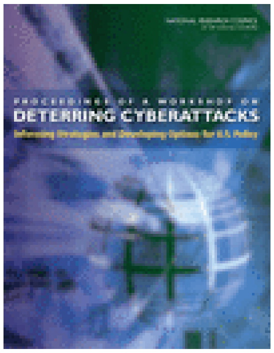

Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council

ISBN: 0-309-16086-3, 400 pages, 8 1/2 x 11, (2010)

Thinking Through Active Defense in Cyberspace

Jay P. Kesan and Carol M. Hayes
University of Illinois at Urbana-Champaign

I. INTRODUCTION

To the collective eyes of the information technology (IT) industry, cyber attacks appear to occur with disturbing frequency. One source indicates that during the six months between September 2007 and March 2008, 1,300 distributed denial of service attacks (DDoS attacks) occurred each day on average.[1] The Pentagon reported being electronically attacked 6 million times during one day in 2008, and a New York executive of a financial house indicated that his company was attacked 1 million times over the course of another day.[2] The danger of cyber crime that defies jurisdictional boundaries is an example of an area where the legal approach requires updating. The current legal system is very effective at addressing attacks using conventional weapons intended to inflict bodily harm, like guns, knives, and bombs. This same legal system, however, is ill-equipped to adequately address issues surrounding attacks where the weapons and targets are computers. This paper is meant to be forward-looking, addressing the use of self defense in response to cyber attacks, which is currently a controversial topic with a questionable legal status, but this topic is also one which many members of the IT industry find attractive.

Cyber attacks, though they generally do not involve bodily harm, are nonetheless very dangerous. Massive economic damage is possible if an important server goes down due to an attack. The damage may be localized, including lost sales due to website down time and substantial costs to replace damaged hardware, but the damage can also be far-reaching due to the extent to which the modern economy relies on Internet activities.[3] Beyond economic harm, if the targeted system is part of the critical infrastructure (such as dams or power plants), damage to the system's network could have dangerous physical consequences. Cyber attacks are also very unpredictable by nature. Because malicious hackers only need a computer and an Internet connection to cause harm throughout the world, the number of possible

[1] Chenfeng Vincent Zhou, Christopher Leckie, Shanika Karunasekera, A survey of coordinated attacks and collaborative intrusion detection, 29 *Computers & Security* 124 (2010).

[2] Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. Rev. 1, 2 (2009).

[3] An estimated $3.5 billion in damage was caused by the Sasser worm in 2004, which exploited a vulnerability in the Windows Operating System. Amitai Aviram, Network Responses to Network Threats: The Evolution into Private Cybersecurity Associations, in *The Law and Economics of Cybersecurity* 143, 144 (Mark F. Grady & Francesco Parisi, eds., 2006).

origins of attack is nearly limitless.[4] This inability to accurately predict the location of attackers on an on-going basis currently renders it difficult for governments to protect attack victims.

Cyber attacks, however, are just one possible avenue of cyber harm. Another category of harm may be referred to as "cyber exploitation," where the goal of the hacker is to obtain data from the target system. This is different from the idea of "cyber attacks," which are executed with the goal of causing direct harm to the target. However, there is some overlap, since an act that is considered cyber *exploitation* may be aimed at obtaining information necessary for executing a future cyber *attack*. The ideas of this paper generally apply to cyber attacks, but there are some implications for cyber exploitation as well. When an issue only implicates cyber exploitations, that term will be used. When both types of harm are implicated, the term "cyber intrusion" will be used. Otherwise, the term "cyber attack" will be used.

What sort of recourse might the organization have in the case of a malicious cyber intrusion? Currently, there are three primary options: civil liability, criminal liability, and purely defensive response. However, it would be difficult to sue the hackers because in almost all cases, hackers route their malicious signals through many different computer systems, finding vulnerable networks that the hacker can use toward his ultimate ends. Even if fast and accurate software could locate the attacking computer, it would be almost impossible to establish who was using the computer to conduct the attack. Criminal liability is also difficult because of criminal jurisdiction issues, since it could be difficult to subject the hackers to criminal liability in another country even if the attacking computer could be found using effective technology to trace the signal back to its original source *and* the human operator of the attacking computer could be identified with sufficient certainty for purposes of prosecution. A purely defensive approach is sometimes effective, but it may be inadequate for mitigating the harm to the system or deterring attacks, and therefore that approach may be insufficient as well.

A fourth more controversial option is that the actors could employ active defense by returning fire at the hackers in order to prevent further disruption of the target system. Active defense can be accomplished by using a combination of intrusion detection systems (IDS) and traceback technology, and then sending data back at the attacker to disrupt the attack. Counterstrikes of this nature have already been occurring on the Internet over the last decade, by both government[5] and private actors,[6] and full software packages designed to enable counterstriking have also been made commercially available,[7] even though such counterstrikes are of questionable legality under the current regime. It is thus apparent that cyber counterstriking is already a practice within the IT industry, and the question then arises as to whether this active defense practice of cyber counterstriking should be regulated and standardized. This paper promotes the idea that currently, technology may not be sufficient to ensure safely executed counterstrikes, and thus continued prohibition may be appropriate. Such prohibition, however, should be explicit and should be in the context of encouraging technological developments so that the sorts of behaviors that are currently being undertaken in secret may eventually be permitted within the optimal framework.

This paper will first discuss a model that evaluates factors to determine whether and when active defense is the socially optimal solution to address cyber attacks. The focus will then shift to a discussion of the policy considerations implicated by this model. What are the capabilities of the current

[4] Even developing countries regularly have internet kiosks available in urban areas.

[5] In late 1998, when the activist group Electronic Disturbance Theater attacked the Pentagon's website with a flood of requests, the Pentagon redirected the requests and sent graphics and messages back to the group's system to cause it to crash. Winn Schwartau, *Striking Back*, Network World (Jan. 11, 1999), http://www.networkworld.com/news/0111vigilante.html.

[6] In 2002, secure software developer Mullen developed a technology for identifying and loading a code on the attacking system in order to "neutralize" the attacking process and stop the propagation of the Code Red and Nimda worms. *See* Thomas C. Greene, *Attacking Nimda-infected Attackers*, The Register (Aug. 8, 2002), http://www.theregister.co.uk/2002/08/08/attacking_nimda infected_attackers/.

[7] In 2004, Symbiot Security announced a new product, iSIMS, that would permit firms to counterstrike when their network came under fire from malicious hackers. Press Release, Symbiot Security Announces World's First Solution to Strike Back Against Network-Based Attackers, http://www.symbiot.com/pdf/pr.030404.pdf (Mar. 4, 2004) ("Symbiot provides the equivalent of an active missile defense system.").

technology, and how might those capabilities shape policy? What sort of attacks (type and strength) could justify counterstrike? Who should be permitted to counterstrike: private companies, the government, or an agency representing the interests of both? If the government is permitted to counterstrike on the behalf of private companies, what might be some possible advantages and controversies arising from such an arrangement? If the government is involved with conducting counterstrikes, what sort of process should be utilized? Lastly, this paper will examine how to address potential harm caused to third parties by active defense.

II. GAME THEORETIC MODEL—WHEN IS ACTIVE DEFENSE THE SOCIALLY OPTIMAL SOLUTION?

In an earlier paper, we proposed using game theory to model the interaction between several measures: technology (IDS and traceback), legal remedies (criminal law and tort-based litigation), and the economic incentives to engage in active defense.[8] One observation was that sufficiently strong criminal enforcement would effectively deter cyber intrusions such that there would be no need for active defense. As noted above, however, there are significant issues with criminal enforcement of laws against cyber crime because of jurisdiction issues and the ease with which hackers can currently render themselves almost impossible to find.

One potential solution to the problem of insufficient criminal enforcement could be to coordinate an international cyber crime treaty to permit enforcement under international law. The Council of Europe's Convention on Cybercrime could potentially provide a regime for international enforcement, but the relatively low participation in the convention makes it difficult to enforce on a wide scale at this time. In an environment where there was accurate technology to identify the origin of cyber intrusions and a capability to hold the hacker criminally liable across national borders, there would be sufficient incentives against cyber crime to avoid needing active defense as an option. Proposing a specific international criminal law treaty on cyber crime is beyond the scope of this paper, but it is an action that we would support and strongly urge the international community to undertake.[9]

As discussed above, criminal enforcement is just one possible way to address cyber crime. Two other alternatives are civil litigation and a purely defensive approach. Active defense is anticipated by the model to be more appealing than civil litigation in situations where litigating would be impractical.[10] The model also concludes that active defense may be appropriate when purely defensive strategies, such as simply dropping incoming packets, would not effectively mitigate harm.

These three primary methods for addressing cyber intrusions (criminal sanctions, litigation, and purely defensive remedies), thus must all be found to be unavailable, impractical, or ineffective in order for active defense to be the socially optimal solution. The model further emphasizes the importance of the technology utilized: reasonable effort must be exerted to employ good IDS technology to assist the firm in detecting intrusions, and advanced traceback technology must also be employed to ensure that the victim firm is accurately targeting the hacker.[11]

The model also anticipates holding counterstrikers liable for damage to innocent third parties, with the expectation that potential tort liability will give firms incentive to not use unnecessary force when engaging in active defense. Potential tort liability to third parties also provides incentive for counterstrikers to use the most accurate technology. The model further posits that third-party damages are an

[8] Ruperto P. Majuca & Jay P. Kesan, Hacking Back: Optimal Use of Self-Defense in Cyberspace (Mar. 2009 Working Paper, Illinois Public Law Research Paper No. 08-20), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932. References to "the model" in this paper refer to the findings of this working paper.

[9] *See* Monika Ermert, *ITU Calls for Global Cybersecurity Measures*, *The H Security* (May 24, 2009), http://www.h-online.com/security/news/item/ITU-calls-for-global-cybersecurity-measures-741711.html (discussing proposals by the International Telecommunication Union for the establishment of a "Cybersecurity Toolkit").

[10] Majuca & Kesan, supra note 8.

[11] Id.

important factor in attaining the socially optimal solution.[12] However, some injured third parties may not have the knowledge or resources to litigate harm caused by a counterstrike, so one possibility is that active defense could be subject to government regulation to protect those third parties. The model also emphasizes that counterstrikers must be permitted to only use necessary and proportionate force and refrain from wantonly damaging hackers' systems out of retaliation.[13] The model does not, however, address who should be permitted to engage in active defense.

At its core, proportionate cyber-counterstriking is self-defense. The right to self-defense springs from the natural instinct for self-preservation, and self-defense is viewed as the use of reasonable force for self-protection. The model focuses on applying this idea of self-defense to the issue of cyber intrusions. The model promotes a view that the socially optimal solution to the threat of cyber intrusions, in the absence of effective remedies being available through criminal law enforcement, civil litigation, or effective passive defense strategies, is to permit (but not require) parties to act in self-defense when reliable technology can be utilized, subject to potential liability for harm caused to the systems of innocent third parties, whose interests are further protected by making counterstrikes subject to government regulation. This liability rule ensures that firms have sufficient incentive to utilize the most effective IDS and traceback technologies to ensure that any counterstrike will have a genuine prospect of hitting the attacker. In sum, this model provides helpful guidance concerning the optimal use of self-defense in cyberspace.

III. THE HOW, WHEN, AND WHO OF ACTIVE DEFENSE IN CYBERSPACE

Having examined the results of our model establishing the socially optimal framework for active defense, the next important questions address the technology involved in active defense, the situations where active defense would be appropriate, and who should be permitted to engage in active defense in a context where such counterstrikes are subject to government regulation. As to the latter question, the two primary possibilities are that the firms themselves could be permitted to counterstrike, or that the government could be the entity entrusted with engaging in counterstriking on behalf of the victim of the cyber intrusion.

A. The Technology Involved in Active Defense

Even in situations where permitting active defense would be socially optimal, allowing cyber counterstriking may still be irresponsible if the technology is inadequate to ensure the accuracy of counterstrikes. In-depth analysis of the full state of the art is outside of the scope of this paper, but it is important to note that the technology involved in active defense is not in its infant stages, and that it is currently the subject of a significant amount of research aimed at improving accuracy and efficiency.

Cyber attacks occur very rapidly, so responses must be prompt in order to best mitigate harm to the targeted system. Detecting a cyber intrusion may require an attack to continue for some time so that a pattern may be detected.[14] Once an attack is detected, however, tracing it to its origin can take a matter of seconds, with error potentially being measured in milliseconds.[15]

When engaging in active defense, the first essential technology is IDS, which has been developing significantly over the past decade. IDS works partly by detecting patterns of attack by a particular attacker, so there is a challenge in detecting intrusions when the intrusion is being executed remotely

[12] Id.

[13] Id.

[14] *See* Zhou, Leckie, & Karunasekera, supra note 1, at 131.

[15] *See* Ethan Katz-Bassett, et. al, Reverse Traceroute 2, 12, USENIX Symposium on Networked Systems Design & Implementation (NSDI) (2010), available at http://www.cs.washington.edu/research/networking/astronomy/reverse-traceroute.html (Awarded Best Paper). Traceroute and traceback are not interchangeable terms, but the underlying technology is similar enough that measurement of errors in traceroute may be used as a description of potential error level in traceback.

by one person attacking through thousands of compromised computers in a botnet. One possible way of addressing collaborative attacks of this nature is to develop collaborative intrusion detection systems (CIDS), and a number of researchers have been examining various methods of doing so.[16] The three primary categories for an approach to CIDS are (1) centralized; (2) hierarchical; and (3) fully distributed.[17] The Zhou et. al article provides a helpful survey of the research concerning CIDS, and also sets out the areas that should be the focus for further research in the topic, including expressiveness, scalability, and accuracy.[18]

Once an attack has been detected, the next step in active defense is to identify the source of the attack. This identification is achieved through some form of traceroute, which is the most widely used diagnostic tool on the Internet.[19] Traceroute is commonly used to evaluate Internet traffic to ensure that data is transmitted effectively, but similar technology can also be utilized to identify an attack's source, and traceroute technology used to achieve that end may be referred to as traceback. Guan's overview of network forensics provides a helpful look into the state of the art of traceback, giving summaries of the four primary IP traceback schemes: (1) active probing; (2) ICMP traceback; (3) packet marking; and (4) log-based traceback.[20] A recent study into reverse traceroute is a helpful illustration of the improvements to the technology.[21] The researchers' reverse traceroute technique was found to offer improvements over both the accuracy and coverage of traditional direct traceroute techniques.[22] The reverse traceroute study found that the median accuracy of reverse traceroute was 87%, compared to 75% median accuracy for direct traceroute.[23]

One additional concern about the technology used in active defense is that the attacker might be spoofing his IP address in order to evade detection. Issues caused by IP spoofing (including harm to third parties) would be most acute in a situation where only traceback technology was used to determine an attack's origin. However, IDS provides additional information to the victim that can indicate if the apparent origin identified by traceback may be inaccurate due to IP spoofing, and this knowledge can prevent the victim from counterstriking against an incorrect IP address, and also potentially help locate the actual source of the attack.[24]

The amount of research into IDS and traceback technology and the results of research into these topics provide strong evidence that the state of the art relevant to active defense is steadily improving. Because the state of the art indicates that the technology will eventually have the capability of addressing some current attribution problems, this paper contains a forward-looking analysis of the potential directions that might be taken by policymakers concerning active defense once the technology is sufficiently advanced. This paper focuses on an idea of active defense that utilizes IDS and traceback technology combined with counterstrikes, in a detect-trace-counterstrike pattern, where the attack is detected via IDS, traced with traceback technology, and then an active response occurs.

Further research is needed to determine what level of confidence in a traceback should be necessary to permit cyber-counterstrikes; for example, is an accuracy rating of 85% sufficient, or should counterstrikes remain illegal until traceback technology's standard error is 5% or less? While additional technological improvements would be beneficial, it is clear that the current state of the technology is adequately advanced to permit the discussion about active defense to move forward into an evaluation of how an

[16] Zhou, Leckie, & Karunasekera, supra note 1.

[17] Id.

[18] Id. at 136 (2010).

[19] Katz-Bassett, supra note 15, at 2, 12.

[20] Yong Guan, *Network Forensics* (Chapter 20), *Computer and Information Security Handbook* (2009).

[21] Katz-Bassett, supra note 15, at 2, 12.

[22] Id. at 9, 11.

[23] Id. at 9.

[24] *See* Tom Chmielarski, Intrusion Detection FAQ: Reconnaissance Techniques Using Spoofed IP Addresses, SANS (Apr. 4, 2001), http://www.sans.org/security-resources/idfaq/spoofed_ip.php. ("One way to help determine which hosts did not send the packets (and therein which host did) is to search firewall and router logs for incoming error messages from the ten hosts that were spoofed, as those hosts react to the packets sent by the target in response to the stimulus from the attacker.")

active defense scheme should be implemented, even if implementation is delayed until the technology is sufficiently accurate. Because one of the key determinants of whether active defense is socially optimal is the availability of accurate technology, this paper does not condone the current vigilante behavior of those currently using less reliable active defense techniques, and instead supports the continued prohibition of cyber-counterstriking until such time as the technology is sufficiently advanced to enable victims to obtain reliable attribution data. The goal of this paper, then, is to provide a framework that can be looked to when the circumstances are ripe for new policy concerning active defense.

B. When Would Active Defense Be Appropriate?

Having established that accurate active defense may be feasible, the discussion now turns to when active defense might be appropriate. This question has two parts: What types of intrusions may justifiably result in counterstrike, and how severe must these intrusions be?

1. What Types of Intrusions Can Be Addressed by Active Defense?

One important consideration is the type of intrusions that could be appropriately addressed using active defense. For our purposes, the key point in the process is the detection stage. Because of the nature of IDS as requiring multiple attempts at accessing the target, active defense would likely not be applicable in circumstances where the intrusion is a single event. There are two types of intrusion that this paper anticipates as being appropriate to address by active defense: DDoS attacks and spiders.

DDoS attacks would be categorized as cyber attacks. One way that a DDoS attack can be undertaken is for the attacker to compromise a large number of computers to create a hoard of zombie systems in order to flood a target with data to knock it off line. When an attacker undertakes a DDoS attack of this type, he first must identify a vulnerability to target and disseminate malicious code to take advantage of that vulnerability (like a virus or a worm) in a large number of systems (perhaps hundreds of thousands). Once the hacker has control of this zombie hoard, he has at his disposal an army of computers that can be ordered to attack repeatedly until the target is taken out. The repetitive nature of a DDoS attack makes it well-suited for the detect-trace-counterstrike pattern of active defense.

The use of spiders to mine data would be categorized as cyber exploitation, rather than cyber attack, because the goal is to obtain data, not to cause immediate harm. Because the hacker accesses the target system repeatedly, there would likely be sufficient activity for a firm's IDS to detect a pattern, making the use of spiders another kind of intrusion that can be appropriately handled using active defense. Whether active defense *should* be used to respond to the threat of spiders, however, is a question related to the severity of the attack.

2. How Severe Should an Attack Be to Justify Active Defense?

The model discussed in Section II sets out a number of factors to consider when determining if active defense is the socially optimal solution. It may be advisable, however, to establish a concrete definition to determine when counterstriking is appropriate. Walker supports a consequences-based approach, where an information-based attack (such as DDoS) would be considered an "act of violence" under international humanitarian law if said information-based attack is aimed at causing the sort of harm (including the damage or destruction of property) that international humanitarian law is intended to prevent.[25] Such an approach provides an important standard that could be applied in the context of active defense, whereby counterstriking would not be deemed an appropriate recourse except in

[25] Paul Walker, Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine at 23 (Journal of National Security Law and Policy, Forthcoming, 2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1586504.

relatively narrow situations where the initial intrusion was severe enough to rise to the level of being an "act of violence."

Since responsive counterstriking is most easily justified as self-defense, and the U.N. Charter permits self-defense in response to an armed attack, another standard is to look at whether the initial attack is an "armed attack" under Article 51 of the U.N. Charter. An armed attack is more than a "use of force," as discussed below, and therefore mere intrusions would not provide sufficient justification for the use of active defense. A threat to critical infrastructure, such as to an electrical grid, would probably rise to the level of being an armed attack, but it is not clear what other type of intrusion would be considered an armed attack such that self-defense would be permissible. It is also unclear whether a cyber exploitation could ever be considered an "armed attack," or if that designation would be restricted to cyber attacks.

C. Should Firms Participate Directly in Active Defense?

In the socially optimal situation where accurate technology is used and no other means of recourse would be practicable, there are potential advantages to permitting the attacked firms to counterstrike directly, such as the increased speed with which counterstrikes could be undertaken, but there are many concerns about permitting this as well. Technology often outpaces legal developments, so private sectors would likely have access to technology that potentially has significant negative effects on third parties, but that essentially exists outside the law. This could lead to hundreds of companies competing to provide IDS, traceback, and counterstrike technologies to thousands of private firms in the absence of any kind of oversight to ensure quality and protect third parties. The lack of technological uniformity could also raise issues. If there is a significant amount of variation and competition among software providers, developers may have incentive to cut costs in order to compete, leading to some software being cheaper but lower quality than others.

Beyond the issues of consistency of implementation and product quality, there is a more significant downside of entrusting active defense to private firms. Our model addressing the optimal use of active defense emphasizes that there are threshold points where permitting counterstrikes would be the socially optimal solution. However, it does not define these thresholds, and determining these thresholds requires some sort of standardization. It would be unwise to allow individual companies to make these decisions on a case by case basis. Some companies would be more risk averse, while some may be more inclined to behave like cyber vigilantes. It is thus important to not place this significant discretion in the hands of private firms, because that would result in a wide array of differing results. In order to ensure that only socially optimal usage of active defense occurs, there needs to be some form of standardization for how an active defense program is implemented. One possible way to achieve this sort of standardization is to utilize a central government entity for the purpose of deciding when counterstriking would be appropriate.

If private firms were permitted to directly engage in active defense, one possible restriction that the government could place would be a requirement that a counterstriking firm have a certain percentage of its capital invested in IT infrastructure. This could potentially help ensure that counterstriking was only engaged in by firms that had the most to lose from an attack that cripples its IT system. If this sort of restriction is adopted, it should probably not apply to firms that control essential services such as hospitals and power grids. However, given the significant downsides of permitting private firms to counterstrike directly, an alternative implementation may be advisable.

D. Should the Government Be Responsible for Conducting Active Defense?

As an alternative to entrusting active defense to the private firms who are injured by the initial cyber intrusions, the government (or a government contractor) may also be placed in charge of any counterstrike deemed necessary. This proposal has several advantages, though there are also some potential pitfalls that must be carefully monitored.

1. *Advantages and Disadvantages to Requiring Government Control of Active Defense*

If the government were placed in charge of any necessary counterstrike, this would simplify matters by ensuring technological uniformity in the software utilized for detection, traceback, and counterstriking. IDS and traceback technologies are developing rapidly, and having one actor responsible for acquiring the technology will ensure that the best technology is put into place for the benefit of society. Another advantage of placing the responsibility for counterstriking with government entities is that there will be uniformity of personnel, and the uniformity can help ensure that all employees responsible for counterstriking will be adequately informed of the processes and dangers.

Our previous paper concluded that a liability rule is important to preserve the optimality of active defense. Targeted firms, under such a liability rule, would be responsible for harm a counterstrike causes to innocent third parties. We also suggest retaining this liability rule if government is responsible for coordinating active defense. If the original liability rule is preserved and firms are still held responsible for harm caused to innocent third parties, on the theory that the government was acting as an agent of the counterstriking firm, that would ensure that firms will not capriciously submit a request to the relevant government agency for counterstrike assistance. A potential liability rule is discussed in more detail below in Section IV.

Another advantage of placing active defense under government control is that such a system would help to control for the dangers of rapid escalation. The future battlefields of cyber wars will likely be found in the private sector. As discussed above, some members of the private sector are already resorting to self-help to defend themselves against cyber attacks. This could lead to a dangerous pattern of attack-counterstrike-countercounterstrike that will escalate rapidly and cause significant damage. Placing control of active defense implementation with the government could help to control this and prevent potentially dangerous rapid escalation of cyber attacks.

On the other hand, there are some potential downsides of permitting the government to control all aspects of active defense. Any advantage that the government has in putting the best technology in place, for instance, is almost exclusively an advantage on the front end only, as once that technology is in place, there may be insufficient incentive to ensure that the technology is consistently kept up to date. Additionally, the nature of government action requires that all actions are undertaken slowly and carefully. While this serves to protect third parties from the hasty responses of others, it may cause issues for those who are the actual victims of attacks due to the increase in response time.

Government involvement could also lead to international political conflicts in the event that a government action has negative effects on another nation's government or population. If individual actors in one country took cyber action against aggressors in another country and inadvertently harmed innocent individuals, the government would likely not be held responsible if it did not somehow encourage the harmful acts. The same government, however, would be the party held responsible if government-sanctioned active defense caused harm to innocents in the other country. This sort of accountability could also be an advantage of government involvement, but it would likely only be optimal if governments uniformly accepted responsibility for active defense within their borders to ensure that the behavior was addressed consistently between all potentially affected countries.

2. *Potential Legal Issues with Active Defense*

There are many possible issues that might arise from counterstrikes. Some of these potential issues would arise in the context of counterstrikes being conducted by state actors, while other potential issues would exist regardless of the party engaging in the counterstrike.

Legal Implications Resulting from Active Defense by State Actors Because of the nature of counterstriking, the act of mitigating harm to the victim's computer could potentially be viewed as inflicting punishment to the attacker in a manner inconsistent with Procedural Due Process under the 5th

Amendment. Under the United States Constitution, the 5th amendment's Due Process clause guarantees that procedures will be adequate to ensure against improper deprivation of life, liberty, or property.[26] However, that is why the model emphasizes the importance of only using as much force as is necessary to mitigate harm to the counterstriker.[27] Our view is that when properly executed, active defense is proportionate response, not punishment, and that it is grounded solely on self-defense and mitigation. Accepting this characterization of active defense, if there is ever an incident where the force inflicted during counterstriking is disproportionate to the amount of force inflicted during the initial intrusion, there may be a Due Process violation. However, if the model is followed appropriately, standard use of active defense should not raise due process concerns.

In addition to constitutional concerns, it is also important to consider the implications of international law. The DOD General Counsel issued an opinion in 1999 stating that the law of war should apply to cyber attacks, and therefore any attacks must be based on the necessity of war in order to avoid potential war crimes charges.[28] The law of war includes requirements such as that the attacker must be able to make effective distinction between combatants and noncombatants, that attacks be founded on military necessity, that steps are made to ensure that any collateral damage is proportionate to the military advantage attained from the attack, and that only weapons that can be targeted with precision at combatants may be used.[29] There would also be a danger of retaliation or retorsion by governments whose citizens are harmed by cyber counterstrikes executed by the U.S. government, which is another reason why it is essential for any government involvement in counterstriking to be very careful and precise. The potential danger of war crimes charges is why our previous paper on the optimality of active defense urges decisions about counterstriking to be made consistent with the idea of a just war.[30]

Other Legal Implications of Active Defense Two other significant areas of law are implicated by active defense, regardless of the party conducting the counterstriking: international humanitarian law, and the Computer Fraud and Abuse Act (CFAA).

War crimes charges would likely only be implicated when the counterstrike is executed by the government, but some international law implications could apply even if the actor was not a state actor. Cyber counterstrikes implicate several elements of international humanitarian law. The initial attack may violate the U.N. Charter if the attack rises to the level of "use of force."[31] However, the U.N. Charter would prohibit the target of an attack from responding in self-defense unless the initial attack was severe enough to be considered an "armed attack."[32] This dichotomy indicates that it is possible for an attack to violate the U.N. Charter without the attack being severe enough to justify the use of self-defense.

On its face, the U.N. Charter applies to states, but because of the nature of cyberspace, it has become apparent to many that private entities will play a key role in future cyberwars. When many government websites operated in the country of Georgia were shut down by DDoS attacks (which evidence linked to computers in Russia), the Georgian government sought "cyber refuge" by moving many of its important websites to private servers in the United States.[33] This action was without the consent of the U.S. govern-

[26] US Const. amend. V. Another potentially relevant clause in the 5th amendment is the Takings Clause, which prohibits the government from taking private property for public use. If state actions cause damage to someone's computer due to cyber counterstriking, this could potentially be a taking under the 5th amendment. It is unclear, however, how Supreme Court takings jurisprudence would apply in this cyber context. Beyond the threshold question of whether a taking occurred, a takings argument would likely fail unless it is shown that the interference with computer property was related to a "public use."

[27] Majuca & Kesan, supra note 8.

[28] Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (May 1999), available at http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

[29] Id. at 10-11.

[30] Majuca & Kesan, supra note 8.

[31] U.N. Charter art. 2 para. 4.

[32] U.N. Charter art. 51.

[33] Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F.L. Rev. 43, 46-47 (2009).

ment, and at least one commentator views this as illustrating that international law issues like neutrality may potentially be implicated by the actions of private actors. The language of Article 51 refers to "the inherent right of individual or collective self-defense" in the event that an armed attack occurs against a U.N. Member,[34] which may suggest that individual actions may be included in the language just like state actions. Since the language seems to permit it and the reality of cyber warfare may even require it, considerations relating to articles of the U.N. Charter should be interpreted as potentially applying to private actors in the context of cyberspace where national boundaries are at best amorphous.

Another domestic legal issue is the implications for active defense from the CFAA. The CFAA's broad language prohibits knowingly transmitting data to intentionally cause damage to a protected computer, and also prohibits the intentional unauthorized accessing of a protected computer where damage is caused recklessly.[35] Some commentators have persuasively observed that even the act of tracing an attack through intermediaries might violate the CFAA if harm is caused to the intermediaries.[36] The phrase "protected computers" is defined as computers that are at least sometimes used by or for financial institutions or the U.S. government where the conduct of the offense affects that protected use, *or* computers that are used in or affect interstate or foreign commerce.[37] The latter category could potentially make all computers connected to the Internet into "protected computers" under the CFAA.

It is an issue of statutory interpretation as to whether a statute enacted in 1986 was passed with the intent that it should apply to the Internet age reality of 2010. The CFAA clearly distinguished between sections that apply to all computers and sections that apply only to "protected computers."[38] The provisions at issue here, the ones prohibiting actions that cause damage, use the phrase "protected computer," whereas provisions that just use the term "computer" cover activities like hacking into systems to obtain information relevant to national security. A broad interpretation of the phrase "protected computers" would be inconsistent with the canons of statutory interpretation, since it would mean that the phrase "protected computer" is redundant of the same concepts communicated by the larger label "computer."[39] If the CFAA was intended to potentially cover every computer in the United States as a "protected computer," there would not have been some sections that referred to "computers" while others specified "protected computers." Therefore, to preserve the vitality of the CFAA, the phrase "protected computer" must be reunderstood in the statute to bring this decades-old statute in line with the reality of the Internet age in 2010.

Preserving the vitality of the CFAA as it was intended can be accomplished in a couple of ways. First, courts can adopt a more narrow interpretation of the second half of the definition of "protected computers," interpreting it to apply only to computers containing sensitive, commerce-related information that would affect a large number of people. This could leave open the possibility of CFAA-based liability for harm caused to health institutions by active defense, without imposing liability under the CFAA for most incidental intrusions into the computers of private individuals whose computers only participate in interstate commerce by virtue of being connected to the Internet. A second way to preserve the integrity of the CFAA for these purposes would be to amend the statute to either eliminate the second half of the definition of "protected computers" or to amend the language in such a way as to narrow the scope of the definition.

International humanitarian law and the CFAA are thus two areas that must be considered when forming a policy concerning active defense. The CFAA is potentially more prohibitive of the sorts of

[34] U.N. Charter art. 51.

[35] 18 USC. § 1030 (2008).

[36] *See* Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 182 (2005).

[37] 18 USC. § 1030(e)(2) (2008).

[38] *E.g.*, 18 USC. § 1030(a)(2) (2008) (". . . intentionally accesses a computer without authorization . . ."); 18 USC. § 1030(a)(4) (2008) (". . . knowingly and with intent to defraud, accesses a protected computer without authorization . . .").

[39] 18 USC. § 1030(e)(1) (2008) ("[T]he term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions . . .").

behaviors that would be involved with active defense, but it is our position that a broad reading of the CFAA would be inconsistent with the canons of statutory interpretation, and thus the CFAA would likely not prove to be a substantial obstacle to implementation of a system to permit active defense.

3. Public-Private Partnerships as an Alternative to Pure Government Control

Even though there are several advantages to permitting the government to have control over active defense, it is important to acknowledge the weaknesses of a pure, state-run regime. As noted in subsection (1), while there is a benefit to having uniformity in software due to a single state entity having control, that benefit exists primarily on the front end, and the benefit would degrade over time if the contractor who supplies the software is not given incentive to continue to improve its product. A purely private regime, on the other hand, would be undesirable, because the lack of uniformity in software and procedure for active defense indicates that a privately run active defense regime would be unpredictable at best.

The importance of the private sector to the future of handling cyber conflicts cannot be under emphasized, however, since the private sector arguably has an interest in addressing vulnerabilities that is at least equal to that of the government. The private sector also may have access to more advanced technologies and more experts than are readily available to the government, since considerable development is undertaken as part of for-profit ventures. One core competency of the private sector, then, is its potentially superior technological expertise and access to cutting edge technology. The corresponding core competencies of the public sector include access to highly relevant, non-public information, the ability to develop uniform procedures, and its access to enforcement mechanisms. One potential way to address these disparities in strengths is to establish a public-private partnership to address active defense issues. A situation where the private sector and government routinely coordinate on matters of active defense would provide the uniformity and legal benefits of government-coordinated active defense, while taking advantage of the private sector's access to top technologies and experts.

Looking to a public-private partnership as a model could be very helpful in forming and shaping a new organization designed to bring private and public actors together to address security and active defense issues. One possible model for such a public-private partnership in this context is the Information Sharing and Analysis Centers (ISACs), which have the goal of advancing and protecting "the physical and cyber security of the critical infrastructures of North America."[40] There are several different ISACs to cover major sectors relating to critical infrastructure, including the Communications ISAC and the Information Technology ISAC.[41] The IT ISAC only lists 20 current members on its website,[42] which does not sound like a significant proportion since some sources indicate that over 70,000 IT companies exist in the United States.[43] However, the member list of the IT ISAC includes Microsoft, IBM, McAfee and Symantec, representing a significant proportion of several areas of the IT market.

The website of the IT ISAC contains several sections, most of which are viewable by members only. The public area of the website includes a Daily News section, a collection of Best Practices documents from a variety of sources, alerts and advisories issued by the United States Computer Emergency Readiness Team (US-CERT), alerts issued by X-Force (a service of IBM Internet Security Systems[44]), a form for members of the public to submit suspicious files to the organization's attention, and a collection of legal documents.[45] The sort of information that is publicly available on the IT ISAC website demonstrates the sort of coordination between private enterprise and government that characterizes public-private

[40] ISAC Council Home Page, http://www.isaccouncil.org/about/ (last visited July 6, 2010).

[41] Id.

[42] IT-ISAC, https://www.it-isac.org/memberlist.php (last visited July 6, 2010).

[43] Information Technology in the United States, manta.com, http://www.manta.com/mb_33_G4_000/information_technology (last visited July 6, 2010).

[44] Internet Security Systems—Research, http://xforce.iss.net/ (last visited July 8, 2010).

[45] IT-ISAC, https://www.it-isac.org/ (last visited July 6, 2010).

partnerships. An analogous arrangement in the context of active defense could consist of frequent updates concerning IDS and traceroute/traceback research, reports concerning potential cyber intrusion trends, and alerts about newly discovered vulnerabilities.

However, public-private partnerships can be difficult to implement. The private sector and government are dominated by two very different cultures, and getting the two groups to work together can be problematic. For instance, there may be a lack of trust between the two groups, with resistance on both sides to share fully with the other, leading to informational asymmetry where one party knows more than the other with respect to some matters. To mitigate these informational asymmetries, the public and private parties need to be encouraged to trust each other and share their expertise so that they can work together in a coordinated fashion in order to attain the expected synergies that drive the collaboration. If a public-private partnership is to succeed, building trust between the parties will be extremely important.

ISACs are generally not viewed as being hugely successful, in part due to the relatively low private sector participation. This low participation is perhaps due to the inherent difficulties of fostering trust between the private and public sectors, and perhaps also because of the resistance some members of the private sector might have to engaging in full cooperation and information sharing with their competitors. A full case study of the ISAC regime is outside the scope of this paper, but would likely be helpful in understanding the advantages and pitfalls of public-private partnerships in the cyber context.

E. Potential Process for Active Defense

Having evaluated the possible advantages and pitfalls of active defense, the next important consideration is the process that should be followed in the event that government-involved active defense is concluded to be the optimal approach. Because of the necessity for quick action when engaging in counterstrike, the first important point is that the process should contain elements conducive to expedited review.

One possible approach might be to establish a process that in some ways resembles the manner in which wiretapping approvals are obtained. Currently, wiretaps are available through the Foreign Intelligence Surveillance Act (FISA), which provides a process for requesting surveillance of a foreign power or an agent of a foreign power through the FISA court.[46] An analogous process could be developed whereby decisions concerning potential counterstrikes are made by an independent body staffed by persons skilled in Internet-related legal issues and who are also specialists in matters concerning complicated computer network and cyber intrusion issues. Such a body could be responsible for evaluating whether counterstrike was appropriate, and could also serve to verify the precision of the technology used.

The agency responsible for active defense must also establish criteria to clearly set forth the threshold requirements necessary to justify active defense intervention. When experiencing a cyber intrusion, the entity requiring assistance should be permitted to petition the agency for such assistance, providing specific information about the intrusion and any harm currently inflicted or anticipated to be inflicted if the harm is not mitigated. The agency in charge of active defense might decide that it would be appropriate to have higher threshold requirements in situations where the victim organization is a private entity versus when the victim organization is a government entity. Such disparate treatment may be justified given the national security importance of prompt termination of cyber intrusions on sensitive government systems. Also, the agency in charge of the active defense process could potentially contract the counterstriking activity out to a private organization with employees that fulfill government or military functions.

IV. EFFECT OF ACTIVE DEFENSE ON THIRD PARTIES

Hackers who engage in cyber intrusions generally seek to avoid getting caught, and one method that they use to evade detection is to route their message through other computers on the Internet in order

[46] 50 USC. § 1805 (2008).

to obscure the origin of their original signal. In addition to using other computers to evade detection, a hacker who compromises a large number of systems could use those computers against the ultimate victim. One possibility is that a hacker might use a virus to gain access to the computers of unsuspecting third parties, turning the computers into "zombies." A hacker with a large army of zombie computers can now initiate DDoS attacks against a firm, flooding the firm's network with data until it crashes.[47] A firm that is monitoring for such attacks could then initiate the process necessary to counterstrike, but what if the ultimate counterstrike causes harm to the zombie computers, whose owners were not involved with or aware of the hacker's malicious intentions?

One very important concern is that these third parties, who we will refer to as "oblivious intermediaries," should be protected from damage caused by counterstrike—but if ignorance of the law is no excuse, why should ignorance of the technology (or at least the basic protections provided by easily available support software) be acceptable? In addition, in some circumstances, the oblivious intermediaries may be unaware not only of the intrusions by the initial hacker, but also of harm caused by counterstrikes. If those oblivious intermediary firms are unaware that their system has been harmed, has their system truly been harmed? And if the oblivious intermediary firms unwittingly became tools of the hacker because of their negligence in maintaining their own systems, why should they be afforded extra protection? One possible solution, then, is to afford no protection for injured third parties, because additional protection creates a moral hazard by permitting firms to avoid the consequence of their own negligence. Policymakers could point to the risk of damage due to counterstrikes as another incentive for computer operators to be more diligent in installing security updates for their operating systems and programs, as well as providing incentive for operators to be more consistent in their usage of firewalls and anti-virus/anti-malware products.

As a policy matter, however, such a harsh approach may be inappropriate. A company with a thousand responsible computer-using corporate employees should not necessarily be punished (via the denial of a remedy) for the careless actions of a single employee on the network. It is standard practice to hold a firm responsible for the negligence of its employees, but ineligibility for remedy would likely be too harsh, since it would be a per se rule that does not easily lend itself to flexibility when considering the circumstances of the situation. Therefore, the firm that finds itself as an oblivious intermediary should be afforded remedy by being permitted to sue the original target of the attack if the oblivious intermediary's system suffered harm as a result of a negligent or reckless counterstrike.

However, we are still left with the problem of avoiding the moral hazard posed by rewarding computer users who willingly remain ill-equipped to handle the threats of modern cyber attacks. The first step that should be taken is education. In order to minimize potential zombie armies, educational materials should be disseminated to underscore the importance of timely security updates and use of software packages that prevent infiltration and that detect if the system has been compromised. Using education to reduce the number of potential third parties that can be harmed could potentially ease the implementation of a liability rule as part of a regime designed to permit defensive actions under the appropriate circumstances.

Failure to protect their systems appropriately should not render parties ineligible for causes of action, but allowing the neglect of the oblivious intermediaries to decrease the damages owed may be an appropriate compromise to ensure that all firms are provided with the incentive to exercise due care in managing their IT infrastructure. Because of variations in tort law between the states, federal statutory intervention may be necessary, potentially in the form of some type of federal cybercrime tort statute. Such a statute should include provisions stating that contributory negligence is not a defense available to a counterstriker in a lawsuit brought by the oblivious intermediary. The statute should, however, make available a comparative negligence option for reducing damages owed. For example, a firm with one careless employee who inadvertently renders the firm's entire network vulnerable would

[47] How Zombie Computers Work, http://computer.howstuffworks.com/zombie-computer3.htm (last visited July 8, 2010).

likely be entitled to a larger damage award than a firm that lacks any systematic controls of network content and quality.

If the government is placed in control of conducting counterstrikes, one possibility to extend civil liability may be to permit suits by foreign citizens against the United States under the Federal Tort Claims Act (FTCA).[48] The government could then resolve the dispute, and then begin a new process to recover the damages from the party that required government assistance. The most significant problem with using the FTCA in this manner, however, is that the FTCA contains an exception for claims that arise in a foreign country.[49] The nature of the Internet age leads to many complications when the question becomes where a cyber harm "arises." One possible solution could be to treat the harm as arising in the state where the counterstrike began, given the almost instantaneous effect that the counterstrike would have on the third party, to be governed by the tort law for negligence of that state.

V. CONCLUSION

In certain circumstances, counterstrikes in response to cyber attacks can be the socially optimal solution. The optimal approach to active defense is to permit (but not require) counterstriking in certain circumstances, while making the exercise of counterstrikes subject to potential liability for damages that the counterstrike causes to the systems of the oblivious intermediaries whose computers have been compromised by the original hacker. Current technology is supported by a large body of research indicating a steady improvement in accuracy in active defense technologies, thus the current state of the art does not necessarily detract from the social optimality of permitting active defense, though further technological developments may be necessary if higher degrees of accuracy are found to be needed.

If active defense is deemed necessary, its existence should be carefully regulated by the government in order to prevent harm to third parties and to prevent escalation by private entities that could potentially lead to crises of international relations. It may also be advisable for a government entity to control the application of active defense in order to ensure consistency and accuracy in counterstriking. Centralizing the exercise of active defense may be preferable to permitting private firms to counterstrike directly due to the need for standardization and consistency when making determinations about whether to counterstrike. A related option could be to create a public-private partnership to address active defense issues, where government and private enterprise would work together on designing and implementing an active defense program.

There are some potential concerns with permitting the government to coordinate active defense efforts. A possible constitutional objection to state involvement in counterstrikes is the danger of a Due Process violation. This paper, however, is based in part on a model emphasizing that the force used during counterstrike should be proportionate and should be no more than that necessary to mitigate the effects of an attack. If this model is followed appropriately, there will be no Due Process violation in standard execution of active defense, because any response will be proportionate and responsive, not punitive. There are, however, other legal provisions, including the self-defense provision of the U.N. Charter, that suggest that the use of active defense would be inappropriate in most cyber intrusion situations.

If the use of active defense is limited to narrow situations and is found to not be inconsistent with current law (including the CFAA), the implications of counterstriking on third parties must also be considered. This paper stresses that the third parties whose computers are used by hackers in furthering attacks against a target must be given incentive to exercise due care in the maintenance of their systems and networks. Offering a pure liability rule that will permit these oblivious intermediaries to recover significant amounts in damages regardless of their own actions would create a moral hazard.

[48] *See* 28 USC. 1346(b) (2008).

[49] Henry Cohen and Vanessa K. Burrows, CRS Report for Congress, Federal Tort Claims Act 5 (Dec. 11, 2007), available at http://www.fas.org/sgp/crs/misc/95-717.pdf.

Avoiding this problem consists of two parts. First, people must be provided with educational material to underscore the importance of maintaining their systems adequately, including installation of all security updates and the usage of functional firewalls and anti-virus/anti-malware software packages. Second, the cause of action brought by the oblivious intermediary against the target of the hacker's attack could be governed by a new federal cybercrime tort statute, which would provide for a comparative negligence scheme, or potentially by an extension of the Federal Tort Claims Act.

In the absence of effective deterrents under international criminal law, a self-help method like active defense offers sufficient deterrence to malicious hacker activity, with the added advantage of possibly mitigating damage to the target of the intrusion. Since there are some situations where the socially optimal solution would be to permit counterstrikes, active defense should not be perpetually prohibited as a matter of policy, but it should be regulated carefully to ensure that counterstrikes are used only in the socially optimal way. Further research in this area is required to ensure the optimal implementation of a potential active defense legal regime.