June 2009

Optimal Hackback

Jay P. Kesan
Ruperto Majuca

Follow this and additional works at: https://scholarship.kentlaw.iit.edu/cklawreview
Part of the Computer Law Commons, and the Criminal Law Commons

Recommended Citation
Available at: https://scholarship.kentlaw.iit.edu/cklawreview/vol84/iss3/10

This Article is brought to you for free and open access by Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in Chicago-Kent Law Review by an authorized editor of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact dginsberg@kentlaw.iit.edu.
INTRODUCTION

In real space, various instances of self-help have been recognized by the law, ranging from the use of reasonable force in self-defense\(^1\) or in defense of property in criminal law,\(^2\) recovery of property\(^3\) and summary abatement of nuisance\(^4\) in tort law, to repossession\(^5\) and commercial arbitration\(^6\) in commercial law, to the right of restraint and self-help eviction remedies in landlord-tenant relations\(^7\) and even to such areas as the First


Amendment,\textsuperscript{8} trade secret law\textsuperscript{9} and patent law.\textsuperscript{10} Self-help in cyberspace has, however, been ignored.

There are several approaches that have been suggested to deal with the problem of Internet attacks, ranging from technological solutions,\textsuperscript{11} to legal solutions,\textsuperscript{12} to economic solutions.\textsuperscript{13} One approach in dealing with Internet attacks is self-help—using reasonable force in self-defense against hackers.\textsuperscript{14} This work contends that there is a legitimate case to be made for the ability to defend oneself in the instance of a digital attack through the Internet.\textsuperscript{15}

In the course of this work, we ask a number of questions. Should society permit hackback?\textsuperscript{16} How should the law on self-defense in cyberspace be designed? Which among the tools of combating cybercrimes—law enforcement, court litigation, hacking back the hacker—should be used to most effectively address cybercrimes? What optimal mix of these alternatives should be used to combat cyber-attacks? What role does technology play?


\textsuperscript{11} For a discussion of technology based remedies to cyber attacks, see, for example, Lilian Edwards, \textit{Dawn of the Death of Distributed Denial of Service: How to Kill Zombies}, 24 CARDOZO ARTS & ENT. L.J. 23 (2006).

\textsuperscript{12} For a discussion of legal remedies to cyber attacks, see, for example, Jennifer A. Chandler, \textit{Security in Cyberspace: Combating Distributed Denial of Service Attacks}, 1 U. OTTAWA L. & TECH. J. 231 (2004).

\textsuperscript{13} For a discussion of economics based remedies to cyber attacks, see, for example, Debin Liu, \textit{The Economics of Proof-Of-Work}, 3 I/S: J. L. & POL.'Y FOR INFO. SOC'Y 337 (2007).


\textsuperscript{15} \textit{Id.} at 88.

\textsuperscript{16} For a discussion of hacking back, see, for example, Neal Katyal, \textit{Community Self-Help}, 1 J.L. ECON. & POL.'Y 33 (2005).
I. SELF-DEFENSE

Self-defense springs from the natural instinct for self-preservation, and hackback should not be banned outright—it is generally accepted that one has the right to defend one’s self and one’s property and, towards this end, use reasonable force. Aurelius Augustinus, generally acknowledged as the first to have articulated the “just war” doctrine, points out that war must be exercised by the sovereign and must be waged in order to achieve peace and not for “love of violence, revengeful cruelty, fierce and implacable enmity, wild resistance, and the lust of power, and such like.” Hugo Grotius, generally known as the father of modern international law, articulated that a just war must contain these basic elements: immediate danger to the nation, necessity of the force employed to adequately defend the nation’s interests, and proportionality of the force employed to the threatened danger. Applying these elements to the question of hackback, we begin to see its justifications.

A. The Alleged Problems with Hacking Back

The litany of criticisms of hackback include the possibility of misidentification of the hacker against whom to retaliate, use of automated program by counter-strikers that will escalate out of control, “shoot-outs” between trigger-happy defenders and intruders, and self-proclaimed “white hats” who release worm patches with good intentions, but end up with bad results. However, the fact that the exercise of a limited right to hackback can be abused does not necessarily mean that the right should be denied at the outset; it does, however, mean that the exercise of this privilege should

17. See Simmons, supra note 1.
20. For a discussion of Grotius, see, for example, T.M.C. ASSER INSTITUUT, THE HAGUE, GROTIUS READER (L.E. Van Holk & C.G. Roelofsen eds., 1983).
23. See Katyal, supra note 22, at 62.
be regulated.

B. The Benefits of Hacking Back

The public and the private sector should be more engaged in the battle against cybercrime. The thought that we should empower ourselves and say to hackers, "this is my property, get out," in the same way that we sometimes (and within limits) allow people to defend real property transgressions is both appealing and worrisome. A legitimate concern that this approach raises for some people would be "What is going on here—vigilantism?" We are not supporting an unbridled right to hackback. What we are saying is that there are some limited situations, for example computer intrusions, where litigation is truly not only impractical but also too costly.

One major argument in favor of hackback is that traditional law enforcement schemes simply do not work in cyberspace because of the speed by which attacks cause damage to e-commerce sites and also because hackers can stage attacks from multiple jurisdictions with varying cybercrime laws and procedures for prosecuting internet crimes. If you are a hacker yourself, you are arguably in the best position to effectively identify and retaliate against someone attacking your systems.

As long as the appropriate technology exists, there is a very strong possibility of the victim correctly identifying the hacker or knowing who the hacker is and of taking him out quickly and efficiently through retaliation. Looking at the numbers in terms of damage due to hacking, the numbers are very significant, and to the extent that you can mitigate the damage to your system and, to the extent that it outweighs damage to third


27. For a discussion of technology available to identify a hacker, see, for example, Bruce P. Smith, Hacking Poaching and Counterattacking: Digital Counterstrikes and the Contours of Self-Help, 1 J.L. ECON. & POL'Y 171 (2005).
parties, self-defense is worth seriously thinking about.\textsuperscript{28}

There is a role to be played by the choice of technology, and this clearly is an important role. Obviously we want to create incentives for people to use state-of-the-art hackback technology. There is a distinction between someone who hacked my system to just show me that they can get into the system and the person who is seeking to cause real harm.\textsuperscript{29} Being able to distinguish these two types of intruders and mounting a proportionate response is the key. It is also important to look at the potential liability to third party systems. Again, the reasonableness of the response is extremely important, as is the accuracy of the trace.

II. BUILDING A LIMITED RIGHT TO SELF-DEFENSE IN CYBERSPACE

When does it make sense to legally give someone the right to hackback and when does it not?

A. Predicting Behavior

Let us begin by considering what a firm’s options are during a denial of service attack; what might the firm do? The firm might do nothing, and merely attempt to recover its computer system and prevent further harm. The firm might invest in an improved intrusion detection system and fire walls to prevent future attacks. The firm might even go out and buy cyber insurance.\textsuperscript{30} The firm may decide to litigate and prosecute an intruder by filing a complaint with the U.S. Attorneys’ Office or pursuing a private suit against an attacker. The third option may be to hackback. Let us try to understand these three options in greater detail. We employed formal game theory\textsuperscript{31} to model the strategic interaction between the firm and the hacker. This allowed us to study the behavior of the hacker given the effectiveness of law enforcement and the potential counter-actions of the firm, and the


\textsuperscript{29} For a discussion behind the motives of hackers and the different types of harm they seek to cause, see for example, Michael L. Rudstad, Private Enforcement of Cybercrime on the Electronic Frontier, 11 S. CAL. INTERDISC. L.J. 63 (2001).

\textsuperscript{30} For a discussion of cyber insurance, see, for example, Wendy S. Meyer Insurance Coverage for Potential Liability Arising from Internet Privacy Issues, 28 J. CORP. L. 335, 341–42 (2003).

inverse, and also capture the interaction between law enforcement, court remedies, and self-help remedies. From the Nash equilibria\textsuperscript{32} that flow from the model,\textsuperscript{33} we observe that the firm will find that police enforcement works best in certain instances, while in some cases, resort to the courts based on civil liability litigation will be the better approach, and in still other situations, self-defense and self-help will best address the cybercrimes problem.\textsuperscript{34}

What you begin to see when these equilibria are analyzed is that there is a boundary where hacking back is a sensible option. But simultaneously, there are also important roles to be played by self insurance and litigation. When looking at the various options available, it is not so much that hacking back is a substitute for the various kinds of remedies available in the law; rather, it is an important option that is available when there is an inability for public solutions to provide a welfare-maximizing option.

What exactly is the role of technology? There have been real improvements in the ability to, even in a dynamic internet protocol world, figure out relatively well who is an attacker and who is hiding the attackers.\textsuperscript{35} A world with better intrusion detection systems is a world where you have better technologies to trace back who the attacker is, allowing you to assess the danger and come up with a narrower, better response. If you are able to do that, then you have a higher probability of hitting the hacker and a lower probability of being liable for third party damages.

Essentially, there is a disconnect between private solutions and socially-optimal solutions, and that is basically what you see here. You can structure liability rules to work in a manner so that it guides the private solution to the socially-optimal solution. In other words, what you are really trying to do is create liability rules that ensure a firm uses a hackback only when it is socially optimal to do so.

This type of structure does not entirely eliminate all of the problems. There are still social problems, for example, the problem of third parties poorly building systems for a company and consequently unexpected events happening that have not been remedied. There are additional costs

\begin{itemize}
  \item \textsuperscript{32} For a more complete explanation of the Nash Equilibrium that resulted from the model, see, for example, Kesan, \textit{supra} note 28.
  \item \textsuperscript{33} \textit{Id.}
  \item \textsuperscript{34} Forensic investigation takes time, but a virus or worm spreads quickly, swift action is needed to mitigate the grave damage that security incidents can cause. Epstein has argued that self-help plays a role because judicial remedy is often too slow. \textit{See} Richard A. Epstein \textit{The Theory and Practice of Self-Help}, 1 J. L. Econ. & Pol'y 1, 26 (2005).
\end{itemize}
associated with these types of risk, and hence, some regulation and obviously some legal regimes are needed in addition to the simple liability rule.\textsuperscript{36}

\textbf{B. Socially Optimal Hackback}

When is hackback optimal? Our game-theoretic model details the following criteria for the valid exercise of self-defense in cyberspace: (1) accounting for traceback costs, the damage to the attacked firm’s (that is, the entity that is hacking back) systems that can be potentially mitigated outweighs the potential damage to third parties; (2) hackback does not result in greater harm to innocent parties compared to the damage to the defender’s (i.e., the attacked firm’s) systems that is sought to be mitigated; and (3) there is a relatively high chance of hitting the hacker, instead of innocent third parties, and recourse to police enforcement or civil litigation is either ineffective or impractical. Furthermore, due care should be exercised to avoid or minimize damage to third parties, and the purpose of the hackback should be limited to the prevention of damage to the firm’s information technology infrastructure. The results also underscore the importance of using good technology (that is, intrusion detection systems (IDS), and traceback technology) in order for hackback to be effective as a deterrent against cyber-attacks. These criteria and guidelines articulate the circumstances under which self-defense is proper in cyberspace, and also the situations in which we should instead rely on the criminal justice system or the courts.

Using this game-theoretic model of the interaction between the defender and the hacker, we were able to capture the interplay between legal remedies (police enforcement and court litigation), technology (IDS and traceback), and economic incentives (cost and benefits of self-help remedies), and thus develop specific rules or tests for resolving whether resort to hackback is justified. Based on the results of the model, the criteria for determining whether resorting to hackback is optimal are: (1) low availability of other alternatives, such as criminal enforcement and/or resorting to litigation, or where the use of these alternatives is impractical or ineffective; (2) where a more defensive strategy, such as recovering damages or dropping incoming packets, would not deter the hacker; (3) the likelihood of hitting the hacker instead of innocent third parties is high; and (4) where the damage to the defender’s systems cannot be mitigated to a point that

does not warrant risking potential damage to innocent third parties.

Additionally, when hackback is justified, the two following rules should govern conduct during hackback. First, defenders must not use excessive force, that is, they must only use force necessary to defend their property and not needlessly destroy the hacker’s digital assets. Even if acceptable preconditions are present—and thus the exercise of the privilege is justified—the conduct *during* hackback must also be regulated by the law. Counter-strikers must also use only “proportionate force,” that is, they must not wantonly damage the hackers’ digital systems out of retaliation, but rather, only use force that is necessary to avoid damage to their own systems. In sum, the law needs to layer liability rules on top of the reasonableness conditions.

Second, counter-strikers would be held liable for damage to third parties. Thus, liability rules should be set in place so that firms internalize the damage to third parties, thereby bringing the private incentive to hackback closer to the socially-optimal outcome. In order to internalize the damage to third parties, active defenders should be held liable to third parties caught in the crossfire. Not holding active defenders responsible for the consequences of their action will result in externalities and excessive amount of hackback activity. In sum, the law should layer the third-party liability rules on top of the reasonableness conditions.

These reasonableness conditions are consistent with the economic approach in tort law, which balances the rights of firms seeking to mitigate damages to their systems and of third parties not being forced to suffer economic harm. These added regulations are necessary in order to move the firm’s Nash equilibrium outcome towards the socially-optimal result. For example, making firms liable for third-party damages will cause them to internalize the potential damage to third parties as a result of their decision-making, and ensure that firms behave closer to the socially-optimal outcome. Because counterstrikes can misfire and damage innocent third parties, what passes as self-defense may in reality be another wrong. Therefore, reasonableness standards must be applied and hacking victims should resort to legal remedies rather than counter-attacks in those situations where a reasonable response is not possible.

As it turns out, these conditions resemble the traditional formulation of the “just war” doctrine, which requires the following elements for a valid counterstrike: (1) there is grave damage (greater than the damage that might result from the action) that will be inflicted to the defender unless it

---

counter-strikes, (2) there is a serious prospect of success, and (3) other means for stopping the evil are either impractical or ineffective.38 Interestingly, our requirement that counter strikers should not wantonly damage the hacker’s system and use only necessary force echoes the classical authors’ position that war must not be waged for “revengeful cruelty”39 and that only necessary and proportionate force ought to be used.40

Thus, in our view, the law should in some instances allow self-help remedies, yet at the same time regulate the exercise of the privilege so as to check against its potential abuse.41 Given the potential benefits self-help can generate when used responsibly, regulating the exercise of the privilege is the best way to deal with these potential excesses. In short, active defense is an extraordinary remedy, available only when other alternatives are ineffective or impractical and when there is a serious prospect of success. There must be a relatively high chance of hitting the hacker, instead of hitting innocent persons. Thus, reasonable effort must be exerted to employ state-of-the-art trace back technology. This helps the firm to carefully ascertain the existence or the imminence of the attack or potential danger. Furthermore, it also decreases the error of hitting innocent persons and enhances the deterrent effect of hackback. If a firm hacks back without these conditions being present, it oversteps the bounds for reasonable exercise of self-defense in cyberspace. The law can hold those who exercise self-help illegally liable for penalties.

CONCLUSION

Using a game theoretic model, we have described what we think the law on self-defense in cyberspace should be. There is no apparent reason why the law should outright ban firms from exercising self-defense in cyberspace. Active self-defense can deter criminals preemptively and supplement law enforcement. Also, once precedents of hacking back are known in the hacker community, such attacks may decline. Absent the showing of widespread misuse, self-defense through hackback should not be outlawed.

38. DeForrest, supra note 21.
41. For a discussion of the abuse of self-help, see, for example, Gerchick, supra note 7, at 773–77.