Richena Purnell-Sayle
BIOD 610
July 22nd, 2014
Dr. Brian Mazanec

Reverse Hacking for Private Industry

Imagine you are a systems administrator for a technology company and you realize that someone has just hacked into the company network and stolen proprietary information. What can you do? Your first thought might be to track the data theft to external servers to delete the data from the thief's computer. However, accessing the thief's networks is in violation of a federal law called the Computer Fraud and Abuse Act[1]. Even embedding triggers into your data to alert you that it is stolen is legally shaky. So what can you do to retrieve your data? Right now, not much. The most likely advice you will receive from law enforcement is that your company should improve security for next time. However, companies of all sizes and functions are beginning to aggressively argue that typical cyber defense tools like firewalls, patching vulnerabilities, and anti-virus software are no longer enough to secure their systems. Reverse hacking, like in the scenario above, could deter attackers and provide information that will help avoid future attacks.

Most coverage and research over reverse hacking discusses whether or not it is illegal under current law. This paper seeks to determine whether the US law accurately reflects the correct line between which types of reverse hacking should be permissible and which should not. Section one defines reverse hacking and examines types of reverse hacking. Section two explains the differences between the public and private sector in the US and makes recommendations for which reverse hacking models should be considered acceptable. Section three examines current policy and makes recommendations for revision and work-arounds. Section four briefly reflects on US actions regarding reverse hacking from an international perspective.

[1] Scenario adapted from "Black Hat: Hacking Back - The Best Defense May Not Be the Best Offense | SecurityWeek.Com," accessed July 17, 2014, http://www.securityweek.com/black-hat-hacking-back-best-defense-may-not-be-best-offense.

I. Reverse Hacking and Active Defense

In the world of offensive cyber security, there are many ways to describe what is essentially the same action: “reverse hack”, “trace-back”, “counter hack”, “hack back” or softer phrase like “active defense”. Since this paper focuses on the actions of private industry it primarily uses the terms “reverse hack” or “active defense” unless the subtlety is important. A reverse hack is whenever the defender leaves his/her own computer network to investigate or retaliate against another network. Active defense is a general term used by security companies to describe a multi-level approach to cyber defense ranging from benign (in network trickery) to full scale retribution attacks. “Hacking back” is a standard term used in the field but is only used in this paper when referring to deliberate and manual accessing of attacker’s networks.

In order to better understand why so many private companies want to implement an active defense model, it is important to understand the current security structure. In general, after a cyber intrusion, the affected company applies the equivalent of a cyber band aid on the intrusion. If possible, it will hire a security expert to stop the attack. They will follow the electronic trail of the attack by examining the packets of data one by one; this could take hours or days depending on the complexity of code. Many companies do not have the resources to investigate the source of the attack. They can only try to stop it and try to limit the fall-out. Private companies have very little legal recourse once they are attacked. Law enforcement usually only investigates high profile cyber intrusions. The FBI and other agencies are understaffed and are often preoccupied with tracking down the intruders of their own networks. Fittingly, in “Defending Networks by Taking the Offense”, Stewart Baker compares law enforcement’s response to that of a local police station when someone’s bike is stolen. (The best they can muster is some sympathy and advice on future security[2].)

[2] Stewart Baker, “Defending Networks by Taking the Offense,” Professional Blog, *Skating on Stilts*, (June 17, 2012), http://www.skatingonstilts.com/skating-on-stilts/2012/06/defending-networks-by-taking-the-offense.html.

Active Defense Options

There are three main categories of anti-hack methods[3]. The first group of active defense tools does not require accessing anyone else's network and therefore does not cross any legal barriers. These measures typically aim to slow or confuse the hackers, giving the defenders time to create a defense.

- Honey pots / fake networks - Honey pots are fake or decoy systems / servers that track and learn about system intruders. They are hosted separate from the main system and are continually monitored.
- Fake Documents - decoy data used to distract cyber thieves from taking the real thing.

The second group of anti-hack measures includes those that are more legally ambiguous, depending on how far the action travels into foreign networks.

- Use beacons -These are tracking devices embedded within code. When information is stolen, they alert the defender that they have been compromised and can provide information about the culprit[4]. These can be coded to provide easy gateways into the attacker's real or stolen network. These are legally ambiguous because beacons must transmit data back from an external network[5].
- Embed code with logic bombs that will delete data once it is stolen. This is currently legally suspect because the data is on someone else's network by the time it is deleted.
- Determine the real IP address of a user that is hiding behind a proxy. One way is to embed a bug inside a word processing document. This helps track down the hacker.
- Use a Trojan horse or other tool to pinpoint the physical location of an internet user.

[3] This list covers the general types of reverse hack but is not intended to be comprehensive.
[4] Baker, "Defending Networks by Taking the Offense."
[5] Ibid.

- Spider traps – These are a set of web pages that cause a search-bot to make so many requests it crashes. Spider traps are hosted on a users own network but cause disruption in the network of the infiltrator.
- Use a program that can disable a Denial of Service (DoS) attack virus by impersonating the hacker's computer system. That system can order the zombie (or proxied) computers to stop sending the attacks or even to re-aim them at the source of the virus[6].

The third group of anti-hack measures includes those that are considered true hack-back actions because they involve breaking into the network of the attacker. Some are considered to be purely retaliatory actions by the victims of cyber attack.

- Hack into intruder's network to retrieve stolen information.
- Hack into intruder's network in order to collect evidence against the thief or even take a picture of the intruder with their own webcam.
- Alter stolen data within the intruder's network.
- Embed malware in data that will attack the thief's computer.
- Hack into the intruder's network directly to disable or destroy the hacker's computer or network.
- Destroy any data of an unauthorized network which has accessed the defenders systems without permission.

Skilled network engineers can create and launch most examples in all three categories of anti-hack strategies on their own. In addition, most of these tools are available in a commercial security product or as a Linux tools.

[6] Vikas Jayaswal, William Yurcik, and David Doss, "Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?," vol. 1 (presented at the Advanced Communication Technology, 2004. The 6th International Conference on Advance Communication Techonlogy, South Korea, 2004), 383, http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=1013841.

Private Companies versus Governmental Agencies

The US government, military, intelligence agencies, and law enforcement are already participating in reverse hacking and hack backing. The military publicly acknowledges its engagement in offensive cyber defense as is supported by Article 22 of the UN Responsibility of States for Internationally Wrongful Acts. The law allows countries to launch counter measures in response to a "wrongful act"[7]. A governmental hack back in response to a cyber attack is considered a justifiable act of self-defense. Indeed, the US military already engages in purely offensive attacks such as Stuxnet; marginally offensive tools like hack backs are substantially less intrusive. The legality regarding American law enforcement's engagement with hacking back is less clear but the FBI and other agencies do it either way. The Patriot Act does allow for law enforcement to reverse hack if they have FISA authorization. Additionally, propose laws such as CISPA seek to increase these agencies' legal ability towards active defense.

While governmental groups can hack back in specific cases, hacking back and other reverse hacking by private businesses is illegal in the US (and most other western countries). Controversy over the legality and appropriateness of reverse hacking has heated up recently as corporate cyber espionage and DoS attacks on companies have increased exponentially. From a financial perspective, the average cost of one cyber attack on a company is over a million dollars[8]. The annual damage to US private business caused by such attacks is estimated at a hundred billion dollars[9]. Like the federal government, US corporations are often victims of international cyber espionage and attacks. In fact, most cyber espionage from China is focused on the theft of trade secrets, technology and intellectual property from companies. Some of these victims are government defense contractors but the rest vary in scope of

---

[7] Kevin Townsend, "The Hack Back Controversy," *Infosecurity*, January 2014, http://www.infosecurity-magazine.com/view/36326/the-hack-back-controversy/.
[8] "Cyber-Attacks Cost $1 Million on Average to Resolve," *Infosecurity*, accessed July 17, 2014, http://www.infosecurity-magazine.com/view/34990/cyberattacks-cost-1-million-on-average-to-resolve/.
[9] *The Economic Impact of Cybercrime and Cyber Espionage* (Center for Strategic and International Studies, July 2013), 4, http://mcaf.ee/1xk9a.

business. For example, the latest Chinese attacks allegedly commited by five Chinese cyber spies were aimed at American solar panel, steel, power plant construction, and special metals corporations[10]. Since cyber threats to US companies are as severe as those the government faces, private companies should have similar defense abilities as the government, especially if there is little demonstrated danger with these accesses.

How Companies Use Active-defense

Despite issues regarding legality, corporations are already engaging in counter attacks. According to the Economist magazine, one third of the 181 attendees of the 2013 Black Hat conference had already engaged in retaliatory hacking[11]. One of the most well-known offensive security companies is called CrowdStrike. The company's Falcon platform uses Big Data collection for real-time detection of threats, attribution of those actors, and disseminates data for immediate action[12]. Crowdstrike supplements the collected data with its other intelligence and research to create a powerful detection system for which it can charge a premium. ($25,000 per year is the base rate.[13]) CrowdStrike is controversial because now that it has the technical capability to react in real-time, it is unclear from a legal standpoint what useful security action they can take that will not require entering any computer's system without permission. (By law they must have permission to access other networks.) CrowdStrike is working with a former FBI lawyer to help identify the line between legal and illegal defensive action[14]. It is likely that the company will test the waters to see how far they can go before receiving legal action.

---

[10] Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Justice News, *Department of Justice*, (May 19, 2014), http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

[11] "Firewalls and Firefights," *The Economist*, August 10, 2013, http://www.economist.com/news/business/21583251-new-breed-internet-security-firms-are-encouraging-companies-fight-back-against-computer?zid=291&ah=906e69ad01d2ee51960100b7fa502595.

[12] Thomas Brewster, "RSA 2013: Get The Lawyers, Offensive Security Is Go," *TechWeekEurope UK*, accessed July 6, 2014, http://www.techweekeurope.co.uk/interview/rsa-2013-crowdstrike-offensive-security-108950.

[13] "Firewalls and Firefights."

[14] Brewster, "RSA 2013."

As we will see in the next section, US laws regarding active defense are ambiguous and this ambiguity leaves small companies afraid to innovate.

Another corporation, called Endgame, has adapted government intelligence technology for corporate use. Endgame has developed a system, called "Bonesaw", which can detect what software is being use by any device that is connected to the internet. The main idea behind "Bonesaw" is that the user can check for vulnerabilities on his or her own system but it can also be used to detect vulnerabilities on other systems[15]. Additionally, FutureVision's "Blitzkrieg" uses DoS attacks to overload the hacker's system and MyKronos' security software detects hacking in real-time and distracts the hacker by presenting fake vulnerabilities for it to attack. Other companies specialize in complicated honey pots, dummy webpage diversions and other diversionary networks. However the anti-hack technology functions, the main goal in offensive security is to convince the attacker that the effort needed to attack a network is not worth the effort and time needed.

The Dividing Line Regarding Active Defense

The arguments against reverse hacking in the private sector fall into three themes: first, as mentioned previously, reverse hacking can harm those who's IPs have been hijacked for cyber attacks; second, reverse hacking is often merely vigilante justice that serves limited purpose beyond revenge; third, since reverse hacking can provide access to the other networks, civil liberty and individual privacy are threatened. These concerns are reasonable and should be closely considered when establishing or editing regulation regarding reverse hacking and active defense.

To examine whether or not the line between legal and illegal in legislation like CFAA is properly placed, this sections refers back at the three categories of active defense laid out earlier in this paper. The first group of defense measures like honey pots and fake documents are obviously legal since they do not require access to another network. The legality of the second group is currently debated. Since

[15] "Firewalls and Firefights."

they require some use of the intruder's network, they are technically illegal as defined by the current version of CFAA. However, they should be allowed as they cause little proven harm to bystanders or even the hackers themselves. For example, beacons that call back to the owner from the attacker's network are clearly acceptable tools of cyber defense as they are part of the originally stolen data. Logic bombs that are set to delete data if it is stolen are suitable for the same reason. Embedding a bug in documents that will reveal the thief's IP addresses once the documents are stolen is acceptable so long as they had to access the original user's network to access the bugged document. Using spider traps to stop intruders is also acceptable because they happen in real time. If the hacker stops the intrusion, the spider traps stops blocking. Decloaking the real IP address of a user is acceptable. However, pinpointing the physical location is a disproportionate action because the resulting privacy invasion is not necessary in order to deter the crime. Instead, the IPs should be turned over to authorities to investigate in order to prevent privacy incursions.

The third category of anti-hack measures veers too far away from a reasonable preventive measure and too close to vigilante justice. Therefore, anti-hack options in category three should remain illegal and unacceptable actions for companies. It is true that once attacked, most administrators would be tempted to destroy a hacker's system, post their picture on Twitter, or even just hack back to retrieve the lost data. However, these actions are not justified as the benefits do not outweigh the potential costs. Allowing hacking backing, even if the hack can be warranted, opens up potential for an uncontrollable domino effect of retaliatory attacks.

III. Current Policy

The Computer Fraud and Abuse Act

Although many laws address computer and network violations, the Computer Fraud and Abuse Act (CFAA) is considered the chief and most comprehensive related legislation. The CFAA was enacted in 1984 but has since gone under many major amendments. The bill originally only protected computers

belonging to the federal government and large financial institutions. By 1998, the CFAA covered practically all computers connected to the internet. Out of the seven sections of the CFAA, two sections are most pertinent to active defense and hacking back:

- Whoever intentionally accesses a computer without authorization or exceeds authorization and thereby obtains information from any protected computer, has committed a felony. Courts have determined a "protected computer" to be **any** computer connected to the internet. Section (2)(C)[16].
- Whoever knowingly causes the transmission of a program, information, code or command and causes damage or intentionally accesses a protected computer without authorization and causes damage, **intended or not,** is in violation. Section (5)(A&C)[17].

Therefore, any time a user accesses another person's computer network without permission, they are in violation of section 2 of the CFAA. The vagueness of this section has caused much confusion and varied interpretation since it is not clear what constitutes authorized access.

Section 5 of the CFAA reflects the well publicized concerns regarding unintended consequences of hacking back. After being the victim of a hack it is tempting to respond in kind. The victim could try to hack back into the hacker's computer or send a logic bomb through stolen data in order to harm the hacker's system. However, since hackers often connect to the target through a proxy system which has potentially also been hacked, it is likely that digital revenge will result in harming an innocent third party. CFAA would hold the person hacking back responsible for whatever damage occurred to all systems, intended or not. An often used example in hack back debates takes the scenario to the

[16] "18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers," *Legal Information Institute: Cornell University Law School*, January 3, 2012, http://www.law.cornell.edu/uscode/text/18/1030.
[17] Ibid.

extreme: a hack back leads back to a hospital network, accidently shuts down ICU computers, people die, and the original hacking vistim is then liable for murder[18].

The Patriot Act resulted in further amendments to the CFAA that allows for increases in fines and prison sentences and the capacity for civil law suits by any person who suffers a loss of $5000 of more. The broad definition of a "loss" includes costs of responding, conducting damage assessments and fixing damaged computer systems; thus illustrating the ease with which active defense companies or individuals can be prosecuted.

Other Legislation

The Electronic Communications Privacy Act of 1986 (ECPA) focuses on extending wiretapping by law enforcement to monitoring and searching electronic communications and allows employers to intercept and monitor communications on their own networks. The ECPA provides companies with a legal mechanism to defend and investigate breaches and to seek criminal claims.

Most US states have their own legislation to protect companies and individuals against computer crime by criminalizing unauthorized access to networks. Many state laws are limited in scope and sometimes clash with federal law. In some states, the defender could argue self-defense[19].

Revising Legislation

US legislation and law enforcement techniques have not evolved as fast as the scope and skill of cyber crime. Those defending networks are at a substantial disadvantage. Currently, in all levels of defense from private industry and national security, the criminals have the advantage. Companies are aggressively pursuing technologies to limit this advantage. Instead of companies innovating around laws or having to blatantly ignore inflexible federal legislation, there should be an opportunity to revisit legislation to clarify national security and law enforcement priorities in order to create better

[18] Baker, "Defending Networks by Taking the Offense."
[19] "The Hackback Debate | Steptoe Cyberblog," accessed July 6, 2014, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

opportunities for self defense. Because of its dominance in the realm of cyber security legislation, the CFAA is the obvious place to look when considering reform. The last direct reform to the CFAA was in 1996 and subsequent reforms have been to operationalize the Patriot Act. The main goal in those reforms was to strengthen the US government's legal ability to pursue intelligence collection and to legally require private business to share some information with the government. These reforms have likely broadened the CFAA too far; the next group of reforms should clarify. Indeed, there have long been calls for revision (or even eliminating) the CFAA from many communities ranging from privacy advocates and hacktivists to security companies. I propose revision to section 2 of the CFAA; Section 5 should be left as is, at least initially.

First, the CFAA does not clearly define authorization. This leaves a gap in the law which is currently used by lawyers to argue probable cause or technicalities of network authorization. However, amending the law would allow everyone, not just those with ex-FBI lawyers, equal access to the internet and network protection. Specifically, the definition of authorization could be extended to allow users to access systems that have accessed theirs. Specifically, if someone hacked my computer, I thereby have a right to hack back theirs. Of course, this is highly problematic because hackers rarely attack a system directly from their own computer. One way to mitigate the concern and injury this proposal might cause is to continue to hold reverse hackers responsible for any damages, regardless of intention. This should limit actions to those defenders who are confident they will connect to the correct computer (not the proxy).

Second, not every computer should qualify for the same level of protection. Other sections of the CFAA have already been amended to add special protections for government and other high security systems. Likewise, section 2 should also specify that users can, in a limited capacity, access IPs that can be proved to have accessed their own first. If the defender or company is prosecuted, they would need to provide evidence proving that the intruder had harmed their system or stolen data. Section 2 should

also lessen the comparative liability of those who access a computer, unlawfully or not, but do not steal data or harm the computer.

New Legislation

As an alternative or in addition to amending the CFAA, new regulation regarding active defense could be created. This would answer concerns about cyber vigilantism by accrediting and reviewing active defense companies and holding them accountable for mistakes. Only these defense agencies could participate in active defense including trace backs and reverse hacking. The companies would have to prove necessity and proportionality[20].

The Next Best Thing: Alternatives to Changing Policy

It is clear that cyber defense companies are going forward with innovative and aggressive new ways to protect networks, regardless of the vague legalities. There are two main ways companies can navigate the waters.

First, although not easy or even reasonable, it is possible for some active defense technology to be innovated around the CFAA's generic authorization requirement. For example, beacons could be coded to work like standard email receipt messages. In this way, anyone who opens the documents can be considered to have "authorized" the document[21]. An additional concern is the fact that in order to follow an IP address thru the internet, one needs to access every server the attacker has compromised. Since traces must occur during live connection, it is possible to send a digital message requesting access to pass through the third party server[22].

---

[20] Adam Segal, "Hacking Back, Signaling, and State-Society Relations," The University of Toronto, *Cyber Dialog*, (March 1, 2013), http://www.cyberdialogue.ca/2013/03/hacking-back-signaling-and-state-society-relations-by-adam-segal/.

[21] Baker, "Defending Networks by Taking the Offense."

[22] Jayaswal, Yurcik, and Doss, "Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?".

Second, if the law cannot be revised to allow companies to actively defend their networks, it may be worthwhile for companies to do it anyway[23]. Companies need to protect their information and clients. The potential financial loss from a federal fine or lawsuit could be much less than the loss from a network attack. So far, the Justice Department has not prosecuted any firm for hacking back. (Although private individuals have been prosecuted under the CFAA under various levels of legitimacy.)

If private companies are left to aggressively defend their own systems, a generally agreed upon standard of conduct is necessary. Michael Tanji's four principles for computer security privateers provide a useful guide[24]. First, in order to practice self-help, companies need to make sure they have taken all proper steps to defend their networks from the outset. Second, reverse hack actions must be in proportion to those of the intruder. Third, companies must have established principles regarding reverse hacking to which they are held accountable. Lastly, companies using aggressive defense practices must demonstrate that they have the skills and infrastructure to do so. Reverse hacking implemented by an incompetent administrator could result in significant damage or loses for the company as well as to third party victims[25].

IV. International Considerations

If the US revised legislation specifying a corporation's right to reverse hacking (in special circumstances), it would set a precedent world-wide. Currently, most countries allowing reverse hacking limit its use to law enforcement. Notably, many countries in the EU extend wider privileges to their law enforcement then the Patriot Act affords American law enforcement[26]. Many other countries are following the US and Europe with various cyber crime legislation. For example, the Philippines passed its first comprehensive computer crimes legislation in 2012. This act, called the Cybercrime Prevention Act

---

[23] Aarti Shahani, "Tech Debate: Can Companies Hack Back?," News, *Al Jazeera America*, (September 18, 2013), http://america.aljazeera.com/articles/2013/9/18/tech-debate-can-companieshackback.html.
[24] Segal, "Hacking Back, Signaling, and State-Society Relations."
[25] Michael Tanji, "Privateering as a Solution to Cyberspace Threats," *Haftofthespeer.com*, 2006, http://www.haftofthespear.com/wp-content/uploads/2010/06/Buccaneer.com_.pdf.
[26] Townsend, "The Hack Back Controversy."

of 2012, is much more specific than the CFAA . It denotes that network intrusions that do not cause damage receive lesser penalties than those that do[27]. Since the US was one of the first countries to create computer abuse legislation, it also has some of the oldest legislation. The US could therefore benefit by examining how these more specific legislative structures are working out. In the meantime, US corporations are experimenting with reverse hacking technology in countries that do not yet have comprehensive computer crimes legislation[28].

Conclusion

When describing active cyber security defense, Stewart Baker said, "Our security may be toast, but so is theirs"[29]. The point here is that cyber attackers demonstrate the same vulnerabilities as all other public or private networks. Hackers make mistakes like leaving bits of code, reusing passwords, and using the same vulnerable software. In other words, why not exploit the same vulnerabilities to defend your network that hackers use to attack your network? Companies in the US create most of the country's innovation and economic development. The massive losses to corporations due to cyber attacks are having a direct affect on the American economy. The question is not whether these companies will have to step up their responses to cyber attacks but whether they will do it in concert with the American government or continue working outside legal frameworks.

---

[27] Congress of the Philippines, "Cybercrime Prevention Act of 2012 - Republic Act No. 10175," Republic of the Philippines, *Official Gazette*, (September 12, 2012), http://www.gov.ph/2012/09/12/republic-act-no-10175/.
[28] Shahani, "Tech Debate."
[29] Stewart A. Baker, *The Attribution Revolution: Raising the Costs for Hackers and Their Customers* (Washington D.C., 2013), http://www.judiciary.senate.gov/imo/media/doc/5-8-13BakerTestimony.pdf.

Bibliography

"18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers." *Legal Information Institute: Cornell University Law School*, January 3, 2012. http://www.law.cornell.edu/uscode/text/18/1030.

Baker, Stewart. "Defending Networks by Taking the Offense." Professional Blog. *Skating on Stilts*, June 17, 2012. http://www.skatingonstilts.com/skating-on-stilts/2012/06/defending-networks-by-taking-the-offense.html.

Baker, Stewart A. *The Attribution Revolution: Raising the Costs for Hackers and Their Customers*. Washington D.C., 2013. http://www.judiciary.senate.gov/imo/media/doc/5-8-13BakerTestimony.pdf.

"Black Hat: Hacking Back - The Best Defense May Not Be the Best Offense | SecurityWeek.Com." Accessed July 17, 2014. http://www.securityweek.com/black-hat-hacking-back-best-defense-may-not-be-best-offense.

Brewster, Thomas. "RSA 2013: Get The Lawyers, Offensive Security Is Go." *TechWeekEurope UK*. Accessed July 6, 2014. http://www.techweekeurope.co.uk/interview/rsa-2013-crowdstrike-offensive-security-108950.

Congress of the Philippines. "Cybercrime Prevention Act of 2012 - Republic Act No. 10175." Republic of the Philippines. *Official Gazette*, September 12, 2012. http://www.gov.ph/2012/09/12/republic-act-no-10175/.

"Cyber-Attacks Cost $1 Million on Average to Resolve." *Infosecurity*. Accessed July 17, 2014. http://www.infosecurity-magazine.com/view/34990/cyberattacks-cost-1-million-on-average-to-resolve/.

"Firewalls and Firefights." *The Economist*, August 10, 2013. http://www.economist.com/news/business/21583251-new-breed-internet-security-firms-are-encouraging-companies-fight-back-against-computer?zid=291&ah=906e69ad01d2ee51960100b7fa502595.

Jayaswal, Vikas, William Yurcik, and David Doss. "Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?," 1:488–91. South Korea, 2004. http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=1013841.

Office of Public Affairs. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Justice News. *Department of Justice*, May 19, 2014. http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

Segal, Adam. "Hacking Back, Signaling, and State-Society Relations." The University of Toronto. *Cyber Dialog*, March 1, 2013. http://www.cyberdialogue.ca/2013/03/hacking-back-signaling-and-state-society-relations-by-adam-segal/.

Shahani, Aarti. "Tech Debate: Can Companies Hack Back?" News. *Al Jazeera America*, September 18, 2013. http://america.aljazeera.com/articles/2013/9/18/tech-debate-can-companieshackback.html.

Tanji, Michael. "Privateering as a Solution to Cyberspace Threats." *Haftofthespeer.com*, 2006. http://www.haftofthespear.com/wp-content/uploads/2010/06/Buccaneer.com_.pdf.

The Economic Impact of Cybercrime and Cyber Espionage. Center for Strategic and International Studies, July 2013. http://mcaf.ee/1xk9a.

"The Hackback Debate | Steptoe Cyberblog." Accessed July 6, 2014. http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

Townsend, Kevin. "The Hack Back Controversy." *Infosecurity*, January 2014. http://www.infosecurity-magazine.com/view/36326/the-hack-back-controversy/.