](mailto:mdv@unsw.edu.au)**

## ABSTRACT

A Distributed Denial of Service (DDoS) attack aims to deprive legitimate users of a resource or service provided by a system, by overloading the system with a flood of data packets, thus preventing it from processing legitimate requests. This article analyzes the doctrines governing the allocation of liability among key players in a DDoS attack. The doctrines are well established and based on common law tort principles and policy considerations. The main contribution of the article is the adaptation of these principles to the novel technological environment in which DDoS attacks occur. The analysis shows that detailed understanding of the technologies and analysis of their role in DDoS attacks are essential to effective judicial decisionmaking.

## INTRODUCTION

Advances in computing and communications technology have taken global prosperity to unprecedented levels, but have simultaneously exposed information infrastructures to new risks. The Internet, with its promiscuous interconnectivity and interdependence, has become increasingly susceptible to escalating cyber attacks emanating from a variety of wrongdoers, such as cyber criminals, terrorist groups, and perhaps even rogue nation states.<sup>1</sup>

Denial of service (DoS) attacks have emerged as a significant cyber attack weapon. A DoS attack aims to deprive legitimate users of a resource or service provided by a system, by overloading the system with a flood of data packets, thus preventing it from processing legitimate requests. In a recent denial of service incident, for instance, a hacker launched an attack on the Port of Houston, the eighth biggest shipping port in the world. The attack made crucial navigating data on the port's Web service temporarily

---

<sup>1</sup> See, e.g., Richard D. Pethia, *Cyber Security - Growing Risk from Growing Vulnerability*, 25 June 2003, Testimony before the House Select Committee on Homeland Security [Stating that "as critical infrastructure operators strive to improve their efficiency and lower costs, they are connecting formerly isolated systems to the Internet to facilitate remote maintenance functions and improve coordination across distributed systems. Operations of the critical infrastructures are becoming increasingly dependent on the Internet and are vulnerable to Internet based attacks."]

unavailable to shipping pilots and mooring companies, creating substantial collision and other risks.<sup>2</sup>

Distributed denial of service (DDoS) attacks seek to achieve the same goal on a larger scale, by enlisting multiple machines to send attack traffic to victims. The enlisted machines are known as "zombies" or "agents," and are attractive intermediaries to attackers, usually because of their poor security, such as porous firewalls.<sup>3</sup> An attacker typically breaks into and takes control of these vulnerable agents, and mobilizes them as launching pads to overload the ultimate target with traffic.

There are two main categories of denial of service attacks, namely vulnerability attacks and flooding attacks. Vulnerability attacks, as the name suggests, exploit a vulnerability in the target application. For instance, a vulnerability known as the buffer overflow,<sup>4</sup> allows an attacker to remotely inject malicious code into a target and deny service from a distance. The malicious code may, for instance, be programmed to severely slow down or crash the target, by monopolizing a significant amount of memory, bandwidth and computational power. A flooding attack does not exploit a vulnerability, but simply overwhelms the resources of its target with a vast number of apparently legitimate messages.<sup>5</sup> An attack can, of course, fall into both categories. This article focuses on liability issues related to vulnerability attacks.

Tactical exploitation of vulnerabilities in information systems plays an important role in DDoS attacks, especially vulnerability attacks.<sup>6</sup> The infamous Internet worm,

---

<sup>2</sup> See S. Gibson, *The Strange Tale of the Denial of Service Attacks against GRC.COM*, at <http://grc.com/dos/grcdos.htm>.

<sup>3</sup> A firewall is a system that controls access to a network by enforcing an access policy. It allows access only to traffic that meet certain criteria. A misconfigured or malfunctioning firewall may allow malicious data packets to enter. See, e.g., Mark Egan, *THE EXECUTIVE GUIDE TO INFORMATION SECURITY THREATS, CHALLENGES, AND SOLUTIONS* (Symantec Press, 2005), at 35; John R. Vacca and Scott R. Ellis, *FIREWALLS JUMPSTART FOR NETWORK AND SYSTEMS ADMINISTRATORS* (2005), 7-14.

<sup>4</sup> The buffer overflow is discussed, *infra*, at xxx.

<sup>5</sup> Jelena Mirkovic et al., *INTERNET DENIAL OF SERVICE ATTACK AND DEFENSIVE MECHANISMS* (2005), at 15-17, 27-28, 79-81.

<sup>6</sup> N. Hanebutte and P.W. Oman, *Software Vulnerability Mitigation as a Proper Subset of Software Maintenance*, *Journal of Software Maintenance and Evolution Research and Practice* 17, 2005, 379, at 381 ["Cyber attacks take advantage of one or more vulnerabilities and can encompass several coordinated intrusions."]; Ron Brandis, *Common System Security Risks and Vulnerabilities and How Malicious Attackers Exploit Them*. Bridgepoint White Paper (2001), at 1. <http://bridgepoint.com.au>. ["A few software vulnerabilities account for the majority of successful attacks because attackers are opportunistic - taking the easiest and most convenient route. ... They rely on organizations not fixing the problems (applying patches), and they often attack indiscriminately, by scanning the Internet for vulnerable systems."]; K.J. Houle and G.M. Weaver, *Trends in Denial of Service Attack Technology*, CERT Coordination Center White Paper, Carnegie Mellon Univ., 2001, at 9 ["This deployment (of DoS attack tools) depends on the

W32/CodeRed, exploited a vulnerability in Microsoft's Internet Information Services (IIS) web servers,<sup>7</sup> and attempted to launch denial of service attacks on the official White House Web page.<sup>8</sup> More destructive sequels of CodeRed followed, which were similar to their predecessor and exploited the same vulnerability.<sup>9</sup> The sequels had an even greater impact on the global information infrastructure, in part due to more efficient propagation algorithms.<sup>10</sup> The new versions spread multiple times faster and also created a back door<sup>11</sup> on infected systems. The backdoor enabled hackers to gain remote, administrator-level access to the infected machine, and to use it as a launching pad for further denial of service attacks.<sup>12</sup>

The success of a DDoS attack involves the cooperation of a number of players. The chain consists of (1) The attackers; (2) Computer users whose machines are enlisted

---

presence of exploitable vulnerabilities on systems and the ability of intruders to exploit those vulnerabilities."]; Symantec Internet Security Threat Report [Trends for July 05 - December 05], Vol. IX, Published March 2006, at 25 ["Attributing the success of an attack to "the high volume of computers running vulnerable software."]; Jelena Mirkovic et al, INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS (2005), at 66. ["Worms spread extremely fast because of their parallel propagation pattern. ... Frequently, this huge amount of scanning and attack traffic clogs networks and creates a DoS effect. Some worms carry DDoS payloads as well, allowing the attacker who controls the compromised machines to carry out more attacks after the worm has finished spreading."]

<sup>7</sup> The attacks occurred shortly after Microsoft had discovered the vulnerability and issued a patch to fix it. Microsoft, *A Very Real and Present Threat to the Internet*. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/codealrt.asp>. Section xxx discusses the principles of the buffer overflow vulnerability.

<sup>8</sup> CodeRed infected over 300,000 machines within 24 hours. Peter Szor, *THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE* (Symantec Press, 2005), at 98.

<sup>9</sup> Attacks occurred despite the fact that a patch had been issued for the vulnerability by Microsoft before the first attack. The Code Red-I as well as Code Red II worms could, for instance, not infect a system that had the MS01-033 patch installed. See, e.g., Baca, at 6 ("There was so much publicity and so many published articles by the time Code Red II hit, that any competent server manager would have had ample opportunity to patch their systems in time.") CodeRed-II also compromised devices with web interfaces, such as routers, switches, DSL modems, and printers. See, e.g., Cisco Systems, Inc., *Cisco Security Advisory: Code Red Worm - Customer Impact*. <http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml>.

<sup>10</sup> CodeRedII infected more than 359,000 computers in fourteen hours. See, e.g., Silicon Defense, *Code Red Analysis Page*. <http://www.silicondefense.com/cr/>.

<sup>11</sup> A back door is a method of gaining remote access to a computer, and is usually not detectable by casual inspection. A backdoor may, for instance, consist of a password recognition routine installed in the computer, perhaps as a modification of a legitimate program. The routine would enable a hacker who provided the right input to gain access to confidential files and programs on the computer. See, e.g., Kevin J. Connolly, *LAW OF INTERNET SECURITY AND PRIVACY* (2004), § 4.02.

<sup>12</sup> Jeremy D. Baca, *Windows Remote Buffer Overflow Vulnerability and the Code Red Worm*. SANS Institute White Paper (September 10, 2001), at 5.

by the attackers and turned into zombies, (3) Target Internet sites; (4) The software vendor responsible for the exploited security vulnerabilities, and (5) Network intermediaries and backbone network service providers, who deliver the attack traffic.<sup>13</sup>

A case involving a DDoS attack is a typical "concurrent efficient causes case."<sup>14</sup> A concurrent efficient causes case is one where several defendants' wrongdoing are but-for causes of the same harm. Typically, one defendant, the original tortfeasor, is responsible for the original cause of the harm. Then, a subsequent tortfeasor intervenes and commits a second tort, which is also a but-for cause of the same harm. The last wrongdoer's liability is undisputed, but a plaintiff may be interested in suing the original tortfeasor, who may be the only solvent defendant.

In a DDoS attack, the actual attackers are the immediate wrongdoers, but courts may extend liability to other tortfeasors who have contributed to the attack. Vendors of vulnerable software may be held liable for facilitating DDoS attacks, and owners of inadequately secured zombie and target computers may be held liable for failing to take corrective precautions that could have prevented the attack. The vendor may also be held liable for exposing the victims of the attack to the inadvertent failure of the computer owners to fix the vulnerability.

The rules allocating liability in concurrent efficient causes cases are well established and based on common law tort principles and policy considerations. These principles are generally applicable to societal risks, including risks associated with information security.<sup>15</sup> The main contribution of this article is the adaptation of these principles to the novel technological environment in which a DDoS attack occurs.

An original tortfeasor, such as a vendor of vulnerable software, may be held liable for providing encouragement to attackers. A doctrine, known as the Encourage Free Radicals (EFR) doctrine, preserves the liability of an original tortfeasor who has encouraged the opportunistic behavior of so-called "free radicals."<sup>16</sup> Free radicals are individuals who are not deterred by the threat of liability, because they are judgment-

---

<sup>13</sup> Margaret Jane Radin, *Distributed Denial of Service Attacks: Who Pays? (Part 1)*, CYBERSPACE LAWYER, (Dec 2001), 2 ["What is a DDoS Attack?"]

<sup>14</sup> Mark F. Grady, *Proximate Cause Decoded*, 50 UCLA L. REV. 293, 299 (2002).

<sup>15</sup> See PROSSER AND KEETON ON THE LAW OF TORTS (5th ed., West Publ. Co., 1984), § 31. Second Restatement of Torts, § 282 (Describing negligence as conduct "which falls below the standard established by law for the protection of others against unreasonable risk of harm.") See, also, Dan B. Dobbs, *The Law of Torts*, at 258 (The plaintiff can assert that *any* conduct counts as negligence.)

<sup>16</sup> The EFR doctrine was pioneered by Professor Mark Grady. See Mark F. Grady, *The Free Radicals of Tort*, SUPREME COURT ECONOMIC REVIEW, 2004, 189.

proof, elusive, protected by anonymity, or blinded by ideological or religious motivations. Examples of free radicals include children, anonymous crowds, criminals, terrorists, and mentally incompetent individuals. The policy rationale behind the EFR doctrine is that solvent defendants should not be allowed to escape judgment by shifting liability to judgment-proof and undeterrable individuals. The deterrence rationale of tort law would otherwise be defeated and plaintiffs left without compensation.<sup>17</sup> An analysis of the nature and motivations of DDoS attackers, DDoS attack and defense technology, and the architecture of the Internet, suggests that cyber attackers exhibit properties commonly associated with free radicals, and that the factors that influence courts in holding a defendant liable for encouraging free radicals are present in a typical DDoS attack.

Negligence law distinguishes sharply between intentional and inadvertent negligence. Courts are more likely to impose liability on an original tortfeasor if his encouragement of a free radical was intentional, and if the resulting harm was serious. Courts may also extend liability for a DDoS attack to tortfeasors who intentionally failed in their duty to take a corrective precaution, such as owners of the intermediate and target computers whose failure to correct a security vulnerability was an efficient cause of the attack. And courts extend liability to tortfeasors who intentionally exposed a plaintiff to the inadvertent negligence of a third party. It is therefore important to courts to be able to classify a defendant's action as intentional or inadvertent.

Although direct proof of a defendant's state of mind is not always available, technology provides a key to classifying a particular instance of negligence as intentional or inadvertent. Information security precautions consist of a durable, long-lived component (such as a vulnerability scanner), complemented by repetitive, non-durable components (such as regularly monitoring the scanner output). The analysis in the article shows that failure to implement a durable precaution is likely the result of intentional negligence. Failure to comply with a non-durable precaution, on the other hand, is likely due to an inadvertent oversight. It may therefore be inferred that a vendor's failure to take a durable precaution which facilitated a DDoS attack likely constitutes intentional encouragement of an attacker. The vendor may also be held liable for intentionally exposing the victim of the attack to the inadvertent negligence of a third party, such as the user of a zombie computer, provided the third party's negligence was indeed inadvertent.

---

<sup>17</sup> Mark F. Grady, *Proximate Cause Decoded*, 50 UCLA L. REV. 293, 306-312 (2002).

The article is organized as follows. Section 2 analyzes the Free Radical concept in tort law and its application in a DDoS context. Section 3 analyzes the distinction between intentional and inadvertent negligence in tort law. Section 4 combines the concepts developed in Sections 2 and 3 to analyze liability issues that arise in connection with DDoS attacks. Section 5 briefly touches upon aspects of the economic loss rule. A final section discusses and concludes.

## 2. THE FREE RADICALS OF TORT LAW

### *Introduction*

The liability of an original tortfeasor is usually cut off by an intervening crime or intentional tort.<sup>18</sup> In *Watson v. Kentucky & Indiana Bridge & Railroad Co.*,<sup>19</sup> for instance, the defendant negligently spilled gasoline. A third party dropped a lit cigar into the spill, and ignited a blaze. The court held that if the intervening person had dropped his cigar intentionally, his act would cut off the liability of the defendant. Professor Robert Rabin comments that this proximate cause liability limitation is rooted in a desire for proportionality between degree of culpability and scope of liability.<sup>20</sup>

Such a liability shift may complicate a DDoS plaintiff's negligence claim. Consider, for instance, a vendor whose negligent quality control introduces a vulnerability into its software product. A brokerage firm purchases and installs the defective product, and it neglects to patch the vulnerability. Due to a subsequent DDoS attack, a time-sensitive transaction of a client of the brokerage could not be executed, and the client suffers losses. The wronged client may file a civil suit against the negligent vendor, the brokerage for failing to prevent the attack, as well as the attacker. However, the attacker is likely judgment-proof, if she can even be identified and tracked down. The alternative defendants, the vendor and the brokerage, are likely solvent and identifiable,

---

<sup>18</sup> Steven Shavell, *An Analysis of Causation and the Scope of Liability in the Law of Torts*, 9 J. LEGAL STUD. 463, 497 (1980) ("Criminal or intentional acts of parties other than the defendant would seem more important to discourage than those involving uncomplicated negligence, and the former but not the latter tend to exclude the defendant from the scope of liability.") Shavell cites *Carterville v Cook*, 129 Ill. 152, 22 N.E. 14 (1889) [defendant was responsible for an excavation close to a sidewalk. The plaintiff fell into the excavation and suffered injuries. The court held that if an intervening tortfeasor intentionally pushed the plaintiff into the excavation, the defendant's liability would be cut off.

<sup>19</sup> 126 S.W. 146 (Ky. 1910).

<sup>20</sup> Robert L. Rabin, *Tort Recovery for Negligently Inflicted Economic Loss: A Reassessment*, 37 STAN. L. REV. 1513, 1534.

but the intentional intervention of the attacker may cut off their liability. Such a liability shift from a solvent original tortfeasor to a judgment-proof and elusive cyber attacker may leave a DDoS victim without recourse.

The Encourage Free Radical (EFR) doctrine,<sup>21</sup> pioneered by Professor Mark Grady, provides an exception. The EFR doctrine preserves the liability of an original tortfeasor who has encouraged the opportunistic behavior of so-called free radicals. Free radicals are individuals who are not deterred by the threat of liability, because they are shielded by anonymity or insufficient assets; or because they lack the mental capacity or good judgment to care about the consequences of their actions. Examples of free radicals include children, anonymous crowds, criminals, terrorists blinded by ideological or religious motivations, and mentally incompetent persons.

The EFR doctrine can be illustrated by the facts in *Weirum v RKO General, Inc.*<sup>22</sup> In *Weirum*, the defendant radio station broadcast a contest in which a disk jockey would drive throughout Los Angeles. He would stop occasionally and announce his location on the radio. Teenagers would race to meet the disk jockey and he would give a prize to the first one who reached him. Eventually, two overeager racing teenagers drove recklessly in their pursuit of the prize, and caused a road accident in which the plaintiff's deceased was killed.

There were two concurrent efficient causes of the accident, namely the organizers of the contest and the reckless teenage drivers. The radio station negligently encouraged the free radical teenagers to drive recklessly. In accordance with the EFR doctrine, the intentional wrongdoing of the teenagers did not cut off the defendant radio station's liability. The radio station was held jointly liable with the teens and, as the deeper pocket, likely paid most of the damages.

In another well-known free radical case, the defendant, an interior decorator, neglected to lock the door of the house of a client. A burglar entered through the open door and stole the plaintiff's jewelry. The court held the defendant liable for the loss. The defendant had created an opportunity for the free radical thief that does not normally exist - valuables are usually kept under lock and key.<sup>23</sup>

In an analogous cyber case, the bookseller, Barnes and Noble, was accused of permitting rogues to gain unauthorized access to confidential client information through

---

<sup>21</sup> Mark F. Grady, *The Free Radicals of Tort*, SUPREME COURT ECONOMIC REVIEW, 2004, 189.

<sup>22</sup> 539 P.2d 36 (Cal. 1975).

<sup>23</sup> *Stansbie v Troman* [1948] 2 K.B. 48.

security vulnerabilities in its website.<sup>24</sup> The alleged security lapse, which had allowed penetration of a firewall,<sup>25</sup> is analogous to leaving a door unlocked. It had presented an unusual opportunity to free radicals - a properly functioning firewall is supposed to block cyber trespassers.

These cases illustrate the policy rationale behind the EFR doctrine, namely that the threat of negligence liability is ineffective against defendants who are undeterred by the prospect of liability. The deterrence goal of negligence law would be defeated if responsible people who foreseeably encourage tortious or criminal behaviour were allowed to escape judgment by shifting liability to undeterrable free radicals. Common law negligence rules therefore impose liability on the first tortfeasor, the encourager of the free radicals, even when intentional or criminal behavior intervenes.<sup>26</sup> The liability of a vendor who negligently created a software product with an embedded security vulnerability would be preserved, provided the security vulnerability provided encouragement to free radical cyber attackers.

The EFR doctrine only applies when a free radical is involved. If the tortfeasor encouraged by the defendant is not a free radical, and if the defendant's encouragement is insufficient to make him a co-actor with the immediate wrongdoer, then the encourager is immune to liability. A defendant would, for instance, not be held liable for encouraging a responsible citizen. If Bill Gates had responded to the *Weirum* radio broadcast by racing to collect the prize, his intervening conduct would almost certainly have cut off the radio station's liability. In the unlikely event that Gates would download a virus kit and use it to create a virus that exploits a security flaw in Windows, the creator of the kit would escape liability, and Mr. Gates held solely liable. If, however, a free radical, such as a judgment-proof hacker did the same, the kit creator's liability would likely be preserved despite the hacker's intervention.

We now turn to an analysis of cyber attackers as free radicals.

### ***DDoS attackers as free radicals***

---

<sup>24</sup> See, *Office of the New York State Attorney General, Attorney General reaches Agreement with Barnes and Noble on Privacy and Security Standard*, April 29, 2004. <http://www.oag.state.ny.us/press/2004/apr/apr29a04.html>. Barnes and Noble entered into a settlement with the New York Attorney General in April 2004.

<sup>25</sup> Firewall is defined *supra*, n. 3.

<sup>26</sup> See Mark F. Grady, *The Free Radicals of Tort*, SUPREME COURT ECONOMIC REVIEW, 2004, 189, 201, 195.

This section analyzes the nature and behavior of cyber attackers, and concludes that they exhibit properties commonly associated with free radicals.

Denial of service has free radical origins. The idea of denial of service was originally rooted in a desire to flout authority and gain recognition in the hacker underground world.<sup>27</sup> DDoS attacks have since outgrown their maverick origins, and matured into tools of crime, economic sabotage and extortion.<sup>28</sup> Regardless of whether they are involved in crime or lesser mischief, cyber wrongdoers often display a defiant attitude towards laws and law enforcement. Rogues such as the virus authors and distributors whose creations play a prominent role in DDoS attacks,<sup>29</sup> appear undeterred by the threat of legal liability and often seem unconcerned about the problems caused by their creations.<sup>30</sup> Survey evidence suggests that cyber rogues would either be unaffected or, perversely, actually encouraged by stricter legislation.<sup>31</sup>

---

<sup>27</sup> Jelena Mirkovic et al., INTERNET DENIAL OF SERVICE ATTACK AND DEFENSIVE MECHANISMS (2005), at 13 ["Some of the early DoS attacks were largely proof of concept or simple pranks played by hackers. The ultimate goal was to prove that something could be done, such as taking a high-profile Web site off-line. Such an achievement brought the attacker recognition in the underground community."]

<sup>28</sup> See, e.g., Jelena Mirkovic et al, INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS (2005), at 14 ["Sophisticated hackers may act on their own accord (when attacking for supremacy in their peer circle or for revenge) or may be hired by an underground movement or a criminal organization."]; In a recent widely reported case, an online business was been threatened with a DoS attack unless a payment was made. See, e.g., *Scotland Yard and the Case of the Rent-a-Zombies*, ZDnet.com, 7 July 2004. [http://zdnet.com.com/2100-1105\\_2-5260154.html](http://zdnet.com.com/2100-1105_2-5260154.html). See, also, Symantec Internet Security Threat Report [Trends for July 05 - December 05], Vol. IX, Published March 2006, at 12 ["(C)riminal extortion schemes based on DoS attacks are becoming more common."]; Id., at 80 ["In another type of bot-conducted cybercrime, companies have reportedly hired attackers to launch DoS attacks against competitors using bot networks."]

<sup>29</sup> Computer viruses and worms play a role in DDoS attacks, both in scanning for exploitable vulnerabilities and in carrying and executing DDoS attack code. The infamous CodeRed worm, for instance, was designed to carry out a DDoS attack from the nodes it compromised. See, e.g., Jelena Mirkovic et al, INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS (2005), at 27 ["The ultimate in automation is an Internet worm - a program that looks for vulnerable machines and infects them with a copy of its code. Worms propagate extremely rapidly. Some worms have used their armies of infected machines specifically to perform DDoS attacks. The worm can even carry the code to perpetrate the DDoS attack."]

<sup>30</sup> Sarah Gordon, *Virus Writers: The End of Innocence*. (Finding no evidence that high profile prosecutions have alleviated the computer virus problem, as measured by the rate of creation of new viruses in the wild subsequent to such persecutions.) See, also, R. Lemos (1999), *'Tis the Season for Computer Viruses*. <http://www.zdnet.co.uk/news/1999/49/ns-12098.html>. [Observing that even after the author of the Melissa virus had been apprehended (and expected to be sentenced to a multi-year prison term), the appearance of new viruses on the Internet continued to proliferate, and at an increasing rate.]

<sup>31</sup> Sarah Gordon, *Virus Writers: The End of Innocence*. [Reference to DefCon survey.] Symantec White Paper.

Cyber attackers are often judgment-proof and shielded by the anonymity of cyberspace, which emboldens them and encourages their deviant behavior.<sup>32</sup> People tend to exhibit out-of-character behavior in an anonymous crowd. In a classic nineteenth century study of mass behavior, Gustave Le Bon concluded that crowd behavior is impulsive and uncritical, and that people act very differently in crowds than they do as individuals.<sup>33</sup> Le Bon's insights about the behavior of individuals in crowds have been confirmed by more recent empirical studies by behavioral economists and social psychologists.<sup>34</sup>

The courts have recognized this phenomenon. In *Guille v Swan*<sup>35</sup>, the defendant descended in a balloon over New York City into plaintiff's garden in a manner that attracted a crowd. The balloon dragged over the plaintiff's garden, but the crowd did most of the damage to the garden. The defendant argued that he should be responsible only for his share of the damages, and not for that caused by the crowd, but the court held him responsible for all the damages. The crowd were free radicals in that particular situation. The defendant's mode of arrival foreseeably attracted the crowd, and the relative anonymity and diminished accountability inspired their behavior, a classic description of the EFR doctrine.<sup>36</sup>

The anonymity of the Internet appears to have a similar behavioral effect. Otherwise upstanding citizens in the physical world sometimes behave in antisocial and

---

<sup>32</sup> See, e.g., Stephen E. Henderson et al., *Frontiers of Law: The Internet and Cyberspace: Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M.L. REV. 11, 11 ["(T)oday's Internet can be crippled by distributed denial-of-service attacks launched by relatively unsophisticated and judgment-proof parties."], and 16 ["Similarly, in the case of a DDoS attack, the person who uses the weapon ... is generally clearly liable, but that person is often either impossible to locate, is judgment-proof, or both."]; A. Householder et al., *Managing the Threat of Denial-of-Service Attacks*, v10.0, CERT Coordination Center, October 2001, at 23 ["It is easy for attackers to avoid getting caught by hiding their identity. They command their attack network from stolen dial-up accounts and other compromised systems, and they use spoofed source addresses for attack traffic. Victim sites and law enforcement face a daunting and frequently unfeasible task to identify and prosecute attackers. Suffering few consequences - if any - for their actions, attackers continue their work. The combination of all these factors provide a fertile environment for DoS agents."]

<sup>33</sup> Gustave Le Bon, *THE CROWD: A STUDY OF THE POPULAR MIND*, at 31.

<sup>34</sup> See Richard A. Thaler, *QUASI RATIONAL ECONOMICS* (1993); Herbert A. Simon, *Theories of Bounded Rationality*, in B. McGuire and Roy Radner (eds.), *DECISION AND ORGANIZATION: A VOLUME IN HONOR OF JACOB MARSCHAK* (1972).

<sup>35</sup> 19 Johns. 381 (N.Y. 1822).

<sup>36</sup> Chief Justice Spencer stated that the defendant's manner of descent would foreseeably draw a crowd with predictable consequences, for which he should be held responsible. For a discussion of the case, see Mark F. Grady, *The Free Radicals of Tort*, *SUPREME COURT ECONOMIC REVIEW*, 2004, 189, 201, 202.

even criminal ways in the anonymous world of the Internet.<sup>37</sup> Professor Jelena Mirkovic comments, "[t]his disassociation and lack of physical proximity encourages people to participate in illegal activities in the Internet, such as hacking, denial of service, or collecting copyrighted material. They do not feel that in reality they are doing any serious harm."<sup>38</sup>

The anonymity of the Internet not only emboldens wrongdoers, but also complicates the task of detecting computer crimes and tracking down offenders, and makes it harder to obtain evidence against a wrongdoer.<sup>39</sup> The Internet provides the technological platform and opportunity to a skilled operator to assume different identities, erase his digital footprints, and transfer incriminating evidence electronically to innocent computers, often without leaving a trace.<sup>40</sup> Courts have recognized the perverse incentives and law enforcement problems created by anonymous and judgment-proof defendants in cyberspace. In *Religious Tech. Ctr. v Netcom On-Line Comm. Servs.*,

---

<sup>37</sup> J.R. Suler and W. Phillips, *The Bad Boys of Cyberspace: Deviant Behavior in Online Multimedia Communities and Strategies for Managing It* (1998). <http://www.rider.edu/~suler/psy cyber/badboys.html>. See, also, J.P. Davis, *The Experience of Bad Behavior in Online Social Spaces: A Survey of Online Users*. Microsoft Research, Social Computing Group.

<sup>38</sup> Jelena Mirkovic et al, INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS (2005), at 30.

<sup>39</sup> D. Lichtman and E. Posner, *Holding Internet Service Providers Accountable*, John M. Olin Law & Economics Working Paper No. 217, July 2004 ("Sophisticated saboteurs use the Internet's topology to conceal their tracks by routing messages and information through a convoluted path that is difficult for authorities to uncover."); Ian C. Ballon, *Alternative Corporate Responses to Internet Data Theft*, 471 PLI/Pat. 737, 739 (1997); M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, November 2000; Jelena Mirkovic et al, INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS (2005), 14 ([V]ery few attackers have been caught and prosecuted. ... [One] factor is the ease of performing a DoS attack without leaving many traces for investigators to follow. ... Another type of DoS perpetrator is a sophisticated hacker who uses several means to obscure her identity and create subtle variations in traffic patterns to bypass defenses."); Howard F. Lipson, *Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues*, CERT Coordination Center, Special Report CMU/SEI-2002-SR-009, Carnegie Mellon University, at 49 ["Although promising, research on tracking and tracing cyber-attacks is in a nascent state. the lack of proven techniques for effectively and consistently tracking sophisticated cyber-attacks to their source (and rarely to the individuals or entities responsible) severely diminishes any deterrent effect. Perpetrators feel free to act with nearly total anonymity."]

<sup>40</sup> *Spammers and Viruses Unite*, BBC News, at <http://news.bbc.co.uk/1/hi/technology/2988209.stm>. (Describing an anonymity-preserving computer hijacking program named Proxy-Guzu.) See, also, Jay Lyman, Authorities Investigate Romanian Virus Writer, at <http://www.linuxinsider.com/perl/story/31500.html> [Referring to "the difficulty of tracking down virus writers, particularly when they are skilled enough to cover their digital tracks, [so that] few offenders are ever caught."]; Noah Levine, *Note: Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526, Section I.A.

Inc.,<sup>41</sup> the court referred to misappropriation of trade secrets by free radicals, and cautioned that an anonymous or judgment proof defendant can do enormous harm and leave the plaintiff without recourse.<sup>42</sup>

Technologies such as anonymous remailers protect and encourage the users of attack technologies that rely on e-mail to propagate their artillery over the Internet. Remailers are servers which forward electronic mail to network addresses on behalf of an original sender who wishes to remain anonymous. A normal e-mail message carries a header with information about its origin, its destination and some information about the route it has taken. This information makes the true source of the message traceable. The purpose of a remailer service is to disguise the true source by delivering an e-mail message without its original header and with a fictitious return address, so as to provide the original sender with a line of defense against identification.<sup>43</sup> Many DDoS attacks rely on e-mail. A recent security update, for instance, reported a buffer overflow vulnerability which could be exploited to achieve denial of service by transmitting a specially configured HTML file by e-mail.<sup>44</sup> Such attacks could fruitfully employ an anonymizing technology such as a remailer.

DDoS attackers have created special techniques to hide their true identities. They often deploy several intermediate machines between themselves and the zombie agents they enlist to launch the actual attacks. These intermediate machines are called "handlers." To confuse matters even more, attackers may work through an additional layer of machines between their own machines and the handlers, called "stepping stones."

DDoS attackers employ additional means of obscuring their identities, such as IP spoofing. IP spoofing involves forging the address of the sender so that the attacker effectively assumes the identity of a third party, such as a legitimate client of the target system. Handlers, stepping stones and IP spoofing constitute a line of defense to DDoS

---

<sup>41</sup> 923 F.Supp. 1231, 1255-57 (9th Cir. 1995).

<sup>42</sup> See, also, C. Butler, *Plotting the Return of an Ancient Tort to Cyberspace: Toward a New Federal Standard of Responsibility for Defamation for Internet Service Providers*, 6 MICH. TELECOM. & TECH. L. REV. 247, 260 (Discussing *Zeran v America OnLine, Inc.*, 129 F.3d 327 (4th Cir. 1997), and commenting that a plaintiff injured by anonymous speech of an ISP subscriber "was left without recourse once the court held AOL to be immune from liability as a distributor of third party information content because the messages had been posted by an anonymous person whose identity was never able to be traced.")

<sup>43</sup> See, e.g., Noah Levine, *Note: Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526.

<sup>44</sup> See, e.g., *Lotus Domino Denial of Service Malformed HTML Email*, Symantec Security Update. <http://www.symantec.com/avcenter/security>.

perpetrators against investigators. If handlers and stepping stones are located in different geographic locations, perhaps different continents, it may be very difficult to trace the identity of the attacker behind the elaborate scheme.<sup>45</sup>

Deterrence is weakened if prosecution is inadequate. Cyber crimes are evidently seriously under-reported and as a consequence, under-prosecuted.<sup>46</sup> DDoS attacks occur very frequently, but very few attackers are brought to justice. This has been attributed in part to the relatively low economic impact of the typical DDoS attack, which makes a lawsuit uneconomical.<sup>47</sup> Other factors making companies reluctant to report security breaches include fear of negative publicity and difficulties in identifying attackers.<sup>48</sup> Firms seem particularly reluctant to report and prosecute cybercrimes that originate from overseas.<sup>49</sup>

---

<sup>45</sup> Jelena Mirkovic et al, INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS (2005), at 18; E.J. Sinrod and W.P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crimes Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 117, 197 ("Tracking down the attackers."), and 202 "[T]he greatest impediment to prosecuting (DDoS attackers) will continue to be technical difficulty of tracing the route of the attack back to the perpetrator."

<sup>46</sup> Sarah Gordon, *Virus Writers: The End of Innocence*. IBM White Paper, <http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.htm>. ("Minnesota statute §§ 609.87 to .89 presents an amendment which clearly defines a destructive computer program, and which designates a maximum (prison term of) ten years; however, no cases have been reported. Should we conclude there are no virus problems in Minnesota?) See, also, Michael K. Block Joseph G. Sidak, *The Cost of Antitrust Deterrence: Why not Hang a Price-Fixer Now and Then?*, 68 GEO. L.J. 1131, 1131-32 (1980); Mitchell and Banker, *Private Intrusion Response*, 11 HARV. J.L. & TECH. 699, 704; Andy McCue, *IT Crime Still Going Unreported*, IT Week, 23 May 2002. Available at: <http://www.informaticsonline.co.uk/analysis/1132021>. ("What we are seeing is an increase in actual and attempted crimes using technology and particularly the Internet. The number of security breaches reported is only the tip of the iceberg. For every one admitted there might be 100 held within companies.")

<sup>47</sup> Jelena Mirkovic et al., INTERNET DENIAL OF SERVICE ATTACK AND DEFENSIVE MECHANISMS (2005), at 14.

<sup>48</sup> See Stevan D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 HARV. J.L. & TECH. 699, 704 n. 10, 708 n. 16 (1998) (One in ten security violations is detected. Of those, estimates of the proportion reported vary between 0.7% and 17%.); J. Grable, *Treating Smallpox with Leeches: Criminal Culpability of Virus Writers and Better Ways to Beat Them at Their Own Game*. Computers & The Law Project. University of Buffalo School of Law ["Both the federal and New York state criminal statutes aimed at virus terror are ineffective because ... [t]he combination of the lack of reporting plus the inherent difficulties in apprehending virus creators leads to the present situation: unseen and unpunished virus originators doing their damages unencumbered and unafraid."] See, also, Sarah Gordon, *Virus Writers: The End of Innocence*. ("[G]iven the small number of virus writers who have been arrested and tried ... this lack of arrests is one of the primary indicators used by some to argue that laws are not a good deterrent.") See, also, Madeline Bennett, *Crime Laws Lack Coherence*, IT Week 20 May 2002.

<sup>49</sup> Andy McCue, *IT Crime Still Going Unreported*, IT Week, 23 May 2002 (Security consulting firm reports that 90 percent of its client companies take no action when attack originates from overseas.)

In the rare cases where cyber criminals are actually identified and apprehended, prosecution may fail because of inadequacy of often untested, newly-enacted statutes.<sup>50</sup> In *United States v LaMacchia*,<sup>51</sup> for instance, an MIT student was prosecuted for distributing copyright-protected software gratis over the Internet. The case was dismissed because of lack of evidence of financial gain by the defendant, an essential element of the criminal wire fraud act under which he was prosecuted. This loophole was eventually eliminated by the No Electronic Theft Act of 1997,<sup>52</sup> but not before rogues had escaped through it.

Recent developments in the common law suggest a judicial awareness of the explosive mix of security vulnerabilities and opportunistic free radical cyber rogues. The role of free radicals and their encouragers has been recognized, for instance, in lawsuits against online copyright infringers as well as venture capitalists who funded free radical infringers.<sup>53</sup> Corporations with lax security practices which resulted in unpatched security vulnerabilities, have been held liable for encouraging cyber criminals to launch attacks on their networks,<sup>54</sup> and a recent class action suit against Microsoft accuses the software giant of releasing information about security vulnerabilities in the Windows

---

<sup>50</sup> See Rustad and Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDIS. L. J. 77, 139 ["The failure of tort law remedies to keep pace with new cyberwrongs is a legal lag, which will persist until the comon law catches up with good sense. The growing impact of information technologies 'is already creating a tremendous cultural lag, making nonsense of existing laws.' ... Courts have yet to develop cybertort remedies for negligent computer security ... "]

<sup>51</sup> 871 F.Supp. 535 (D. Mass. 1994).

<sup>52</sup> Pub. L. 105-147, 2(b), 111 Stat. 2678 (1997), 17 U.S.C. 506(a) (2000).

<sup>53</sup> Initial litigation in online music copyright infringement, for instance, was directed at websites that "encouraged" alleged infringers by matching music uploaders with downloaders. See, e.g., *A&M Records, Inc. v Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001); *MGM Studios, Inc. v Grokster*, 259 F.Supp. 2d 1029 (C.D. Cal. 2003). Subsequent copyright suits targeted venture capital firms that funded the websites, as well as Internet service providers who provided the infrastructure for their services. See, e.g., *RIAA v Verizon Internet Servs.*, 351 F.3d 1229 (D.C. Cir. 2003). In *Metro Goldwyn Meyer Studios, Inc. v. Grokster*, 125 S. Ct. 2764, 2780 (2005), the Supreme Court held unanimously that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."

<sup>54</sup> Inquiry Regarding the Entry of Verizon-Maine Into the InterLATA Telephone Market Pursuant To Section 271 of Telecommunications Act of 1996, Maine Public Utilities Dkt. No. 2000-849 (Apr. 30, 2003) (Order). See, also, *Office of the New York State Attorney general, Attorney General reaches Agreement with Barnes and Noble on Privacy and Security Standard*, April 29, 2004. <http://www.oag.state.ny.us/press/2004/apr/apr29a04.html>. [Security vulnerabilities in corporate website allegedly permitted cyber rogues to gain unauthorized access to confidential information.]

operating system in such a way that the information aids free radical cyber wrongdoers more than legitimate users.<sup>55</sup>

In conclusion, cyber rogues, including DDoS attackers, have the deterrence-teflon properties associated with free radicals. They are often judgment-proof and shielded by the anonymity of cyberspace, are increasingly motivated by crime, and appear unconcerned about the problems caused by their actions. Furthermore, cyber attacks are under-reported, under-prosecuted, and perpetrators appear to be unconcerned and, perversely, often encouraged by the threat of legal liability and tougher laws.

### **3. INTENTIONAL AND INADVERTENT NEGLIGENCE**

A defendant's negligence may be intentional or inadvertent. She may have deliberately chosen not to take a precaution, or, despite original good intentions, inadvertently omitted it. Although the negligent act may be identical in both cases, the two types of conduct will have different legal consequences. Courts are reluctant to extend liability for inadvertent negligence, but courts do extend liability for intentional acts, even where the actual harm was done by an intervening wrongdoer. Courts are, for instance, more likely to impose liability on an original tortfeasor if her encouragement of a free radical were intentional.<sup>56</sup> Courts may extend liability for inadvertent encouragement of free radicals, but only if the foreseeable harm was serious. Courts may also extend liability for a DDoS attack to tortfeasors who intentionally failed to take a corrective precaution, such as owners of the intermediate and target computers whose failure to correct a security vulnerability was an efficient cause of the attack. And courts extend liability to tortfeasors who intentionally exposed a plaintiff to the inadvertent negligence of a third party.

Direct proof of intent is not always feasible. We show in this section that the technology involved in an attack allows an inference of intentional or inadvertent action, and thus whether liability will be extended.

#### **3.1 Durable and Non-durable Security Precautions**

---

<sup>55</sup> Hamilton v Microsoft, Superior Court of California (Los Angeles), Case No. (2003), § F ["[W]hile Microsoft has issued strings of alerts, they cannot be understood by the General Public and the method of delivery of the warning has actually increased the probability of harm from hackers who are educated by the information about the flaws and potential breach in the operating systems as described by Microsoft."]

<sup>56</sup> Mark F. Grady, *The Free Radicals of Tort*, SUPREME COURT ECONOMIC REVIEW, 2004, 189, 216-18.

Results in the law and economics literature have suggested that there should be no negligent behavior under a negligence rule of liability, in the absence of errors about legal standards, when precaution is not random, and when private parties have identical precaution costs. It seems therefore, that the frequent occurrence of negligence in society must be explained in terms of non-uniform precaution costs, errors by courts and private parties about the relevant legal standards, or that precaution has a random or stochastic component.<sup>57</sup> Professor Mark Grady has argued that none of these theories explain the prevalence of negligence entirely satisfactorily. Professor Grady has developed a theory of negligence which postulates a pocket of strict liability within the negligence rule.<sup>58</sup>

"Strict liability" refers to imposition of liability in the absence of fault, in other words, for efficient conduct. Conduct is efficient if it provides societal benefits in excess of its cost.<sup>59</sup> Grady postulates that there are circumstances in which a rational injurer may find a precautionary lapse efficient and thus preferable to perfect compliance with the legal standard of due care. These circumstances are termed a "pocket of strict liability," because courts view what is actually reasonable behavior as negligence. The behavior is reasonable in the view of the injurer, but negligent in the view of the court.

The pocket of strict liability is a creature of technology. It can be explained by observing that security precautions commonly have a durable as well as a non-durable component. A durable precaution has a long service life, once it is installed. Use of a durable precaution must usually be complemented by shorter-lived, non-durable precautions, which have to be repeated more frequently than durable precautions. A kidney dialysis machine, for instance, is a typical durable precaution against kidney failure. A dialysis machine cannot function properly without complementary non-durable precautions, such as regular monitoring of the hemodialytic solution.<sup>60</sup>

The required level of durable precautions and frequency and intensity of non-durable precautions are governed by the Learned Hand formula. Courts require clinics to

---

<sup>57</sup> See, MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887, 889-91, and references cited in note 5.

<sup>58</sup> Mark F. Grady, *Why Are People Negligent? Technology, Nondurable Precautions, and the Medical Malpractice Explosion*, 82 NW. U.L. REV. 293.

<sup>59</sup> See George P. Fletcher, *The Fault of Not Knowing*, THEORETICAL INQUIRIES IN LAW, v. 3, no. 2, Article 1, at 2 ["Faultful conduct is inefficient in the sense that its costs exceed its benefits. Liability for efficient conduct is called strict"].

<sup>60</sup> Mark F. Grady, *Why Are People Negligent? Technology, Nondurable Precautions, and the Medical Malpractice Explosion*, 82 NW. U.L. REV. 293, 299.

invest in dialysis machines up to the point where the benefit of additional investment would be less than the additional cost. The optimal monitoring rate of the hemodialytic solution is determined similarly.

Courts require perfectly consistent compliance with the Learned Hand precautions to avoid a finding of negligence. If, for instance, the courts require a network to be scanned for vulnerabilities twice per day, then even one deviation on any given day would be considered negligent.<sup>61</sup> Actual rates of compliance with the non-durable precaution rate may deviate from the Learned Hand optimal rate, however. Even a diligent IT manager will occasionally inadvertently skip a scan. Such an inadvertent deviation from the required non-durable precaution rate is known as a "compliance error."

The frequent occurrence of compliance errors in the real world can be explained by observing that there are two types of cost associated with perfect compliance, namely the cost of each individual trial, and the cost of remembering to perform each trial consistently over time. The root cause of a compliance error lies in the fact that courts expect perfect compliance, because they appear to take into account only the cost of each individual trial and ignore the cost of consistency.<sup>62</sup>

When courts apply the Hand formula to determine an efficient precaution level and rate, the calculation weighs the costs and benefits of the precaution *each time* it is performed but ignores the cost of consistently performing it *over time*. Suppose, for instance, the cost of scanning a network is \$10, and the expected marginal benefit of each scan is \$11 in risk reduction. Failure to perform even one such scan would be viewed as negligence by the courts. If the required rate is two scans per day, then over, say, 300 days, the courts expect 600 scanning sessions. However, human nature is such that over a 300 day period, an IT security manager will occasionally fail to perform a scan.<sup>63</sup> The

---

<sup>61</sup> In *Kehoe v. Central Park Amusement Co.*, 52 F.2d 916 (3d Cir. 1931) an amusement park employee had to apply a brake to control the speed of the car each time the roller coaster came around. When he failed to do so once, the car left the track. The court held that the compliance error by itself constituted negligence, i.e. the court required perfect compliance and considered anything less as negligence. 52 F.2d 916, at 917 ("If the brake was not applied to check the speed as the car approached ... it was clear negligence itself.") For other cases, see Grady, at 901. In *Mackey v. Allen*, 396 S.W.2d 55 (Ky. 1965) plaintiff opened a "wrong" exterior door of a building and fell into a dark storage basement. The court held the owner of the building liable for failing to lock the door. See, however, *Myers v. Beem*, 712 P.2d 1092 (Colo. Ct. App. 1985), action brought against an attorney for legal malpractice (holding that lawyers are not required to be infallible.)

<sup>62</sup> MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887, 899.

<sup>63</sup> See, e.g., IVARS PETERSON, *FATAL DEFECT* (Times Books, 1995), at 194 ("Even under the best of circumstances, our brains don't function perfectly. We do forget. We can be fooled. We make mistakes. Although complete failures rarely occur, neural systems often suffer local faults.")

courts would nonetheless equate such an efficient lapse to negligence, because they do not consider the cost of consistency, i.e. of *never* forgetting or lapsing inadvertently.

Perfect consistency, namely ensuring that 600 scans will actually be achieved over 300 days, would require additional measures, so-called risk-dumping technologies,<sup>64</sup> such as automated scanning, or perhaps additional human supervision. These measures may improve the operator's compliance rate, but not to zero, as they do not totally replace human intervention. Risk-dumping measures may also not be cost-effective. If, for instance, such a measure would add an additional \$2 to the cost of a scan, the marginal cost of an update (\$12) would now exceed the marginal benefit (\$11.) The marginal improvement in compliance would therefore not be cost-justified.

Most negligence claims will come from someone's failure to use a nondurable precaution. Most reasonably careful physicians will invest in a durable precaution, such as a kidney dialysis machine, if cost-justified, but even reasonably careful physicians will occasionally forget to monitor the hemodialytic solution.<sup>65</sup> The cost of remembering is low in the case of durable precautions. Remembering to replace a dialysis machine every five years is not a significant mental burden. In contrast, paying constant and perfect attention to the hemodialytic solution minute by minute, over the same five years, is a significant burden.

In the case of durable precautions, the courts and the care taker agree on the costs in the Learned Hand calculation. Investing in durable precautions up to the efficient Learned Hand level is profit-maximizing because such investment reduces the provider's liability exposure by more than it costs. Imperfect non-durable compliance, on the other hand, is also efficient due to the high cost of perfect consistency, hence, likewise profit-maximizing. Negligent behavior will therefore be most likely where compliance errors are most likely. The more burdensome the rate of compliance and the more difficult and expensive perfect compliance with the non-durable precaution rates, the greater the likelihood of a compliance error.

Although perfectly consistent compliance over time is humanly impossible, hence never cost-effective, courts are nevertheless quite unforgiving of memory lapses. The

---

<sup>64</sup> Risk-dumping technologies take risks out of the negligence system by reducing the number of negligence claims. See Mark F. Grady, Book Review, *Better Medicine Causes More Lawsuits, and the New Administrative Courts Will Not Solve the Problem*, 86 NW. U. L. REV. 1068.

<sup>65</sup> See Meiring de Villiers, *Virus ex Machina Res Ipsa Loquitur*, 2003 STAN. TECH. L. REV. 1, Section V [Rational software provider will implement Learned Hand optimal level of durable anti-virus precautions, but will likely commit compliance error in non-durable precautions.]

reason is that it is impossible or expensive to determine whether any given deviation from perfect compliance was efficient.<sup>66</sup> Who can judge, for instance, whether a pilot's momentary inattentiveness was an efficient or inefficient lapse?<sup>67</sup> Courts therefore do not acknowledge efficient non-compliance where it is difficult to distinguish between efficient and inefficient non-compliance. Instead of incurring the considerable measurement cost to make this distinction, courts simply equate any and all non-compliance to negligence.<sup>68</sup> Courts tend to be forgiving, however, where the cost of ascertaining the efficiency of non-compliance is low or zero. In cases where the deviation is demonstrably efficient or unavoidable, courts have not imposed liability.<sup>69</sup>

We now turn to an analysis of compliance in information security precautions.

## 3.2 DDoS and COMPLIANCE ERROR

### *Introduction*

A civil action involving a DDoS attack would most likely be pursued under a negligence theory, the most widely used theory of tort liability.<sup>70</sup> Negligence is generally defined as

---

<sup>66</sup> Mark F. Grady, *Why Are People Negligent? Technology, Nondurable Precautions, and the Medical Malpractice Explosion*, 82 NW. U.L. REV. 293, 295 ["Negligence law does not forgive inadvertence, even reasonable amounts of it."]; MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887, 905 ["Uneconomic compliance errors are rarely distinguishable from economic ones."]

<sup>67</sup> The policy rationale behind the courts' insistence on perfect compliance was expressed by Lord Denning in *Froom v. Butcher*, 3 All E.R. 520, 527 (C.A.) (1975): "The case for wearing seat belts is so strong that I do not think the law can admit forgetfulness as an excuse. If it were, everyone would say 'Oh, I forgot.'" See, also, MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887, 906; W. LANDES AND R. POSNER, *THE ECONOMIC STRUCTURE OF TORT LAW*, at 73 (1987).

<sup>68</sup> MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887, 906 ["Because courts face positive measurement costs, they impose liability on all compliance errors, both economic (or inevitable) compliance errors and uneconomic (or reasonably avoidable) ones. This is the strict liability component within the negligence rule."].

<sup>69</sup> See, e.g., *Ballew v. Aiello*, 422 S.W.2d 396 (Mo. Ct. App. 1967) (finding defendant not liable for negligence because he was half asleep at the time he was allegedly negligent.) See, also, MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887, n. 59 ("For faints and other slips, it is possible for courts to judge whether they should have been avoided. Indeed, courts' measurement of unusual slips reintroduces the negligence component back into the negligence rule.")

<sup>70</sup> See, e.g., James A. Henderson, *Why Negligence Law Dominates Tort*, 50 UCLA L. REV. 377 (2003). See, also, Gary T. Schwartz, *The Vitality of Negligence and the Ethics of Strict Liability*, 15 GA. L. REV. 963 (1981); Gary T. Schwartz, *The Beginning and the Possible End of Modern American Tort Law*, 26 GA. L. REV. 601 (1992).

a breach of the duty not to impose an unreasonable risk on society.<sup>71</sup> The concept of "unreasonable risk" is general and includes threats to information security, such as DDoS attacks.<sup>72</sup> A victim of a DDoS attack may therefore bring legal action under a negligence theory against anyone who failed in a duty to reduce or eliminate a risk associated with the attack.<sup>73</sup>

To pursue a successful negligence cause of action, a victim of a DDoS attack has to prove (1) that the defendant had a duty to the plaintiff to take reasonable care to avoid the attack or reduce its risk, (2) that she breached that duty, (3) that the breach was the actual and legal cause of the attack, and (4) that the breach resulted in actual harm.<sup>74</sup>

Generally, a duty exists (i) where someone sells a product; (ii) where someone has committed an affirmative act; (iii) when a special relationship exists; (iv) when a special kind of contract exists that benefits the plaintiff; and (v) where there is an undertaking by the defendant. Duty is also not an impediment to the plaintiff when a defendant has acted maliciously to destroy property.<sup>75</sup> Courts are, for instance, likely to find that software designers have a duty to their customers to deliver a "reasonably safe" product.<sup>76</sup>

Courts have not yet explicitly imposed a duty of care on software vendors to produce secure software,<sup>77</sup> although the judiciary has shown a willingness to recognize

---

<sup>71</sup> PROSSER AND KEETON ON THE LAW OF TORTS (5th ed., West Publ. Co., 1984), § 31. Second Restatement of Torts, § 282 (Describing negligence as conduct "which falls below the standard established by law for the protection of others against unreasonable risk of harm.")

<sup>72</sup> See, e.g., Dan B. Dobbs, *The Law of Torts*, at 258 (The plaintiff can assert that *any* conduct counts as negligence.)

<sup>73</sup> The perpetrators of the attack are the immediate wrongdoers, but courts may extend liability to other tortfeasors who have contributed to the attack. Vendors of vulnerable software, for instance, may be sued for encouraging and facilitating DDoS attacks, and owners of vulnerable zombie and target computers may be held liable for failing to take corrective precautions that could have prevented the attack.

<sup>74</sup> See, e.g., *McCall v. Wilder*, 913 S.W.3d 150 (Tenn. 1995) (discussing elements of a negligence claim.)

<sup>75</sup> Mark F. Grady and A. Farnsworth, *TORTS: CASES AND QUESTIONS* (2004).

<sup>76</sup> See, e.g., *Diversified Graphics v Groves*, 868 F.2d 293, 297 (8th Cir 1989) [Holding computer professionals to an elevated duty of care because of their specialist expertise.] See, also, *Hospital Computer Sys. v Staten Island Hosp.*, 788 F.Supp. 1351, 1361 (D. N.J. 1992) (Stating that computer specialists can be held liable for ordinary, although not professional negligence.)

<sup>77</sup> See Jonathan B. Mintz, *Strict Liability for Commercial Intellect*, 41 CATH. U. L. REV. 617, 649 (1992); Stephen E. Henderson and 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, 15 (2002).

such a duty.<sup>78</sup> Authors, such as Professors Michael Rustad and Thomas Koenig have argued that "the epidemic of software vulnerabilities constitutes a compelling reason to recognize a new duty of reasonable Internet security."<sup>79</sup> Rustad and Koenig explain that the recognition of new tort duties by the judiciary is driven by policy considerations. The courts would consider factors such as the foreseeability of harm from security breaches, the existence of a systematic causal relationship between security vulnerabilities and harm from cyber attacks, and deterrence-related policies. Rustad and Koenig's conclusion is couched in terms of optimality, namely that "the judiciary should be open to crafting creative new duties of care for the information age when the magnitude of risk caused by bad software outweighs the burden of precaution."<sup>80</sup>

Courts have occasionally used a finding of "no duty" to limit the expansion of certain cybertorts.<sup>81</sup> In *Lunney v Prodigy Services Co.*,<sup>82</sup> the court held that the defendant, an Internet Service Provider (ISP) was not negligent for allowing an imposter to send threatening e-mail messages on a Prodigy account. The court declined, as a matter of public policy, to impose a duty on ISPs to screen all their e-mail communications, reasoning that the result would be "to open an ISP to liability for the wrongful acts of countless potential tortfeasors committed against countless potential

---

<sup>78</sup> See Michael L. Rustad and Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L. J. 1553, 1568, and cases cited in n. 73-79.

<sup>79</sup> Michael L. Rustad and Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L. J. 1553, 1587.

<sup>80</sup> Rustad and Koenig, at 1886. For a quantitative analysis of optimal anti-virus precaution levels, see Meiring de Villiers, *Computer Viruses and Civil Liability: A Conceptual Framework*, TORT TRIAL & INSURANCE PRACTICE LAW J., Fall 2004 (40:1).

<sup>81</sup> Michael L. Rustad and Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 132, 133 ["The courts' ability to cut off new channels of liability through a 'no duty' determination is the ultimate form of judicial contraception against cybertort expansion. Even if an Internet defendant negligently injures a consumer, there is no liability unless a court is willing to find that duties of care exist for web site activities. .. Substantive types of cybertorts will be stillborn unless a court recognizes a strong public policy basis for establishing an Internet defendant's liability for a particular act."]

<sup>82</sup> 723 N.E.2d. 539 (N.Y. 1999).

victims."<sup>83</sup> The duty doctrine in negligence analysis has been analyzed extensively in the context of information security, including DDoS attacks.<sup>84</sup>

Courts impose on a negligence plaintiff the burden to specify an untaken precaution that would have prevented the accident or reduced its risk. The defendant will be considered to have breached her duty of care if the benefits of risk reduction provided by the pleaded precaution exceeds its cost.<sup>85</sup> The untaken precaution is a central element in negligence analysis. In a successful negligence action, failure to implement the untaken precaution must not only constitute a breach of duty, but must also be the actual as well as proximate cause of the plaintiff's harm.

The role of the untaken precaution in negligence law is well illustrated in *Cooley v. Public Service Co.*<sup>86</sup> In *Cooley*, the plaintiff suffered harm from a loud noise over a telephone wire. She suggested two untaken precautions that would have prevented the harm, namely (i) a strategically positioned wire mesh basket and (ii) insulating the wires. The court ruled that neither untaken precaution constituted a breach of duty. Both precautions would have increased the risk of electrocution to passersby sufficiently to outweigh the benefits in harm reduction.

The risks associated with a vulnerability attack can be substantially reduced and, in some cases, eliminated by identifying and "patching" exploitable vulnerabilities. A patch is a fix for a security vulnerability, usually issued by a vendor after becoming aware of the vulnerability. A "patch and vulnerability management program" is an organizational procedure for monitoring security alerts, implementing patches, and managing their performance in an organization's network. It is a central element of an

---

<sup>83</sup> *Id.*, at 543. See, also, *James v Meow Media*, 90 F.Supp. 2d 798, 819 (W.D. Ky. 2000). [Plaintiffs argued that video game manufacturers owed a duty of care to victims of violence allegedly inspired by certain types of video games. The court found no duty and granted defendant's motion to dismiss. The court stated that imposing such a duty would be detrimental to artistic freedom of speech of media defendants.]

<sup>84</sup> See, e.g., Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U. OTTAWA L.T.J. 231, Section 4.1; Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11 (2002); David L. Gripman, *The Doors Are Locked But the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO L. 167, 179-191.

<sup>85</sup> MARK F. GRADY, UNTAKEN PRECAUTIONS, 18 J. LEGAL STUD. 139, 143 (1989). [The courts "take the plaintiff's allegations of the untaken precautions of the defendant and ask, in light of the precautions that had been taken, whether some particular precaution promised benefits (in accident reduction) greater than its associated costs."]; *Delisi v. St. Luke's Episcopal-Presbyterian Hosp., Inc.*, 701 S.W.2d 170 (Mo. App. 1985) (Plaintiff had to prove physician's breach of duty by specifying the antibiotic he should have been given.)

<sup>86</sup> 90 N.H. 460, 10 A.2d 673 (1940).

organization's information security protocol, and any defect in such a program may be pleaded by a DDoS negligence plaintiff as an untaken precaution that could have mitigated or prevented the attack and resulting damage.

### ***Security vulnerabilities and vulnerability attacks***

Security vulnerabilities are errors in information systems that can be exploited to compromise information in the affected systems.<sup>87</sup> Information can be compromised by theft, rendered useless by corruption, or made unavailable to legitimate users, as in the case of a DDoS attack. Hackers routinely exploit vulnerabilities, for instance, to gain unauthorized access to a Web server, enabling them to steal information from the server, and to use it as a launching pad for further attacks.<sup>88</sup> Tactical exploitation of vulnerabilities in information systems plays an important role in DDoS attacks.<sup>89</sup> In fact, cyber attacks are commonly defined as "attempts to exploit vulnerabilities in hardware or software."<sup>90</sup>

---

<sup>87</sup> Symantec Internet Security Threat Report [Trends for July 05 - December 05], Vol. IX, Published March 2006, at 45 [Defines vulnerabilities as "design or implementation errors in information systems that can result in a compromise of the confidentiality, integrity, and/or availability of information stored upon or transmitted over the affected system."]

<sup>88</sup> See *Theft of Information: A Multilayered Prevention Strategy* ("[A] hacker could use HTTP to execute a buffer overflow attack with the intent of gaining control of a Web server. After seizing control, the hacker could either steal information from that server or use the server as a beachhead to steal information from other servers.") Cisco White Paper. <http://www.cisco.com/en/US/netsol/>.

<sup>89</sup> N. Hanebutte and P.W. Oman, *Software Vulnerability Mitigation as a Proper Subset of Software Maintenance*, Journal of Software Maintenance and Evolution Research and Practice 17, 2005, 379, at 381 ["Cyber attacks take advantage of one or more vulnerabilities and can encompass several coordinated intrusions."]; Ron Brandis, *Common System Security Risks and Vulnerabilities and How Malicious Attackers Exploit Them*. Bridgepoint White Paper (2001), at 1. <http://bridgepoint.com.au>. ["A few software vulnerabilities account for the majority of successful attacks because attackers are opportunistic - taking the easiest and most convenient route. ... They rely on organizations not fixing the problems (applying patches), and they often attack indiscriminately, by scanning the Internet for vulnerable systems."]; K.J. Houle and G.M. Weaver, *Trends in Denial of Service Attack Technology*, CERT Coordination Center White Paper, Carnegie Mellon Univ., 2001, at 9 ["This deployment (of DoS attack tools) depends on the presence of exploitable vulnerabilities on systems and the ability of intruders to exploit those vulnerabilities."]; Symantec Internet Security Threat Report [Trends for July 05 - December 05], Vol. IX, Published March 2006, at 25 ["Attributing the success of an attack to "the high volume of computers running vulnerable software."]

<sup>90</sup> See Symantec Internet Security Threat Report [Trends for July 05 - December 05], Vol. IX, March 2006, at 24.

Sophisticated DDoS attackers frequently use viruses or worms to scan the Internet for vulnerable hosts, to carry attack code, and to launch a DDoS attack.<sup>91</sup> Internet worms such as the W32/CodeRed worm and its successors were deployed to exploit a vulnerability in Microsoft's Internet Information Services (IIS) web servers<sup>92</sup> to achieve a global denial of service effect on the Internet.<sup>93</sup> The type of vulnerability exploited by CodeRed, known as the "buffer overflow", is (currently) the most commonly exploited security vulnerability.

### *The buffer overflow*

Buffers are limited capacity data storage areas in computer memory. Buffers often function as temporary storage for data to be transferred between two devices that are not operating at the same speed. A mechanical printer, for instance, is not capable of printing data at the speed at which it receives it from a computer. A buffer in the interface between the computer and printer resolves this bottleneck. Instead of feeding the printer directly, the computer sends the data to the buffer. The buffer relays the information to the printer, at the printer's speed, and the computer is freed up to continue with other tasks.<sup>94</sup>

A buffer overflow occurs when a program attempts to fill a buffer with more data than it was designed to hold. This is analogous to pouring ten ounces of water into a glass designed to hold eight ounces. The water must obviously overflow somewhere and create a mess. The glass represents a buffer and the water the application or user data.<sup>95</sup> The

---

<sup>91</sup> Jelena Mirkovic et al, INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS (2005), at 66. ["Worms spread extremely fast because of their parallel propagation pattern. ... Frequently, this huge amount of scanning and attack traffic clogs networks and creates a DoS effect. Some worms carry DDoS payloads as well, allowing the attacker who controls the compromised machines to carry out more attacks after the worm has finished spreading."]

<sup>92</sup> The attacks occurred shortly after Microsoft had discovered the vulnerability and issued a patch to fix it. Microsoft, *A Very Real and Present Threat to the Internet*.  
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/codealrt.asp>.

<sup>93</sup> K.J. Houle, Trends in Denial of Service Attack Technology, CERT COORDINATION CENTER (October 2001), 19.

<sup>94</sup> William S. Davis, OPERATING SYSTEMS: A SYSTEMATIC VIEW, at 27, 28.

<sup>95</sup> Mark E. Donaldson, *Inside the Buffer Overflow Attack: Mechanism, Method, & Prevention*, SANS Institute White Paper, at 3.

excess data typically overflow into adjacent memory locations where it can corrupt existing data, possibly changing the instructions and resulting in unintended executions.

The unintended executions may be harmless, but could also be malicious by design. In the most benign scenario, the buffer overflow will cause the program to abort, but without much further harm.<sup>96</sup> In a darker scenario, a buffer overflow could allow a hacker to remotely inject executable malicious code, perhaps DDoS attack code, into the memory of a target computer, and execute it.

Suppose, for instance, the adjacent area ("overflow area") contained an instruction pointer, which defines the instruction to be executed next. By overwriting this pointer, the attacker can influence the program's next execution. The attacker may, for instance, fill the buffer with malicious code and overwrite the pointer with the address of the buffer. The pointer now identifies the malicious content of the buffer as the next instructions to be executed.<sup>97</sup>

In 1989, the so-called Morris Worm, created by Cornell University graduate student, Robert T. Morris, used a buffer overflow vulnerability in a UNIX program to launch a massive DDoS attack on the Internet. It was the first worm of its kind to become a household name, and, by some accounts, brought the destructive potential of the buffer overflow to the attention of the computer community.<sup>98</sup>

Much of the risk associated with security vulnerabilities, such as the buffer overflow, can be mitigated by an effective patch and vulnerability management program, the topic of the next section.

### ***Security patch and vulnerability management***

Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of software, hardware and human vulnerabilities within the IT network

---

<sup>96</sup> The effect of a buffer overflow would be to abort the application program, resulting in a segmentation fault and terminating with a core dump.

<sup>97</sup> See, e.g., Mark E. Donaldson, *Inside the Buffer Overflow Attack: Mechanism, Method, & Prevention*, SANS Institute White Paper, at 3.

<sup>98</sup> Takanen et al., *Running Malicious Code By Buffer Overflows: A Survey of Publicly Available Exploits*, 162. EICAR 2000 Best Paper Proceedings. ("The day when the world finally acknowledged the risk entailed in overflow vulnerabilities and started coordinating a response to them was the day when the Internet Worm was introduced, spread and brought the Internet to its knees.") Available at <http://www.papers.weburb.dk>.

of an organization.<sup>99</sup> An effective patch and vulnerability management program encompasses more than simply identifying a vulnerability and applying a fix.<sup>100</sup> It is an organizational and managerial process that consists of several critical elements, including the following:<sup>101</sup>

1. A sound patch management program needs support at the executive level, including recognition of the problem, as well as mobilization of the necessary personnel and financial resources.
2. A current inventory of hardware and software should be created and maintained to keep track of potentially vulnerable components. When security updates are reviewed, the patch management team needs to rapidly identify the affected systems.
3. The patch management group should constantly monitor the latest security updates, including new vulnerabilities and available patches, and how they may impact the computing environment. This requires ongoing relationships with key vendors, and monitoring of public Web sites and alert lists, such as Bugtraq and SecurityFocus.<sup>102</sup>
4. Continuous scanning and monitoring of the network is necessary to identify new vulnerabilities.
5. Pre-deployment testing of a new patch is essential. Patches are sometimes defective or incompatible with an organization's network. It is therefore prudent to test a newly issued

---

<sup>99</sup> B. Brykczynski and R.A. Small, *Reducing Internet-Based Intrusions: Effective Security Patch Management*, IEEE SOFTWARE Jan/Feb 2003, 50; S. Whitaker et al., *Solaris™ Patch Management Recommended Strategy*, Sun Blueprints™ Online, February 2005. <http://www.sun.com/blueprints>; Peter Mell et al., *Creating a Patch and Vulnerability Management Program*, NIST Special Publication 800-40 v 2.0, at VI. [Stating that the expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an exploitation has occurred.]

<sup>100</sup> See Matt Bishop, INTRODUCTION TO COMPUTER SECURITY (2005), at 389 ["Vulnerabilities arise from computer system design, implementation, maintenance, and operation. A computer system is more than hardware and software. It includes the policies, procedures, and organization under which the hardware and software is used. Security breaches can arise from any one or a combination of these areas. The study of vulnerabilities should therefore not be restricted to hardware and software problems."]

<sup>101</sup> See T. Gerace and H. Cavusoglu, *The Critical Elements of Patch Management*, SIGUCCS'05, November 6-9, 2005, Monterey, California; *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*. Testimony of Robert F. Dacey Before Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform. GOA-03-1138T; Peter Mell et al., *Creating a Patch and Vulnerability Management Program*, National Institute of Standards and Technology Special Publication 800-40 Version 2.0 (November 2005).

<sup>102</sup> BugTraq disseminates information and research on vulnerabilities to direct subscribers, and is hosted by SecurityFocus. <http://www.securityfocus.com>.

patch in a controlled environment before actual implementation. The test results may prompt the security manager not to implement the patch, or to delay implementation until more is known about the patch and the vulnerability.

6. Patch installation and deployment.

7. Post-deployment scanning and monitoring. The operation of a newly installed patch should be monitored to ensure its compatibility with the network, and to audit the ongoing performance of the patch management program.

9. A patch management program must have contingency and recovery plans, in case the patch does not work as expected.

A patch and vulnerability management program clearly consists of durable and complementary non-durable components. Durable components, such as a current inventory of hardware and software vulnerabilities, must be complemented by non-durable precautions, such as continuous monitoring of the network to identify new vulnerabilities.

We now turn to an analysis of compliance error in patch and vulnerability management.

### ***Patch and vulnerability management & compliance error***

We argue in this section that the technological and managerial configuration in patch and vulnerability management makes a compliance error likely. The high stakes inherent in cyber attacks, the low cost and high productivity of many non-durable precautions, and positive synergies between durable and non-durable precautions mandate significant investment in durable precautions, complemented by high levels and intense rates of non-durable precautions. Furthermore, compliance is difficult because many non-durable precautions are memory-driven and the technological environment volatile. These factors make a compliance error likely.

### ***High level of harm and volatile technological environment***

High danger levels threatened by information security breaches demand high Learned Hand precaution levels and rates. Breaches such as theft of confidential information and DDoS attacks on firms that depend on the Internet for their core business have a substantial economic impact on the victim. Other types of attacks cause less damage.

High profile security breaches, such as Web site defacements,<sup>103</sup> for instance, tend to capture headlines, but do not always have a significant long-term economic impact. Denial of service attacks on companies that do not depend on the Internet for their core business, likewise, tend to generate significant publicity, but have a relatively small impact.<sup>104</sup>

Published estimates of the economic impact of DDoS attacks are often based on survey results. However, surveys are subjective and tend to be biased, especially concerning indirect losses, which respondents tend to underestimate or overlook.<sup>105</sup> Direct losses include theft of digital assets such as information and computational resources; productivity losses; and the cost of reinstalling software and reconfiguring computer systems. Indirect losses include reputational harm and costs associated with legal liability.<sup>106</sup>

Total loss suffered by the target of a DDoS attack would likely be captured more accurately by measuring the decline in market value of a target's stock following announcement of a DDoS attack, provided the target is a publicly traded company in an efficient market.<sup>107</sup> The value of a company's stock depends on its free cash flow to equity, which in turn depends on earnings and revenue.<sup>108</sup> DDoS-related losses, including indirect losses such as reputational loss, affect earnings and revenue, and thus also the

---

<sup>103</sup> Web defacement occurs when an intruder maliciously alters a Web page by modifying data on the page. Defacement can mislead visitors to the site and discredit the owner of the site. The defacement victim may lose revenue if its customers perceive it to be insecure, especially in the case of financial institutions where trust and perceptions of integrity are especially important.

<sup>104</sup> Symantec Internet Security Threat Report [Trends for July 05 - December 05], Vol. IX, Published March 2006, at 12, 40 ["(DDoS attacks) are a major threat to organizations, especially those that rely on the Internet for communication and to generate revenue."] Academic studies have reached similar conclusions. See A. Garg et al., *Quantifying the Financial Impact of IT Security Breaches*, INFORMATION MANAGEMENT AND COMPUTER SECURITY 11/2 [2003], 74.

<sup>105</sup> Computer Security Institute, 2005 CSI/FBI Computer Crime and Security Survey, at 14, 15; A. Garg et al., *Quantifying the Financial Impact of IT Security Breaches*, INFORMATION MANAGEMENT AND COMPUTER SECURITY 11/2 [2003], 74 ["It has been difficult to quantify losses due to security breaches, because such losses include not only tangible costs, such as loss of revenues and damage to systems, but also intangible costs, such as loss of reputation and intellectual property."]

<sup>106</sup> See Bruce Schneier, Risk, Complexity and Network Security. Available at <http://www.counterpane.com/presentation1.pdf>.

<sup>107</sup> An efficient market is commonly defined as one that reflects all relevant publicly available information. See Fama, E.F., *Efficient Capital Markets: A Review of Theory and Empirical Work*. J. FINANCE 25, 383 (1970).

<sup>108</sup> See Aswath Damodaran, INVESTMENT VALUATION (2d ed.), Chapters 14, 16.

market value of the firm. These losses, although difficult to estimate directly, can therefore be conveniently measured by changes in the target's market value.

A statistical methodology known as an "event study" is suited to assessing the economic impact of security breaches on a target company.<sup>109</sup> An event study measures the effect of an "event", such as the announcement of a cyber attack, on a related variable, such as the stock price of the target firm.<sup>110</sup> Measurement of the market impact of an event is complicated by the fact that stock prices move in response to multiple factors in addition to the event of interest. An unexpected increase in interest rates, for instance, perhaps coinciding with the event, will tend to depress stock prices. However, a well-designed event study can isolate the effect of the event of interest from the effects of other factors.<sup>111</sup> An event study is therefore capable of accurately capturing the full economic impact of a security breach on a publicly traded company.

Empirical work based on event studies has estimated the impact of an information security breach on a target company's value. A study commissioned by Ernst & Young, for instance, provided numerical estimates of the economic impact of four types of security breaches, namely Web site defacement; Denial of service attacks; Theft of financial information; and Theft of other customer information.<sup>112</sup> The authors report that theft of sensitive financial information had the greatest impact, namely an average cumulative loss in market value of the firms in their sample of 15 percent, over three days following the incident.<sup>113</sup> The corresponding figures for denial of service and Web site

---

<sup>109</sup> A. Garg et al., *Quantifying the Financial Impact of IT Security Breaches*, INFORMATION MANAGEMENT AND COMPUTER SECURITY 11/2 [2003], 74. See, also, Mark L. Mitchell and Jeffrey M. Netter, *The Role of Financial Economics in Securities Fraud Cases: Applications at the Securities and Exchange Commission*, 49 BUS. LAW. 545, 556 ["Event Study Methodology."]

<sup>110</sup> See, e.g., Bhagat and Romano, *Event Studies and the Law: Part I* (Technique and Corporate Litigation), and *Part II* (*Empirical Studies of Corporate Law*). Yale International Center for Finance (2001).

<sup>111</sup> See, e.g., R. GILSON and B. BLACK, *THE LAW & FINANCE OF CORPORATE ACQUISITIONS*, Chapter 6.

<sup>112</sup> Ashish Garg, *The Cost of Information Security Breaches*, CROSSCURRENTS, Spring 2003, 8. See, also, A. Garg et al., *Quantifying the Financial Impact of IT Security Breaches*, INFORMATION MANAGEMENT AND COMPUTER SECURITY 11/2 [2003], 74; A. Garg et al., *The Real Cost of Being Hacked*, published online in Wiley Interscience, [www.interscience.wiley.com](http://www.interscience.wiley.com).

<sup>113</sup> The market reaction appears to reflect not only the sensitivity of the information compromised, but also the quantity. The market reaction appears to be correlated with the magnitude of the breach, as proxied by the number of credit card numbers stolen. Larger thefts resulted in larger stock price declines. The authors report, for instance, that Western Union (First Data Corporation) had exposed 15,000 customers and experienced a decline of 0.8% over a three day period. Egghead put 3.3 million credit cards at risk and experienced a decline of 36% over three days. This is, of course, consistent with an efficient market.

defacement, are average losses of 3.6% and 1.1%, respectively. The reported figure for DDoS is an average over the firms in the sample, which includes Internet pure plays, such as Amazon, Yahoo!, and eBay, as well as others which are not Internet-dependent. Internet-based companies suffered a greater loss due to denial of service than other companies. The study reported a negligible impact due to theft of non-confidential customer information.<sup>114</sup>

The damages figures reported in studies such as the Ernst & Young paper are significant in dollar terms. According to the study, a denial of service attack on Microsoft on 9 February, 2000, resulted in an abnormal return of -3.1% on the same day. A conservative estimate of the one-day loss in value is \$1.3 billion.<sup>115</sup>

The Learned Hand optimal level of a security precaution is determined by balancing its cost against ex ante expected reduction of risk from all foreseeable threats, not just the actual risk that materialized.<sup>116</sup> A vendor's breach of duty, for instance, will be adjudicated by the same standard, regardless of whether its vulnerability resulted in a relatively harmless Web site defacement or a much more serious compromise of confidential information. The nature of the actual risk that materialized ex post does, for course, play a role in issues such as proximate cause and damages.

Current trends suggest that information security risks are escalating. The Computer Emergency Response Team (CERT) reports the following trends in network attacks:<sup>117</sup>

- Increasing degree of automation and speed of attack tools;
- Increasing sophistication of attack tools;
- Faster discovery of vulnerabilities by attackers;
- Increasing permeability of firewalls;
- Increasingly asymmetric threat;<sup>118</sup>

---

<sup>114</sup> See also K. Campbell et al., *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*. JOURNAL OF COMPUTER SECURITY 11 (2003), 431-448.

<sup>115</sup> Microsoft's 2000 balance sheet reports its book value of equity as \$41.368 billion, on which the \$1.3 billion figure is based. This figure is conservative, because the balance sheet understates the February 2000 market value of Microsoft's equity.

<sup>116</sup> See, e.g., Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U OTTAWA LTJ 231, 240 ["Improvements in software security would not only help to reduce DDoS attacks, but would also reduce the incidence of other cyber-scourges, such as epidemics of malicious code."]

<sup>117</sup> 2003 Network Attack Trends Analysis of Computer Emergency Response Team [http://www.cert.org/archive/pdf/attack\\_trends.pdf](http://www.cert.org/archive/pdf/attack_trends.pdf).

- Increasing frequency of attacks on national information infrastructure.

Other advisories are consistent with the CERT report. The March 2006 Symantec Internet Security Threat Report, for instance, documents an average of 1,402 detected DDoS attacks per day during the second half of 2005, a 51% increase over the first half of the same year.<sup>119</sup> New vulnerabilities and security updates documenting them are, likewise, arriving at a high and increasing frequency. The Symantec report documents the highest ever recorded number of new vulnerabilities, as well as the highest yearly total volume of recorded vulnerabilities since the vulnerability database was established in 1998. Of the disclosed vulnerabilities, 79 percent are classified as "easy to exploit", up from 73 percent in the previous period. Symantec also documents a slight increase in malicious code, such as worms and viruses.<sup>120</sup>

As vulnerabilities multiply, so do patches. New security patches are released on a daily basis and at an increasing rate, creating significant burdens for network administrators, who must monitor not only the appearance of new vulnerabilities, but also new patch issues. Their task is further complicated by the discovery of vulnerabilities for which no ready-to-use patch is available. In such cases, administrators have to improvise, and fix the vulnerability by modifying existing security measures.<sup>121</sup>

As security threats escalate, so do compliance externalities. An increase in the compliance rate of a particular non-durable precaution frequently spawns increases in the required compliance rates of related precautions. Each security alert requires evaluation of its relevance to the organization's network. If the evaluation suggests that the update merits serious consideration, further precautions are triggered, including acquisition of a

---

<sup>118</sup> See, e.g., Cadet First Class Michael L. Kolodzie, *The Asymmetric Threat*, 1 ["Defining an asymmetric threat as "a broad and unpredictable spectrum of military, paramilitary, and information operations ... specifically targeting weaknesses and vulnerabilities within an enemy."]  
<http://www.almc.army.mil/alog/issues/JulAug01/MS628.htm>.

<sup>119</sup> Symantec Internet Security Threat Report [Trends for July 05 - December 05], Vol. IX, Published March 2006, at 4, 11-12, 40-41.

<sup>120</sup> *Id.*, at 5, 9-12.

<sup>121</sup> See, e.g., Peter Mell and Miles C. Tracy, *Procedures for Handling Security Patches: Recommendations of the National Institute of Standards and Technology*. NIST SPECIAL PUBLICATION 800-40, at iv ["Due to the way software is created, there are literally thousands of flaws in commercial software, with hundreds being discovered each month. Each one is an exposed flaw that allows a hacker or worm to gain control. New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches. Further complicating the matter is that monitoring for new patches is not sufficient since one must monitor also for vulnerabilities. Not all vulnerabilities have related patches; thus, system administrators must not only be aware of vulnerabilities and patches, but also mitigate 'unpatched' vulnerabilities through other methods (e.g., workarounds, firewalls, and router access control lists)."]

suitable patch, predeployment testing of the patch, and, if a decision is made to install the patch, post-deployment scanning and monitoring of the performance of the patch in the organization's computing environment.

### *Synergies*

Positive synergies between durable and non-durable precautions enhance their combined productivity.<sup>122</sup> A durable precaution, such as a vulnerability inventory, is an essential component of a security program, but it cannot be fully effective if it is not updated frequently. A newly installed patch will prevent future attacks, but only as long as it remains compatible with its computing environment, which requires ongoing monitoring of its performance.

The benefits of the synergies are substantial compared to the cost of the precautions. The CodeRed worm, for instance, paralyzed much of the Internet because a widely available vulnerability patch was not implemented. Failure to take a precaution provided free of charge by the vendor rendered many organizations' patch and vulnerability management programs ineffective against a costly invasion.

Courts have recognized the role of synergies in their liability analysis. In *Swiney v Malone Freight Lines*,<sup>123</sup> the plaintiff was injured by a loose wheel that had become detached from an eighteen-wheel truck. The court noted that inspections of tractor-trailer wheels were both easy and effective. Based on the evidence, the court sent the case to the jury on a *res ipsa loquitur* theory.<sup>124</sup> The strongest *res ipsa* cases are those where the likelihood of a compliance error is the highest.<sup>125</sup> The *Swiney* court's decision recognized that the productivity of inspections gave a high required compliance rate, resulting in a high likelihood of compliance error.

---

<sup>122</sup> F. Cohen offers the following analogy to illustrate the importance of non-durable precautions in computer security: "Suppose we want to protect our house from water damage. It doesn't matter how good a roof we buy ... We have to maintain the roof to keep the water out. It's the same with protecting information systems." FREDERICK B. COHEN, *A SHORT COURSE ON COMPUTER VIRUSES* (Wiley, 1994, 2d ed.), at 148.

<sup>123</sup> 545 SW 2d 112 (Tenn Ct App 1976).

<sup>124</sup> The court distinguished other cases with less productive non-durable precautions. One of the distinguished cases was *Smith v. Fisher*, 11 Tenn. App. 273 (1929) [frequent inspection of brake bands and universal joints is invasive and costly, and not nearly as effective as inspection of wheel lugs.]

<sup>125</sup> MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887.

## *Cost of remembering*

Remembering to take a precaution is a significant part of the cost of compliance. The higher this cost the more likely a compliance error will be.<sup>126</sup> In *Druzanich v. Criley*,<sup>127</sup> an automobile driver was fatigued, but not so fatigued that her decision to drive constituted negligence. The driver was involved in an accident, and the injured plaintiff, her passenger, prevailed in a negligence suit. In the view of the court, the driver's sleepiness increased her compliance cost, thus increasing the likelihood of a compliance error. Fatigue increased the cost of remembering to take precautions that could have prevented the accident.

Cost of remembering is generally lower in an environment where events serve as a timely reminder of the need to use precaution. Such precautions are said to be event-driven. Motorists are, for example, reminded to stop at intersections by an "event", namely a red traffic light. Precautions are said to be memory-driven where there are no timely reminders to take precautions. A compliance error is more likely in an environment where non-durable precautions are memory-driven.<sup>128</sup>

Durable precautions are generally event-driven. Decisionmakers are not only constantly reminded, but also have more time to remember to implement durable precautions, because they are implemented less frequently than non-durable precautions. General awareness of information security risks serves as an effective reminder to implement durable precautions, in part due to the publicity generated by the prevalence of viruses and other hazards such as DDoS attacks, identity fraud and Web site defacements. IT managers will not inadvertently "forget" to have a patch and vulnerability management program, but they may occasionally miss an update, or overlook an e-mail alert. Failure to implement a durable precaution is therefore likely the result of intentional, rather than inadvertent, neglect.

Non-durable precautions, on the other hand, are generally memory-driven. Managers must remember each time to monitor the performance of a new patch or consult a security Web site. A manager who relies on a security-related "event", such as

---

<sup>126</sup> MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887, 937.

<sup>127</sup> 122 P.2d 53 (Cal. 1942).

<sup>128</sup> See, MARK F. GRADY, *Res ipsa Loquitur and Compliance Error*, 142 U. PENN. L. REV. 887, 937 ["It seems likely that compliance rates are higher when precaution is event-driven rather than memory-driven."]

an actual DDoS attack, to remind her to take a non-durable precaution will usually act too late.

Some non-durable precautions are both memory and event-driven. The act of patching a vulnerability, for instance, is driven by an event such as a reminder from a security alert, but the act of systematically paying attention to incoming alerts in the first place, is memory-driven. Most non-durable precautions do not come with a timely reminder and attentiveness plays a much more significant role in non-durable than durable precautions. This contributes to a high compliance error rate.

In summary, high required levels and intense rates of memory-driven, productive non-durable precautions in a patch and vulnerability management program, combined with a volatile technological environment, make compliance burdensome and a compliance error likely.

#### **4. LIABILITY ANALYSIS**

This section analyzes doctrines governing the allocation of liability among participants in a typical DDoS attack. The immediate perpetrators of an attack are obvious defendants in a civil suit, but other players may also face liability. A software vendor may be held liable for providing an opportunity to attackers in the form of vulnerabilities in the software of the zombie and target computers which were exploited by the attackers. The owners of the vulnerable computers may be held liable for failure to correct the defect in their software. The vendor may also be held liable for exposing third parties to the inadvertently negligent failure of the owners of vulnerable computers to fix the vulnerability.

##### **4.1 Vulnerability as Encouragement**

A typical DDoS attack exploits one or more security vulnerabilities. An exploitable vulnerability may be perceived as encouragement in the form of a scarce opportunity to attackers. Several players may be viewed as encouragers, including the vendor originally responsible for the vulnerability, as well as others, such as the users of the zombie computer and the target organization who failed to patch the vulnerability. The Encourage Free Radicals (EFR) doctrine governs the liability of an original tortfeasor

who encouraged an immediate wrongdoer, provided the latter is a free radical and certain additional conditions are met.<sup>129</sup>

The encouragement may have been intentional or inadvertent. Suppose, for instance, a DDoS target had failed to identify and patch the exploited vulnerability. The lapse may have been clearly intentional, such as failure to apply a patch after explicit notification of the vulnerability and obtaining the appropriate patch from the vendor. Intent may also be inferred if the attack succeeded because of a failed durable precaution, such as failure to have a patch and vulnerability management program. A failed non-durable precaution, on the other hand, such as a lapse in monitoring a security update, was likely due to an inadvertent compliance error.

The distinction between intentional and inadvertent wrongdoing is important in the doctrines that govern extension of liability from the immediate wrongdoer to other tortfeasors. Courts are, for instance, more likely to impose liability for encouraging free radicals if the encouragement was intentional.<sup>130</sup> In a case of unintentional or inadvertent encouragement, courts generally impose liability only for serious harm. Someone who has left explosives around children,<sup>131</sup> for instance, is more likely to face liability than someone who has left a pile of dirt clods;<sup>132</sup> and someone who fails to supervise juvenile delinquents<sup>133</sup> is more likely to face liability than a school teacher who leaves ordinary school children momentarily to their own devices.<sup>134</sup>

---

<sup>129</sup> Courts are more likely to impose liability for encouraging free radicals when the following conditions are met: The defendant's encouragement of the free radical was substantial; The defendant created a scarce opportunity for the free radical; The free radical's behaviour was foreseeable; The free radical harmed a third party, as opposed to himself; The foreseeable harm was serious; The fact that the defendant's encouraging behaviour was deliberate, as opposed to inadvertent, was considered important in some cases; The defendant had a special relationship with the free radical, the victim, or both. See Mark F. Grady, *The Free Radicals of Tort*, SUPREME COURT ECONOMIC REVIEW, 2004, 189, 207.

For an analysis of the EFR factors and their application to security vulnerabilities, see Meiring de Villiers, *Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare*, 4 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY (2005), 13.

<sup>130</sup> Mark F. Grady, *The Free Radicals of Tort*, SUPREME COURT ECONOMIC REVIEW, 2004, 189 ["(C)ourts do not normally like to extend the liability of people who may have made an innocent mistake."]

<sup>131</sup> *Travell v Bannerman*, 75 N.Y.S. 866 (App. Div. 1902).

<sup>132</sup> *Donehue v Duvall*, 243 N.E.2d 222 (Ill. 1969).

<sup>133</sup> *Home Office v Dorset Yacht Co.*, [1970] 2 A.C. 1004 (appeal taken from Eng.)

<sup>134</sup> *Segerman v Jones*, 259 A.2d 794 (Md. 1970).

In *Mills v Central of Georgia Ry.*,<sup>135</sup> the defendant had left a signal torpedo on its tracks. A signal torpedo is an explosive device which would blow up upon impact, such as when hit by an oncoming train. Its purpose was to warn crews working on railroad tracks of an approaching train. If a torpedo had not been detonated, it was supposed to be picked up and put away. Contrary to this precaution, however, the torpedo in question was inadvertently left on the tracks. The plaintiff's sons found the torpedo, played with it and injured themselves when it exploded. The Georgia Supreme Court ultimately found for the plaintiff. Although the defendant created the opportunity inadvertently, the harm threatened was sufficiently serious and probable to justify imposing liability.<sup>136</sup>

We have determined that the economic impact of an attack depends on the type of attack and the nature of the target. Denial of service attacks on companies that depend on the Internet for their core business and attacks that result in theft of confidential information tend to have a more serious impact on the target's long-term economic performance than, for instance, Web site defacements and DDoS attacks on firms without a significant Internet dependence.<sup>137</sup> A vendor whose inadvertent oversight resulted in a Web site defacement may therefore escape liability. If the attack resulted in the compromise of valuable financial information by free radicals, even an inadvertently negligent vendor may be held liable under the EFR doctrine.

## **4.2 Exposing plaintiff to third party's negligence**

The Dependent Compliance Error (DCE) doctrine of proximate cause applies where a defendant has exposed the plaintiff to the inadvertent negligence of a third party.<sup>138</sup> The DCE doctrine preserves the liability of the original defendant when the inadvertent error results in injury to the plaintiff. The original defendant will then share liability with the last wrongdoer. The following case illustrates the doctrine.

---

<sup>135</sup> 78 S.E. 816 (Ga. 1913).

<sup>136</sup> The *Mills* case is discussed in Mark F. Grady, *The Free Radicals of Tort*, SUPREME COURT ECONOMIC REVIEW (2004), 189, 217.

<sup>137</sup> *Supra*, fn. 110-115 and associated text [Discussion of empirical evidence of economic impact of various types of cyber attacks.]

<sup>138</sup> Mark F. Grady, *Proximate Cause Decoded*, 50 UCLA L. REV. 293, 312 (2002)

In *Hairston v Alexander Tank and Equipment Co.*,<sup>139</sup> a technician negligently failed to fasten the wheels of plaintiff's car properly. A wheel came off, leaving the plaintiff stranded on a busy highway. The stranded plaintiff was subsequently struck by a passing driver whose attention had momentarily lapsed. The court preserved the liability of the original tortfeasor, the auto technician, because he had foreseeably put the plaintiff in a situation where the plaintiff was exposed to a high likelihood of harm due to the compliance error of a third party, such as an inattentive driver.<sup>140</sup>

The distinction between inadvertent and intentional negligence plays a key role in the DCE doctrine. The third party's negligence must have been inadvertent. Furthermore, courts are more likely to hold an intentionally negligent original tortfeasor liable under the DCE doctrine. However, an original tortfeasor's inadvertent negligence could nevertheless yield liability if it created a significant likelihood of serious harm from a third party's compliance error.<sup>141</sup>

This distinction can be illustrated by revisiting our hypothetical vendor whose negligent quality control has introduced a vulnerability into its software product. A brokerage firm purchases and installs the defective product. The brokerage neglects to patch the vulnerability. Due to a subsequent DDoS attack an investor's time-sensitive transaction could not be executed. The strongest case for imposing liability on the vendor under the DCE doctrine would be where the vendor was intentionally negligent, the brokerage inadvertently negligent, the vendor's negligence substantially increased the likelihood of the investor's harm, and the harm was serious. If, however, the brokerage were intentionally negligent, the vendor's liability would be cut off.<sup>142</sup> This would be the case if, for instance, the brokerage's failure involved a durable precaution, such as having no patch and vulnerability management program in place at all.

---

<sup>139</sup> 311 S.E.2d 559 (N.C. 1984).

<sup>140</sup> See, also, *Ferrogiarro v Bowline*, 315 P.2d 446 (Cal. Dist. Ct. App. 1957) [Defendant negligently ran power pole over, cutting off electricity to a nearby traffic light. A driver negligently failed to notice that the light was not working causing a collision in which plaintiff's deceased died. Court held defendant liable for exposing the victim to the driver's inadvertent negligence.]

<sup>141</sup> Mark F. Grady, *Proximate Cause Decoded*, 50 UCLA L. REV. 293, 313 (2002) ["In the clearest DCE cases, the original wrongdoer's negligence is more deliberate or reckless than the relatively inadvertent negligence of the *Hairston* car dealer. Nevertheless, *Hairston* shows that even inadvertent negligence by an original wrongdoer can yield liability when it significantly increases the probability ... (of) someone else's compliance error."]

<sup>142</sup> Provided the organization cannot be characterized as a free radical. See n 43, *supra*, and accompanying text.

Although courts are more likely to hold an intentionally negligent original tortfeasor liable under the DCE doctrine, an inadvertently negligent vendor may still be held liable if its wrongdoing substantially increased the likelihood of the plaintiff's harm. We argue, in the remainder of the section, that an exploitable security vulnerability substantially increases the likelihood of a security breach, such as a DDoS attack. In particular, (i) There is a substantial likelihood that a vulnerability will remain unpatched due to a compliance error in the patch and vulnerability management program of the user of the vulnerable software; and (ii) An attacker will likely locate and exploit the unpatched vulnerability. We have argued that a compliance error is likely in a typical patch and vulnerability management program. We now turn to the second argument, (ii).

DDoS attacks, especially vulnerability attacks, prey on exploitable security vulnerabilities.<sup>143</sup> In fact, a large percentage of cyber attacks, including the infamous CodeRed worm, have exploited vulnerabilities for which a patch had been available at the time of the attack.

New vulnerabilities are likely to be discovered rapidly and promptly exploited. Worms and viruses employed in sophisticated DDoS attacks are programmed to automatically search for and locate exploitable vulnerabilities. Furthermore, software tools are available to assist software designers in identifying security vulnerabilities in their products.<sup>144</sup> Although such tools are intended to assist designers of "legitimate" software in troubleshooting and debugging, the technology is, of course, equally available to wrongdoers.<sup>145</sup>

Once a valuable (from the viewpoint of the attacker) vulnerability is identified, it will likely be exploited. In his recent treatise on buffer overflow attacks, James Foster comments, "[i]t's no coincidence that once a good exploit is identified, a worm is created.

---

<sup>143</sup> See K.J. Houle and G.M. Weaver, *Trends in Denial of Service Attack Technology*, CERT Coordination Center White Paper, Carnegie Mellon Univ., 2001, at 9 ["This deployment (of DoS attack tools) depends on the presence of exploitable vulnerabilities on systems and the ability of intruders to exploit those vulnerabilities."]; James C. Foster et al., *BUFFER OVERFLOW ATTACKS* (2005), at 142 ["Microsoft's Frontpage Server Extensions (MSFE) have been identified with numerous severe denial of service vulnerabilities."]

<sup>144</sup> See, e.g., James C. Foster et al., *BUFFER OVERFLOW ATTACKS* (2005), at 424 [Describing the CodeAssure Vulnerability Knowledgebase troubleshooting system, which is capable of reliably identifying flaws such as buffer and integer overflows in software.] See, also, Joel McNamara, *SECRETS OF COMPUTER ESPIONAGE: TACTICS AND COUNTERMEASURES* (2003), at 235 [Discussing commercial, sometimes free, scanners, that can be used to probe a system for vulnerabilities.]

<sup>145</sup> Symantec Internet Security Threat Report [Trends for July 05 - December 05], Vol. IX, Published March 2006, at 47 ["(R)ecent advances in technologies that analyze software code have made the discovery of vulnerabilities and the creation of associated exploit code easier than ever before."]

Given today's security community, there's a high likelihood that an Internet worm will start proliferating immediately. Microsoft's LSASS vulnerability turned into one of the Internet's most deadly, costly and quickly proliferating network-based automated threats in history. Multiple variants were created and released within days."<sup>146</sup> In fact, current attack trends and patterns suggest that the time lag between discovery and exploitation of vulnerabilities is shrinking.<sup>147</sup>

Certain vulnerabilities have features that compel their prompt exploitation. These features include ease of exploitation and a technical configuration that gives DDoS perpetrators exactly what they need.<sup>148</sup> A properly exploited buffer overflow, for instance, can act as a gateway to inject and execute attack code, and assume unauthenticated<sup>149</sup> remote control of a system or network, including root control.<sup>150</sup>

A vulnerability is considered easy to exploit if no special programming skills are necessary to take advantage of it, or if the necessary exploit code is publicly available

---

<sup>146</sup> James C. Foster et al., *BUFFER OVERFLOW ATTACKS* (2005), at 8.

<sup>147</sup> See, e.g., Chen & Robert, *The Evolution of Viruses and Worms*, at 13 ["Blaster suggests a trend that the time between discovery of a vulnerability and the appearance of a worm to exploit it is shrinking (to one month in the case of Blaster.)"] See, also, *Universal City Studios, Inc. v Corley*, 273 F.3d 429, 451-52 (2d Cir 2001) (quoting), aff'g, *Universal City Studios, Inc v Reimerdes*, 111 F.Supp. 2d 294, 331 (SDNY 2000).

<sup>148</sup> See Crispin Cowan et al., *Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade*, Working Paper, Dept. of Computer Science and Engineering, Oregon Graduate Institute of Science & Technology., at 1 ("Buffer overflow vulnerabilities particularly dominate in the class of remote penetration attacks because a buffer overflow vulnerability presents the attacker with exactly what they need: The ability to inject and execute attack code. The injected code runs with the privileges of the vulnerable program, and allows the attacker to bootstrap whatever other functionality is needed to control ("own") the host computer.")

<sup>149</sup> The term "authentication" refers to the procedures by which a computer system verifies the identity of a party from whom it has received a communication. The login procedure is probably the best-known example of an authentication procedure. A login prompt asks the user to identify herself, followed by a request for a password. The system then authenticates the stated identity of the user by validating the password, if the password and identity match. If they do not match, the user is restricted from accessing the system. Other examples of authentication include the requirement of confirmation e-mail to activate an on-line account, ATM access, cryptographic authentication of a digitally signed contract, and biometric identification in applications such as Internet banking.

Authentication provides a line of defense against unauthorized access to a restricted system. A vulnerability that allows unauthenticated access may allow an attacker to bypass this line of defense. Network vulnerabilities, including buffer overflows, allow unauthenticated remote access to attackers without authentication. See Meiring de Villiers, *Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare*, 4 *NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY* (2005), 13, § 4.3 E.

<sup>150</sup> "Root" is the conventional name of the superuser who has all rights in all modes on the computer system. This is usually the system administrator's account.

and ready to use.<sup>151</sup> Writing a successful vulnerability exploit from scratch takes considerable programming skill, but exploit code is often publicly available and accessible, even to individuals without technical sophistication. As new vulnerabilities are discovered, exploits are habitually published shortly after discovery.<sup>152</sup> Technical articles continuously appear, describing vulnerabilities and how to exploit them, often in considerable detail.<sup>153</sup> A vulnerability in the Solaris KCMS Library Service System, for instance, was easy to exploit. Exploitation could be accomplished by drawing on a standard and widely available software tool and basic computer literacy.<sup>154</sup> There is a slight trend towards greater ease of exploitation. The 2005 Symantec Internet Security Threat Report<sup>155</sup> documents 40 percent more security vulnerabilities in 2005 than 2004, of which 79 percent were classified as "easy to exploit", up from 73 percent.

The pervasiveness of exploits and the IT community's awareness of the vulnerabilities and the risks they pose, are empirical evidence of the foreseeability of exploitation of common security vulnerabilities.<sup>156</sup> Critical vulnerabilities are widely reported and their exploitation is escalating.<sup>157</sup> The buffer overflow, for instance, is

---

<sup>151</sup> *Symantec Internet Security Threat Report*, Volume III, February 2003, at 47.

<sup>152</sup> For a review of publicly available exploits, see Takanen et al., *Running Malicious Code By Buffer Overflows: A Survey of Publicly Available Exploits*. EICAR 2000 Best Paper Proceedings. <http://www.papers.weburb.dk>.

<sup>153</sup> See, e.g., Smith, N.P., *Stack Smashing Vulnerabilities in the UNIX Operating System*. Southern Connecticut State University (1997). Available at <http://destroy.net/machines/security/> (Thorough academic survey, covering history and terminology, various vulnerabilities and related technologies, as well as solutions); Litchfield, D., *Exploiting Windows NT 4 Buffer Overruns* (1999). Available at: <http://www.infowar.co.uk/mnemonix/ntbufferoverruns.htm>.

<sup>154</sup> SUN Advisory: <http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/50104>.

Not all buffer overflow vulnerabilities are easy to exploit. See, e.g., Peter Szor, *THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE* (Symantec Press, 2005), at 402 (Describing the OpenSSL buffer overflow vulnerability as challenging to exploit.); Id, at 547 ("Some vulnerabilities are easily exploited by the attackers, while others take months to develop.")

<sup>155</sup> Symantec Internet Security Threat Report, Trends for July 05 - December 05, Volume IX, Published March 2006, at 5.

<sup>156</sup> See, e.g., Stephen E. Henderson et al., *Frontiers of Law: The Internet and Cyberspace: Suibg the Insecure?: A Duty of Care in Cyberspace*, 32 N.M.L. REV. 11, 23 ["Given the high-profile nature of recent DDoS attacks, it is absolutely foreseeable that some third party can and will use insecure systems to harm other systems."]

<sup>157</sup> See, e.g., James C. Foster et al., *Buffer Overflow Attacks* (2005), at 20 ["Buffer overflow vulnerabilities are the most feared of vulnerabilities from a software vendor's perspective. They commonly lead to internet worms, automated tools to assist in exploitation, and intrusion attempts."] See, also, Peter Szor, *THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE* (Symantec Press, 2005), at 538 ["Every month critical vulnerabilities are reported in a wide variety of operating systems and applications."]

currently, and has been for a decade or so, the most commonly exploited security vulnerability and the most common way for an attacker outside of a target system to gain unauthorized access to the target system.<sup>158</sup> If buffer overflows were eliminated, the incidence of security breaches would be substantially reduced.<sup>159</sup>

The foreseeability and high likelihood of exploitation of new vulnerabilities by cyber attackers have been recognized in the common law. In their suit against the retailer Guess?, alleging negligent failure to patch a security vulnerability, the Federal Trade Commission emphasized this issue.<sup>160</sup> In a similar case, in April 2003, the Maine Public Utilities Commission denied Verizon Maine's request for a waiver of performance standards on its network for the month of January 2003. Verizon had failed to meet certain performance standards on its network because of a successful attack on its network by the SQL Slammer worm. Citing evidence of the foreseeability of the Slammer worm attack, the Commission concluded that the company had failed to take reasonable precautions to fix the vulnerability that allowed the worm to penetrate its network. The complaint also referred to other factors that had made the attack ex ante

---

Similarly, the number of computer worms that exploit system vulnerabilities is growing at an alarming rate."]

<sup>158</sup> Rupert Goodwins, *Playing Silly Buffers: How Bad Programming Lets Viruses In*, ZDNet White Paper (January 2004). ("The buffer overflow is the mechanism of choice for the discerning malware merchant. New hardware and software techniques are reducing the incidence of this perennial problem, but it's unlikely ever to go away completely.")

Available at <http://insight.zdnet.co.uk/internet/security/0.39020457.39119117.00.htm>.

See, also, Crispin Cowan et al., *Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade*, Working Paper, Dept. of Computer Science and Engineering, Oregon Graduate Institute of Science & Technology. (Describing buffer overflows as not the "most common form of security vulnerability" over the last decade, but also the dominant penetration mechanism for anonymous Internet users to gain remote control of a computer or network. ... Because buffer overflow attacks enable anyone to take total control of a host, they represent one of the most serious classes of security threats.")

Available at: <http://www.cse.ogi.edu/DISC/projects/immunix>.

<sup>159</sup> Crispin Cowan et al., *Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade*, Working Paper, Dept. of Computer Science and Engineering, Oregon Graduate Institute of Science & Technology. <http://www.cse.ogi.edu/DISC/projects/immunix>. ("If the buffer overflow vulnerability could be effectively eliminated, a very large portion of the most serious security threats would also be eliminated.")

<sup>160</sup> See FTC complaint, In the Matter of GUESS?, Inc and GUESS.Com, Inc.

<http://www.ftc.gov/os/2003/06/guesscmp.htm>. [Alleging that the subject information security breach was a well-known and foreseeable consequence of the vulnerability that the defendant had failed to fix.] See, also, *Guess settles FTC Security Charges: Third FTC Case Targets False Claims about Information Security*, at <http://www.ftc.gov/opa/2003/06/guess.htm>; Guess? complaint: United States of America, In the Matter of GUESS?, Inc and GUESS.Com, Inc. <http://www.ftc.gov/os/2003/06/guesscmp.htm>.

foreseeable, such as security alerts issued by Microsoft and recommended use of a software patch that would have prevented the attack.<sup>161</sup>

In conclusion, this section has analyzed the liability of a defendant, such as a vendor of vulnerable software, who has exposed a plaintiff to the inadvertent negligence of a third party. The liability of the vendor may be preserved if (i) it acted intentionally, or (ii) the vendor's negligence was inadvertent, but substantially increased the likelihood of significant harm. We have argued that even if condition (i) were not satisfied, condition (ii) would likely be satisfied in a given case involving a vulnerability DDoS attack. An exploitable vulnerability substantially increases the likelihood of an attack, because it may remain unpatched due to a compliance error, and will likely be located and exploited by an attacker.

### **4.3 FAILURE TO CORRECT VULNERABILITY**

The victim of a DDoS attack may have a cause of action against a party who failed in her duty to prevent or mitigate the attack. The No Corrective Precaution (NCP) doctrine of proximate causality<sup>162</sup> governs the duty of a third party to rescue a person from threatened harm. The doctrine applies where a tortfeasor has created a hazardous situation threatening the plaintiff. A responsible person who recognizes the dangerous situation, and who has a duty to the threatened plaintiff to prevent the harm, nevertheless intentionally or recklessly, does nothing. In this case, the original tortfeasor's liability will likely be cut off under the NCP doctrine, and the last wrongdoer held solely liable. The following case illustrates the doctrine.

In *Pittsburg Reduction Co. v. Horton*,<sup>163</sup> the defendant inadvertently left blasting caps where children often played. Children collected some of the caps and took them home. The parents, knowing that the caps may be live, nevertheless failed to confiscate them. The plaintiff, a playmate of the children was subsequently injured when one of the caps went off. The court held that the parents' reckless failure to confiscate the caps cut off the defendant's liability. The parents recognized the dangerous situation and

---

<sup>161</sup> State of Maine Public Utilities Commission, Inquiry Regarding the Entry of Verizon-Maine into the InterLATA (Long Distance) Telephone Market Pursuant to Section 271 of the Telecommunications Act of 1996. Docket No. 2000-849 (October 18, 2000). [Citing opinion by WorldCom, "[T]he Slammer worm attack was not, as Verizon claims, an unforeseeable event that was beyond Verizon's control."]

<sup>162</sup> Mark F. Grady, *Proximate Cause Decoded*, 50 UCLA L. REV. 293, 315 (2002).

<sup>163</sup> 113 S.W. 647 (Ark. 1908).

obviously had a duty to protect their children, yet recklessly failed to take a corrective precaution, a classic NCP case.

The NCP doctrine does not transfer liability to a last wrongdoer who inadvertently failed to take a corrective precaution, as was the case in *Elbert v. City of Saginaw*.<sup>164</sup> In *Elbert*, a toddler escaped his mother's attention and fell into an excavation which had been left open due to the defendant's negligence. The court held the defendant liable, in spite of a claim that the mother had been negligent in supervising her child. The defendant's negligence involved a durable precaution and he had had an extended period of time over which to realize the danger of the excavation and do something about it. His negligence was therefore likely intentional and inefficient. The mother's negligence (if indeed it was negligence) was due to an attention lapse, a failed non-durable precaution, and therefore likely inadvertent.<sup>165</sup> The NCP doctrine would therefore not transfer liability to the mother, even if she were found negligent.

The NCP doctrine may apply where a user of defective software is aware of a vulnerability and the harm it threatens, yet intentionally fails to rectify it, thus exposing a third party to harm from a cyber attack. Consider, for instance, a vendor which sells vulnerable software to a Shipping Port Authority. The vendor has created a hazardous situation, of which the Port Authority is aware, perhaps due to a security alert and news reports of actual attacks exploiting the same vulnerability elsewhere. Suppose the vulnerability remains unpatched due to an oversight in the Authority's security management program, and is exploited by an attacker to launch a DDoS attack. As a result of the attack, shipping pilots in the vicinity of the port are denied access to crucial navigating data, resulting in a collision. The Port Authority, which had a duty of care to the shipping pilots, may be held liable under the NCP doctrine, provided it was aware of the hazard, had a duty to the plaintiff to mitigate the risk, and intentionally or recklessly failed to do so.

On the facts of the hypothetical, the Authority's act of negligence was likely intentional, considering that it had ignored notification of the vulnerability, the risks it posed, and the availability of a patch to fix it. The Authority likely has a duty of care to the pilots, due to a contractual relationship. In this case, the vendor's liability will likely be cut off and the Port Authority held solely liable under the NCP doctrine. If, on the

---

<sup>164</sup> 109 N.W.2d 879 (Mich. 1961).

<sup>165</sup> See Mark F. Grady, *Efficient Negligence*, 87 GEO. L.J. 397, 411 ["The plaintiff's son was an active child and had to be watched constantly. She missed one of these inspections for her son's whereabouts, and that became the second cause of the accident (the excavation being the first.)"]

other hand, the PA's lapse had been inadvertent, the vendor's liability would be preserved and the vendor would likely become a joint tortfeasor with the Port Authority.<sup>166</sup>

## 5. DDoS AND THE ECONOMIC LOSS RULE

A negligence theory of liability would be irrelevant if no damages were recoverable. A doctrine in tort law, the so-called economic loss rule, appears to significantly limit recovery for damages caused by cyber torts such as denial of service. The doctrine denies a defendant's liability for pure economic loss, namely loss not based on physical harm to person or property.<sup>167</sup> Legal scholarship have dealt with the problem of pure economic losses resulting from cyber wrongdoing, including DDoS attacks.<sup>168</sup>

Damages related to cyber attacks may be recoverable, the economic loss rule notwithstanding, (i) where a cyber attack, such as a DDoS attack, has caused physical harm due to the malfunction of a computer system in applications such as medical systems, aviation and nuclear energy;<sup>169</sup> (ii) in the few jurisdictions which have relaxed the rule against recovery for pure economic loss; and (iii) because an increasing number, perhaps a majority, of jurisdictions recognize electronic information as legally protected property.<sup>170</sup>

---

<sup>166</sup> Mark F. Grady, *Proximate Cause Decoded*, 50 UCLA L. REV. 293, 316 (2002) ["The last wrongdoer's merely inadvertent failure to use corrective precaution preserves the original wrongdoer's liability and probably makes the last wrongdoer a joint tortfeasor."]

<sup>167</sup> Robert L. Rabin, *Tort Recovery for Negligently Inflicted Economic Loss: A Reassessment*, 37 STAN. L. REV. 1513. *Robins Dry Dock v. Flint*, 275 U.S. 303 (1927) (Early Supreme Court opinion by Justice Holmes.) See, also, 22 Am Jur 2d, Damages § 20.

<sup>168</sup> Meiring de Villiers, *Virus ex Machina Res Ipsa Loquitur*, 1 STANFORD TECH. L. REV., 2003 (§VI.B, "The economic loss rule"). For a discussion of the economic loss rule in a DDoS context, see, e.g., Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U OTTAWA LTJ 231, Section 4.2 ["The Harm of DDoS Attacks: Pure Economic Loss?"] See, also, David L. Gripman, *Comments: The Doors Are Locked But the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO L. 167, 177 ["Today, many courts recognize the fundamental unfairness of the economic loss rule and, therefore, are allowing recovery in negligence for purely economic losses."]

<sup>169</sup> Courts have imposed product liability for defective software that resulted in physical injury or death. See, e.g., *Roberts v. Rich Foods, Inc.*, 654 A.2d 1365 (N.J. 1995). See, generally, Patrick J. Miyaki, Comment, *Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?*, 8 SANTA CLARA COMPUTER AND HIGH TECH. L. J. 121 (1992).

<sup>170</sup> Meiring de Villiers, *Virus ex Machina Res Ipsa Loquitur*, 1 STANFORD TECH. L. REV., 2003 (§VI.B, "The economic loss rule").

The trend towards recovery for computer-related economic loss has been recognized by United States Congress, as well as State Legislatures. The Computer Fraud and Abuse Act, for instance, allows hacking victims to recover for economic harm.<sup>171</sup> Furthermore, as pointed out by Professor Margaret Jane Radin, recent cases have suggested that transmission of unwanted messages to a computer system constituted physical harm to the system. These cases have imposed tort liability under the doctrine of trespass to chattels for activities such as "spam" (unsolicited commercial electronic mail) that had an effect similar to denial of service, namely slowing down a system or consuming excessive bandwidth.<sup>172</sup> In *America Online, Inc v. IMS*,<sup>173</sup> for instance, the court held "that AOL's loss of good will when customers complained about the slow and balky operation of their service was an element of actionable damages, above and beyond physical damage to the system itself."<sup>174</sup>

Federal and State legislation provides for monetary damages for spam. The Federal CAN-SPAM Act of 2003,<sup>175</sup> signed into law to combat the problem of spam, provides for criminal and civil penalties for unlawful marketing e-mail. The Act includes a provision for damages of up to \$250 per spam e-mail, capped at \$2 million. The cap can be tripled for particularly egregious violations, and the cap does not apply to e-mail using false headers.<sup>176</sup> Several states have enacted their own anti-spam legislation, most of which allow for civil damages.<sup>177</sup>

## 6. DISCUSSION AND CONCLUSION

---

<sup>171</sup> See 18 U.S.C. 1030 (g) (2000). For State legislation permitting recovery for economic loss, see, e.g., Vt. Stat. Ann. tit. 13, 4106 (2001).

<sup>172</sup> Margaret Jane Radin, *Distributed Denial of Service Attacks: Who Pays? (Part 1)*, CYBERSPACE LAWYER, (Dec 2001), n. 14, 15.

<sup>173</sup> 1998 US Dist. LEXIS 20448 (ED Va).

<sup>174</sup> Richard E. Epstein, Centennial Tribute Essay: *Cybertrespass*, 70 U. CHI. L. REV. 73, 81, citing *Id.*, 14, n. 13.

<sup>175</sup> The full title of the act is "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003."

<sup>176</sup> See Elizabeth A. Alongi, Note: *Has the US Canned Spam?*, 46 ARIZ. L. REV., 263, 286-289.

<sup>177</sup> See, e.g., California Business and Professions Code §17538.45.

This article has analyzed tort doctrines that govern the allocation of liability among key players in a distributed denial of service attack. The traditional tort doctrines are well established and based on common law principles and policy considerations. The main contribution of the article is the adaptation of these principles to the novel technological environment in which DDoS attacks take place. The analysis shows that key concepts in negligence law, such as free radicals, foreseeability, compliance error rate, and the distinction between intentional and inadvertent negligence, can only be properly analyzed and understood in the context of the relevant technology.

We have argued that exploitation of a security vulnerability is foreseeable, because cyber attackers have both the incentive as well as the means to find and exploit vulnerabilities, both of which are driven by technology. Vulnerabilities are tempting because their configuration is often convenient to the aims of attackers. Skillful exploitation of the well-known buffer overflow, for instance, allows administrator-level control of a target computer and remote injection of malicious code. Furthermore, sophisticated attack tools exist that can be programmed to automatically search and locate exploitable vulnerabilities.

The liability of a player such as a vendor of defective software, depends on characterization of attackers as free radicals. We have argued that attackers generally exhibit properties that either make them immune to, or unconcerned with tort or criminal liability. These properties are shaped by the technological environment in which they operate. The anonymity of the Internet, and technologies such as anonymous remailers, reliance on stepping stone and handler intermediate computers, and the use of IP spoofing, for instance, not only embolden cyber wrongdoers, but also make it difficult to identify and apprehend them.

Key doctrines, such as Encourage Free Radicals (EFR), Dependent Compliance Error (DCE), and No Corrective Precaution (NCP), make a sharp distinction between intentional and inadvertent negligence. The EFR doctrine is strengthened, for instance, if the encouragement of a free radical was intentional. The DCE doctrine is likewise strengthened if an original tortfeasor intentionally exposed a plaintiff to the inadvertent negligence of a third party. And the NCP doctrine imposes liability for intentional failure to take a corrective precaution by a person who had a duty to take such a precaution.

The intentional/inadvertent distinction is related to the technology involved in a DDoS attack. Information security precautions are characterized by a durable component, such as a patch and vulnerability management program, complemented by a significant amount of non-durable precautions, including post-deployment vulnerability patch scanning and monitoring. High levels and intense rates of durable precautions are

generally necessary due to the high stakes inherent in information security, the volatile technological environment, increasing degree of automation and sophistication of attack tools, and positive synergies between durable and non-durable precautions. Absent direct evidence of a defendant's state of mind, a court may infer that failure to take a durable precaution was likely intentional, and that a non-durable lapse was likely inadvertent. Furthermore, the higher and more intense the levels and rates of non-durable precautions, the more likely a compliance error becomes.

In conclusion, an analysis of liability issues in DDoS attacks, and information security generally, is closely related to the technology involved, including attack technology, security precautions, and the architecture of the Internet. An understanding and detailed analysis of these technologies is therefore essential to effective judicial decisionmaking.