A Legal Defense of Counter-Hacking

Ben Richards

Follow this and additional works at: https://scholarsarchive.byu.edu/byuplr

BYU ScholarsArchive Citation
Available at: https://scholarsarchive.byu.edu/byuplr/vol28/iss1/6

This Article is brought to you for free and open access by the All Journals at BYU ScholarsArchive. It has been accepted for inclusion in Brigham Young University Prelaw Review by an authorized editor of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.
A LEGAL DEFENSE OF COUNTER-HACKING

Benson Richards

The world has been fundamentally transformed by the advent of computing technology over the past fifty years. Technological advances such as computers, the Internet, and e-mail have drastically changed the way people interact with each other. The online experience has made shopping, banking, and even dating easier and more convenient for millions around the world.

As technology becomes more integrated into every aspect of daily life, the consequences of a powerful attack on computing infrastructure grow more severe. In April 2013, the Syrian Electronic Army (SEA) hacked dozens of Western media outlets, including the New York Times, CBS, the BBC, and the Associated Press (AP). In one of these attacks, the SEA took over the AP’s official Twitter account, and tweeted false information regarding a terrorist attack on the White House. U.S. financial markets lost more than one percent of their value before the tweet was repudiated. Unfortunately, Twitter accounts and Facebook pages are not the only potential targets. Hackers that infiltrate air traffic control systems, electrical grids, and water treatment facilities have been portrayed in movies and

1 Benson Richards is a senior at Brigham Young University. He is majoring in finance and minoring in statistics. He plans to attend law school in the fall of 2014 and pursue a career in corporate law. The author would like to give special thanks to Davis Green and Jarom Auna for their many insightful contributions to this paper, as well as their lasting patience and dedication. Without their persistent efforts, this paper would not have been possible.

TV shows for years, but threats of this kind are no longer simply confined to the realm of science fiction.

The information age has fostered a rash of identity thefts and cases of cyber-espionage. The motives of the hackers responsible for these crimes vary widely. Some seek financial gain, while others use cyber-mischief as a tool to further their political agendas. Still others are driven by nothing more than egotistical vindication; they want to prove that the latest and greatest defense systems are no match for their hacking skills. The widespread success of hackers is discouraging. Former Homeland Security Secretary Janet Napolitano recently warned that a cyber-attack equal in scale to the September 11th terrorist attacks could happen “imminently . . . Attacks are coming all the time. They are coming from different sources, they take different forms. But they are increasing in seriousness and sophistication.”

Section I of this paper will examine the rise of the hacking epidemic and its impact on an increasingly digital world.

In response to the escalating threat of major cyber-attacks, dozens of organizations worldwide have attempted to improve their digital security. Most of these institutions have historically focused on improving their defensive capabilities; these include state-of-the-art firewalls, sophisticated encryption algorithms, and other measures designed to keep intruders out. In Section II, current computer-related legislation and the defensive measures organizations may legally use against attackers will be discussed.

However, despite an increasingly intense focus on improving computer security, hackers continue to successfully infiltrate and disrupt thousands of corporate, government and individual networks. A recent report issued by the Commission on the Theft of American Intellectual Property (IP Commission) asserts that “Even the best security systems . . . cannot be relied on for protection against the most highly skilled targeted hackers . . . Effective security concepts against targeted attacks must be based on the reality that a perfect

defense against intrusion is impossible". As a possible response to these threats, computer scientists have begun to explore the power of counter-hacking as part of a firm’s ‘active defense’ against hackers. Counter-hacking involves either the release of malicious code by the victim on the attacker’s machine, and/or the actual infiltration and remote control of the attacker’s computer. Section III of this paper will argue that counter-hacking should be recognized as a legally acceptable weapon against computer criminals.

I. NECESSITY OF COUNTER-HACKING

In his 2005 book The Art of Intrusion, former criminal hacker Kevin D. Mitnick detailed an attempt by the United States government to assess the reality of the threat posed by cyber-terrorists. Government leaders were astonished by what they learned:

In 1997 and again in 2003, the Department of Defense launched Operation Eligible Receiver – an effort to test the vulnerability of this nation to electronic attack. According to an account published in the Washington Times . . . “Senior Pentagon leaders were stunned by military exercise showing how easy it is for hackers to cripple the U.S. Military and civilian computer networks” . . . the National Security Administration assembled a group of its computer specialists as a ‘red team’ of hackers, allowed to use only off-the-shelf computer equipment available to the public, along with any hacking tools . . . they could download from the Internet.

In a few days, the red team hackers infiltrated the computer systems controlling parts of the nation’s electronic power grid and with a series of commands could have turned sec-

---


tions of the country dark. “If the exercise had been real,” the Christian Science Monitor reported, “they could have disrupted the Department of Defense’s communications systems (taking out most of the Pacific command) and gained access to computer systems aboard US Navy vessels.”

Computer scientists typically refer to this kind of an attack as a ‘targeted attack’, distinct from an ‘opportunistic attack’. Opportunistic attackers seek out and exploit vulnerabilities in existing network defenses, but targeted attackers focus on a single organization and launch a series of attacks until one or more of the hacks are successful. Opportunistic hackers can be thought of as thieves who walk through an entire neighborhood, only entering where doors have been left unlocked. On the other hand, targeted attackers would select a single house, and spend days, weeks, or years trying to get inside. Given enough time, the targeted attacker will almost always succeed. The IP Commission Report states:

Companies spend inordinate amounts of money attempting to protect their networks against all threats, but in reality only succeed in keeping out the opportunistic hackers . . . If presented with a challenging network defense, [opportunistic hackers] simply move on to more lightly defended networks. Perhaps more importantly, vulnerability-mitigation measures have proved largely ineffective in defending against targeted hackers . . .

Brilliant young hackers will consistently continue to invent ingenious ways to circumvent the latest firewalls and digital encryptions. Sometimes these targeted attacks will seek to prove a political point; more often, they will attempt to cause significant damage to existing computing infrastructure, or steal data stored on network servers. A survey conducted at the 2013 Information Systems Security Association conference indicated that 79 percent of computer security

6 Id. at 42 (Quoting “Tom Regan, Wars of the Future . . . Today”, Christian Science Monitor, June 24, 1999).

7 Blair et al., supra note 3, at 79.
professionals correctly predicted that hackers would succeed in performing a “major” cyber-attack within one year.\footnote{Sean Gallagher, \textit{Security pros predict “major” cyber-terror attack this year}, \textsc{arstechnica} (Jan. 4, 2013, 8:20 AM), http://arstechnica.com/security/2013/01/security-pros-predict-major-cyberterror-attack-this-year. As will be discussed shortly, these security experts were proven correct in their assessment of the danger posed by hackers when Target and several other major retailers were successfully attacked in November 2013.}

Perhaps the most jarring indication of the need for improved cyber-security is a 2013 report released by Mandiant, an American IT security firm. The report details the hacking exploits of the Chinese People’s Liberation Army’s Unit 61398, designated by Mandiant as “Advanced Persistent Threat 1 (APT1).” Mandiant claims that APT1 operates with the knowledge and approval of the Chinese government. According to Mandiant, APT1 has compromised 141 companies, mostly based in the United States, since 2006.\footnote{MANDIANT, \textit{APT1: Exposing One of China’s Cyber Espionage Units 3} (2013).} If state-sponsored cyber-attacks (such as those perpetrated by APT1) are, in reality, becoming more frequent, the risk of intrusion faced by corporations and government entities that protect intellectual property or personal information is large indeed.\footnote{It should be noted that although attacks on U.S.-based corporations and other entities frequently originate overseas, a detailed discussion of potential international responses to the hacking epidemic is beyond the scope of this paper. We will focus exclusively on the legal justification for U.S.-based organizations to protect themselves from domestically-launched attacks.}

Mandiant showed that APT1 has been very successful at infiltrating U.S.-based corporate networks, and then maintaining access to those networks for an extended period of time. APT1 was able to maintain access to victim networks for an average of 356 days; one company even remained exposed for nearly five years.\footnote{MANDIANT, \textit{ supra} note 8.} The amount of data stolen from compromised corporations is staggering; Mandiant claims that APT1 was responsible for the theft of more than 6.5 terabytes of compressed data (including data on manufacturing
procedures, strategic business plans and product development) from a single corporation over a ten-month period.\textsuperscript{12} The theft of this information results in a significant loss of competitive advantage, and raises the possibility of severely reduced revenue and profits.

Even more disconcerting, however, is the potential for cyber-attacks to undermine consumer confidence and macroeconomic stability. Consumers who no longer trust commercial websites that require credit card information or social security numbers may stop using the Internet as a mode of commerce. The situation becomes even more dangerous if financial institutions that manage credit or debit card transactions are compromised; individuals may lose confidence in the electronic payment system altogether. In the same way that fiat currency has value because of trust in the issuer, electronic transactions are accepted because of trust in the system’s ability to conveniently and reliably turn a card swipe into currency.\textsuperscript{13} Any attack that destroys the credibility of this system would have serious repercussions for both business owners who rely on the system to receive payment and customers who trust that the system will charge only what they owe.

A recent security breach at Target, a major U.S. retailer, demonstrates the power that hackers can wield over the economy as a whole. Hackers were able to infiltrate Target’s point-of-sale system days before the start of the holiday shopping season in 2013. Over the next three weeks, thieves were able to obtain the credit card numbers, debit card PINs, phone numbers and e-mail addresses of nearly

\textsuperscript{12} Id. at 25.

\textsuperscript{13} Fiat currency is a form of payment that has value because a government declares so. A large majority of world currencies are fiat currencies, including the euro and the U.S. dollar. If citizens lose confidence in the government’s continued support of the currency, the entire economic system becomes vulnerable to collapse, as seen in post-WWI Germany and the early days of the American Revolution. Internet transactions, which similarly rely on trust and confidence in the continued viability of the system to maintain value, could be susceptible to the same failures seen by historical fiat currencies if the system’s security was called into question.
110 million individuals.\textsuperscript{14} Although final costs will not be known for years, early estimates indicate that banks and retailers could lose as much as $18 billion as a result of the hack, with consumers liable for another $4 billion in uncovered losses and other costs.\textsuperscript{15} If hackers continue to be successful in launching these kinds of attacks, retailers concerned with potential liability and lost profits may stop accepting electronic forms of payment, insisting on ‘safer’ methods such as cash or checks. Additionally, consumers that refuse to use credit cards and other forms of electronic payment for fear of identity theft or fraud could become more common.

As hackers improve their skills and potential targets become more tempting, relying solely on enhanced defensive security measures such as firewalls and defensive software to protect critical data is both naïve and irresponsible. The IP Commission Report argues that “current law and law-enforcement procedures simply have not kept pace with the technology of hacking and the speed of the Internet. Almost all the advantages are on the side of the hacker; the current situation is not sustainable . . .”\textsuperscript{16} The challenges faced by information technology security teams demand a more flexible and powerful solution to the increasing proliferation of major cyber-attacks. By providing corporate and government-sponsored IT security professionals an explicit legal justification for counter-hacking, the judiciary makes it possible for these professionals to utilize the means necessary to deter and identify would-be cyber-criminals, resulting in greater economic prosperity and security.

\section*{II. Current Laws Concerning Hacking}

The advent of computing technology has brought about a need to legislate thousands of new business transactions and a host of criminal activities that had never been dreamed of prior to the Internet age. One of the first attempts to address the need for new legislation

\textsuperscript{14} Elizabeth A. Harris et al., \textit{A Sneaky Path Into Target Customers’ Wallets}, N.Y. Times, Jan. 18, 2014, at A1.

\textsuperscript{15} \textit{Id.}

\textsuperscript{16} Blair et al., supra note 3, at 81.
in this area was the Computer Fraud and Abuse Act (CFAA), passed in 1986. Although several amendments and addendums have been passed since then, the CFAA is still considered the hallmark piece of legislation on digital security.

The CFAA prohibits individuals from “knowingly access[ing] a computer without authorization”.17 This definition permits the first several steps in an attempted counter-hack. Any computer code installed on a hacking victim’s machine may legally be manipulated by the victim to either halt the attack, or turn against the hacker and allow the victim (now counter-hacker) access to the machine being used to control the attack. Going a step further and actually accessing or controlling a hacker’s computer seems to be in violation of the CFAA; however, there are several previous court cases and well-established legal precedents that appear to justify such action.

The definition of the term “authorization” is nowhere to be found in the CFAA. Although subsequent judicial opinions have provided some clarity, a universally accepted definition of the term has not yet been established. A Justice Department memo on prosecuting computer crimes is equally vague in its instructions on appropriate responses to an attempted hack, saying only that counter-hacking “may be illegal”.18 The Supreme Court’s ruling in McBoyle v. United States indicates, “[I]t is reasonable that a fair warning should be given to the world, in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible, the line should be clear.”19 In the absence of a widely accepted definition of the word “authorization”, and lack of direction regarding potential criminal consequences, successful governmental prosecution of a counter-hacker would be extremely difficult. Indeed, a recent notable case exhibits a scenario where counter-hacking was deemed legal by the courts, in spite of the CFAA and other anti-hacking statutes.

In December 1999, University of Wisconsin system administrator Jeffery Savoy noticed that one of the university’s mail servers may have been compromised by a hacker. Savoy traced the intrusion to a specific computer and blocked that computer’s Internet Protocol (IP) address, completely restricting access to any university resources. He then contacted local police and the FBI, who instructed him not to take any additional action until a search warrant could be obtained. However, the hacker changed his computer’s IP address and regained access to the server. When Savoy realized that the hacker had once again infiltrated the server, he became concerned that the integrity of the server and the data it contained was in serious jeopardy.

Savoy wanted to confirm that both attacks on the university’s mail server had originated from the same computer. To do this, Savoy used his own workstation to remotely control the suspect computer and then executed several commands to verify that the computer in question was the source of both hacks. Savoy contacted the FBI again and relayed his growing concern. FBI agents asked Savoy not to take any more action until they had a search warrant, at which point the FBI would begin a thorough investigation.

However, Savoy felt that preserving the security of the university’s system required immediate action. Savoy decided to coordinate with university police to physically remove the computer from the network. Savoy and a university police detective made their way to the suspected hacker’s apartment. The suspected hacker, Jeremy Heckenkamp, was not in the apartment, but a roommate invited Savoy and the detective inside. Once Heckenkamp returned, Savoy obtained his permission to confirm that the computer in question had been used to gain access to one of the university’s e-mail servers.

Heckenkamp later contended that Savoy’s remote control of his computer constituted an illegal search under the Fourth Amendment, and was an infringement of his reasonable expectation of privacy. He argued that any evidence obtained in this manner was inadmissible in court and his conviction should be overturned. The United States Ninth Circuit Court of Appeals disagreed.
Under these circumstances, a search warrant was not necessary because Savoy was acting purely within the scope of his role as a system administrator. Under the university’s policies, to which Heckenkamp assented when he connected his computer to the university’s network, Savoy was authorized to “rectif[y] emergency situations that threaten the integrity of campus computer or communication systems . . . “ Savoy discovered through his examination of the network logs . . . that the computer that he had earlier blocked from the network was now operating from a different IP address . . .

This discovery, together with Savoy’s earlier discovery that the computer had gained root access to the university’s Mail2 server, created a situation in which Savoy needed to act immediately to protect the system. Although he was aware that the FBI was already seeking a warrant to search Heckenkamp’s computer in order to serve the FBI’s law enforcement needs, Savoy believed that the university’s separate security interests required immediate action.20

The court concluded that “[a]lthough Heckenkamp had a reasonable expectation of privacy in his personal computer; a limited warrantless remote search of the computer was justified under the special needs exception to the warrant requirement.”21 This exception indicates that warrants are not required when “special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.”22 Because Savoy acted to protect the university’s systems, and not to aid law enforcement officials, the counter-hack (and the evidence it provided) was legally justified.

20 United States v. Heckenkamp, 482 F.3d 1142, 1147–48 (9th Cir. 2007).
21 Id., at 1147.
III. COUNTER-HACKING’S LEGALITY

Clearly, there are issues with the consistency of the American judicial system’s views on the legality of counter-hacking. The vague and sometimes contradictory nature of legislation and judicial rulings demands further clarity and exposition. However, Heckenkamp and other well-established legal principles demonstrate the value of several arguments for the establishment of legal protections for counter-hackers in specific situations.

Self-defense is universally recognized in American courts as an acceptable form of affirmative defense, whereby a defendant can confirm that they have committed a crime, but for legally justifiable reasons. Black’s Law Dictionary defines self-defense as “the use of force to protect oneself, one’s family, or one’s property from a real or threatened attack.”23 Eugene Volokh, law professor at UCLA, notes that even in the absence of a clearly defined self-defense clause within a piece of criminal legislation, this affirmative defense still may be successfully applied.24 Thus, even though the CFAA makes no mention of self-defense in the face of an attempted computer hacking, the law necessarily allows the use of reasonable force to protect one’s property against imminent or immediate attack.

In Passailaigue v. United States, property is defined as “more than just the physical thing — the land, the bricks, the mortar — it is also the sum of all the rights and powers incident to ownership. . . It is the tangible and the intangible.”25 Therefore any data stored on a server or network, as well as the right to use the network itself, can be recognized as property of a given entity. It also follows that agents of an organization that are specifically tasked with defending the data and other networking systems of the organization would be justified in responding with appropriate force to repel attacks directed at the organization and its computing infrastructure. This

principle was clearly demonstrated in *Heckenkamp*, wherein Savoy acted within his role as system administrator to protect the property of the University of Wisconsin.

As long as the system administrator uses reasonable force, the administrator would be legally justified in taking necessary action to ensure the continued security of the systems for which he is responsible. This reasonable force may legally be used to halt the attack, and possibly identify the attacker for law enforcement officials, as shown by *Heckenkamp*. However, it should be noted that what constitutes ‘reasonable force’ in a defense of property case is also open to interpretation. In *People v. Kane*, the New York Court of Appeals ruled that “The law, . . . in peculiar cases where the act is effectual to repress a wrong, does not hesitate explicitly to authorize the destruction of the instrument with which the wrong is both done at the moment, and threatened for the future.”26 This ruling seems to justify any action a counter-hacker might take to defend their network against attack, including actions that result in permanent damage to the hacker’s machine. Although this case has not been successfully used as precedent in a counter-hacking case to date, it is interesting that the court has already determined that the willful destruction of private property is justified, if done in defense of property rights.

Critics of counter-hacking, however, contend that the hacker and counter-hacker are not the only two parties impacted by a counter-hack. Hackers have found it useful to hack hundreds, or even thousands of computers that can then be used as part of a more powerful attack on the hacker’s real target. These commandeered computers can also help to mask the identity of the hacker, by creating dozens of layers between the victim’s computer and the actual hacker. Because the true owners are unaware that their computers are being used in this manner, computers that have been hijacked by hackers are often referred to as ‘zombies’ or ‘bots’. Privacy advocates contend that the widespread use of zombies makes counter-hacking indefensible, since the counter-hacker can never be sure if he is hacking a computer owned by an innocent third-party, or the hacker’s own computer.

26 *People v. Kane*, 131 N.Y. 111, 111 (1892).
Indeed, one of the most persuasive arguments against the applicability of *People v. Kane* in this context is the existence of zombies. Is a victim justified in participating in the willful destruction of a computer (and by extension, the data it contains) owned by an ignorant, innocent third-party when that computer is being used to infringe upon the victim’s property rights? The complexity of this question and its implications in a digital world require a detailed analysis beyond the scope of this paper. Nevertheless, this unresolved question demonstrates the urgent need for clarification of current computer-related legislation.

Detractors of active defense techniques illustrate the dangerous and illegal nature of counter-hacking by formulating hypothetical scenarios where unintended consequences of the counter-hack create chaos. However, laws have never been written to be applicable to every conceivable situation; laws are written to set out general, guiding principles. It is then the role of the courts to examine individual cases and determine the relative importance of circumstance in the application of the law. By stripping away dozens of complications and ‘what-ifs’, the basic, legal justification for counter-hacking becomes clear.

A system administrator faced with a decision of whether or not he should attempt a counter-hack can be thought of as a homeowner being threatened at gunpoint. Both the counter-hacker and homeowner would be justified in defending themselves and their property if given the opportunity. This self-defense can occur either through physical interference with the aggressor or by interfering with the means by which the threat of harm is being communicated. In other words, a homeowner would be justified in damaging or destroying the gun being used by the burglar, if he believed that the gun posed a threat to his life or property. Similarly, a counter-hacker would have the same right to interfere with the instruments being used by a hacker during the commission of a crime, which in this case would be the hacker’s computer.

At this point, a complicating factor can be added. Suppose that instead of using his own handgun, the burglar is brandishing a previously stolen Civil War-era revolver. The homeowner damages the valuable firearm, and the burglar is arrested. The authorities trace
the handgun to its rightful owner, who proceeds to file a civil lawsuit against the homeowner, seeking damages for the homeowner’s willful destruction of private property. Was the homeowner justified in damaging or destroying the revolver that was being used to threaten him? Surely, the court would not force a defendant to determine ownership of a weapon before taking action to protect himself from that weapon. Rather, it seems reasonable that the court would conclude that the burglar would be liable for any damages that occurred as a result of his use of the gun as an instrument used in the commission of a crime. In this hypothetical situation, the homeowner is justified in responding with reasonable force to an immediate threat to his person or property, regardless of whether the legal owner of the instrument is involved in the criminal act or not.

This admittedly contrived example demonstrates the basic arguments for the legalization of counter-hacking. Lack of knowledge of the ownership of the instrument that is being used in the commission of a crime does not restrict the manner in which the victim may legally defend himself and his property. That is not to say that doing so is the morally or ethically correct course of action; indeed, the ethical justification of defending a network by intentionally damaging or destroying a computer that may not be owned by a hacker is questionable at best. However, the law clearly does not require a system administrator to conclusively prove that the legal owner of the attacking computer is the actual hacker before taking action to defend his network.

There is also a strong policy case for the legalization of counter-hacking. Stewart Baker, former NSA and Department of Homeland Security official, notes “. . . the social value of identifying and alerting [victims] outweighs the already attenuated privacy interest of the true owner.”27 By alerting third-parties that their computers have been compromised, counter-hackers actually serve to protect the privacy of a hacker’s victims. Baker also points out that a law that restricts counter-hackers’ ability to defend their systems because of ignorance as to the owner of the attacking computer would effec-

27 Baker et al., supra note 23.
tively provide immunity to attackers. A hacker that knows that the chance of retaliation or capture is low will be much more likely to continue hacking than one who is concerned about the possibility of being caught by a competent counter-hacker.

The stakes are simply too high to continue limiting the ways in which system administrators can defend their networks. Administrators need to be able to use every weapon in their arsenal to protect the computing infrastructure that is relied upon by millions every day. As the reach of the Internet continues to grow, the consequences of a successful hack have expanded beyond theft of intellectual property or confidential consumer data. Hackers threaten both the global economy and national security. System administrators must be allowed to swiftly respond to threats against their systems in order to protect both their organization, and those who interact with that organization through their own computers.

IV. CONCLUSION

Computers have made the world more connected than ever before. Unfortunately, they have also put private information and national security at greater risk as well. In order to respond to the persistent, real threats posed by hackers working as individuals or groups, a judicial answer to the question of the legality of counter-hacking is necessary. System administrators for corporations, educational institutions and government entities must be allowed to respond with necessary force to repel and deter attacks designed to steal sensitive information and cause massive disruption to daily living. Of necessity, this involves the legalization of counter-hacking in situations where there is a clear and present danger or ongoing attack. IT security experts are justified in responding with reasonable force to repel and end the attack in defense of the networks and data for which they are responsible.

While it would be naïve to think that the clarification of counter-hacking’s legality will stem the hacking epidemic, it is possible that an additional weapon against cyber-criminals would be of tremen-
dous benefit to the information technology community. In a world where teenagers are capable of circumventing the security systems of billion-dollar corporations, network defenders need every advantage they can get, including counter-hacking. Hopefully, as network infrastructure that has been over fifty years in the making becomes safer, further advances in technology will continue to improve digital security and convenience for millions of people worldwide.