Highway to Hell: The Shortcomings of the ACDC Act

Highway to Hell: The Shortcomings of the ACDC Act

H.R. 4036 - The Active Cyber Defense Certainty Act (ACDC Act) is a current bill in the House of Representatives which would provide a defense to criminal prosecution for hacking for victims defending against unauthorized intrusion into their systems. This bill, in effect, seeks to legalize defensive hacking by amending 18 U.S.C § 1030 to allow for criminal defense of the use of "Active Cyber Defense Measures" against unauthorized intruders. This paper will demonstrate that in addition to the litany of loopholes, ambiguities, and shortcomings within the language of the bill itself; the idea of legalizing and legitimizing hacking back as a practice is fundamentally flawed as a means of private sector cyber deterrence.

H.R. 4036 - The Active Cyber Defense Certainty Act (ACDC Act) is a current bill in the House of Representatives that was proposed in October 2017 by Representative Tom Graves(R-GA-14) and Representative Kyrsten Sinema(D-AZ-9). The proposed bill would add an exception to the Computer Fraud and Abuse Act (CFAA), the U.S. anti-hacking statute, that would allow defenders to access the network of an attacker should they be the victims of "persistent unauthorized intrusion"[1] into their network. However, as much as the text of the bill leaves to be desired, many of the failings in the bill come from inherent failings in the conceptual foundation upon which the bill is placed.

This paper will take a three-part approach to addressing these problems. First, this paper will analyze the ACDC Act as a self-contained entity; demonstrate that the wording of the bill is flawed in such a way as to exacerbate the issues already present in a hack-back doctrine. Then this paper will consider the bill within the larger context of hacking back as a macro strategy of cyber deterrence in the private sector, and consider popular arguments in favor of a retaliatory doctrine, before finally refuting those arguments and demonstrating why the ACDC Act falls short both technically and conceptually. Among the issues examined are the already common hacking back policies in place at many companies; the legal problem of defining attacker and victim in the context of this bill; the issue of proper attribution; and the moral, legal, and practical grey areas in permitting "defense" while differentiating it from retaliation.

To the Community

The original concept for my paper was an analysis of various retaliatory techniques, as well as a proposal for a novel means of what I learned is frequently termed 'Active Defense' however, while doing research about various means of hacking back, I found many articles deriding the concept as a whole, which piqued my interest, as it wasn't a view I had considered. As I read more about the potential ramifications of legalizing hacking back, I more and more came to believe that the ACDC Act was a bad idea. Recognizing the act as a topical means of discussing hacking back in a broader context, I chose to abandon my original topic, and instead focus on hacking back and the ACDC Act.

The Active Cyber Defense Act

The ACDC Act seeks to amend the CFAA to include an exception for the use of "attributional technology" and "Active Cyber Defense Measures" (ACDM) under the umbrella of acceptable activities. The section on "attributional technology" is relatively straightforward, allowing a 'defender' to use "a program, code, or command for attributional purposes that beacons or returns locational or attributional data" to identify the source on an unauthorized intrusion into their network. The section takes care to

prohibit actions that would go beyond attribution, such as destruction of data, impairment of "essential operating functionality" and intentionally creating a backdoor into the attacker's system[1].

The bill's section on "Active Cyber Defense Measures" is far more interesting and a dissection of the ambiguities and problems in that section will be a major component of this paper. "Active Defense" is a term that, as a recent Slate article put it, "is a polite term for offense"[1]. More specifically, the ACDC Act defines an "Active Cyber Defense Measure" as unauthorized access into the computer of the attacker to establish attribution, disrupt an ongoing attack, or monitor the behavior of the attacker in order to develop defense against future attacks. The bill goes on to qualify what actions are not covered, such as those that destroy data that isn't the victim's, recklessly causes physical injury, creates a threat to the public safety, intentionally surveils or intrudes upon an intermediary's computer beyond what is needed for attribution, intentionally disrupts internet connectivity, or impacts any government computer. In all of this discussion, there have been multiple mentions of attackers and defenders, both of which are defined under the bill as "a person or an entity that is the source of the persistent unauthorized intrusion into the victim's computer" or "the victim of a persistent unauthorized intrusion of the individual entity's computer", respectively. The issue in those definitions alone should make clear some of the problems contained within the bill itself.

The Problems with the ACDC Act

The most significant problem with the ACDC Act and the most immediately obvious is the broad, bordering on useless, definition of Attacker and Defenders. Let's assume that the ACDC Act has become law and that a company, D, believes with near certainty that Company D has installed a back door into their system, and has been stealing confidential information. Whether Company D is guilty or not doesn't matter, per the bill, the defender need only be "qualified" and have, "a high degree of confidence in attribution."[3] Company D now has to notify the FBI of their intention to utilize ACDMs, informing them of the type of breach, the intended target, and how Company D intends to preserve evidence of Company D's cyber crimes, and prevent damage to intermediate computers. Company D cannot legally proceed without the FBI's approval. While this is an excellent way to ensure some oversight, it also negatively affects the stated goal of the bill; this bill was prompted in part by the inability for law enforcement to, "respond to and prosecute cybercrime in a timely manner"[3] further, by requiring companies to wait for approval, they lose the ability to react in the moment to an attack, and by the time the FBI can respond, any sensitive information that was obtained in the breach has likely been copied. However, let's assume, that Company D received peremptory review of their ACDMs, which negates the issues above, but also removes all oversight that the notification requirement entailed. In response, Company D, clearly the defender, intrudes into Company A's system and begins monitoring Company A "to assist in developing future intrusion prevention or cyber defense techniques." Company A now detects an unauthorized persistent intrusion into their networks" and under this bill, now qualifies an a defender, and having also received peremptory review, retaliates against Company D. Each company, believing themselves to be under attack, continues to escalate; lawfully destroying data they believe to be theirs, monitoring the others' activity, and taking action to disrupt any continued unauthorized access. Both companies continue to be civilly liable, but both have valid defenses against prosecution, even if, it is later discovered that it was, in fact, not Company A that originally intruded on A's network. This example hopefully illustrates specific issues with the way this bill would define the attacker and defender, issues with the broad action and lack of oversight that is legally permitted, and the problem with having little to no standard of evidence for attribution. Further, this example didn't include additional issues with the

difficulty of the original attribution, the likely collateral damage to intermediary systems, an excusable casualty so long as it wasn't an intentional result, and the potential economic and business effects this escalating cyber battle would have on both companies. Many of these issues lie in the way the bill chooses to define attackers and defenders, the potential for lack of oversight, the low bar for attribution, and the broadly defined actions that constitute Active Cyber Defenses; however, the core issue is not in the language of the bill, poor as it may be, but all of these problems are perennially raised whenever hacking back is proposed, because they are more specific takes on the issues found in any legalization of hacking back.

The Problem with a Hack-Back Doctrine

A common comparison made by proponents of hacking back is that of self-defense in the home[4] which is at best a gross simplification; if your home is robbed, and the police are unable to get there in time that does not give you permission to chase down the thief and steal back your TV. Nor are you allowed to follow the thief to their hideout and spy on them to "assist in developing future intrusion prevention" because as a society we have decided to designate specific people to do those things, and to collectively call those people law enforcement. The problem with hacking back is, as was seen more specifically in the bill, when Company A hacks Company D, and Company D hacks back, the line between defender and attacker becomes blurred, because this isn't a case of defensive action, its a case of following the thief and engaging them in a fight after they've absconded with your property.

The blurred lines of aggressor and defender, aside, legalized hacking back is not a feasible cyber defense doctrine in an interconnected world. Then FBI director James Comey spoke out against the bill when it was first proposed, opposing it not on particulars, but that hacking back would make law enforcement's job harder, warning that, "It runs a risk of tremendous confusion in a crowded space"[5]. Buried within any liberalization of restrictions is the potential for those lacking in scruples to take advantage of the openness. Buried within the legalization of hacking back is the potential for companies to exploit the lack of a hard line on hacking and take malicious action on their competitors under the pretense of "defense." Obviously, false flag operations are not being legalized by the ACDC Act, nor is anyone advocating them to be, but with the law as it is right now, regardless of whatever actions Company A is accused of taking against Company D, if Company A can demonstrate that D hacked them, Company D has violated the law. However, under the ACDC Act, COmpany A can provide a defense to hacking Company A if they have a "high degree of confidence" in the attribution, even if they're wrong, which moves the legal bar for Company A to demonstrate that Company D broke the law beyond just showing an intrusion into A's systems, but they must also prove that D did not, and could not, have had a high degree in the confidence of the attribution. This new legal standard would allow companies to justify "defensive" action against competitors while having a much easier time defending false flag operations and other illegal, but more easily defensible actions. Beyond making the job of law enforcement harder, and the possibility of escalation between companies as was outlined above, and the capability of companies to take advantage of the liberalization of hacking laws to get ahead, the most potentially catastrophic consequence of legalizing hacking back is the involvement of international actors in cyber-attacks on U.S. companies, and, less intentional, but with equal potential for catastrophe, the potential for international networks to serve as intermediate computers for an attack. The ACDC Act does discourage taking action against action with international consequence, finding that, "Computer defenders should also exercise extreme caution to avoid violating the law of any other nation where an attacker's computer may reside."[3], however it is not explicitly made illegal, and the frequency with which major

attacks on U.S. companies come from abroad; particularly considering this bill came in the wake of attacks such as WannaCry, attributed to North Korea; NotPetya, seemingly originating in Ukraine; and the Equifax leak, which remains unattributed as of May 2018; cast doubts on whether urging extreme caution will have any substantial impact on international action.. That being said, the potential repercussions to responding far outweigh any potential benefits. Even ignoring cases where an attacker is based in another country, either as a state or non-state actor, the internet, by virtue of design, is a globe spanning system, and the vast majority of attacks, and nearly all attacks worth being worried about, will not come directly from an attacker's network, but be routed through either willing, as in the case of TOR nodes. or unwilling, as in the case of botnets and other compromised systems. These intermediaries could be located in any number of countries, and trying to follow an attacker through an intermediary located in a different country could violate the laws of that country, with all the criminal liability that entails, or, if that intermediary is a state operated system, could result in a major incident and accusations of espionage. The more serious possibility is that the origin of the attack is a state actor, as was the case in the 2014 Sony hack and 2017's WannaCry both attributed to North Korea and the 2018 Winter Olympics attack, 2017's NotPetya, a 2016 hacking of voter registration, 2016's DNC hack, and 2014's Yahoo hack all attributed to Russian actors. Keith Alexander, former director of the NSA, warned, "[...] you can't have companies starting a war. That's an inherently governmental responsibility, and plus the chances of a company getting it wrong are fairly high"[6] when asked about hacking back against state actors. Despite the widespread and often high profile opposition to the practice, there are those in both the private sector and the public sector who believe that hacking back is an appropriate, effective cyber doctrine.

In Support of Hacking Back

Among the most vocal of the supporters of legalizing hacking back is former counsel to the NSA Stewart Baker, who argued, "Hacking is a crime problem and a war problem. You solve those problems by finding hackers and punishing them. When they feel their profession isn't safe, they'll do it less."[7] while Tom Graves, author of the bill, invites the criticism that this bill will only turn the internet into the Wild West with the retort, that he's just "asking for a neighborhood watch—an extra set of eyes and ears, to notify law enforcement so they can do their job a little bit quicker."[7]. The primary problem with both Graves' and Baker's arguments is that the problems in this bill, and the problems with a doctrinal defense of hacking back are not the parts about enabling greater attribution, but that by allowing retaliation, it goes beyond "finding hackers and punishing them", or establishing a "neighborhood watch [to be] an extra set of eyes and ears"[7] and veers into vigilantism. A neighborhood watch doesn't have the power to stop a robbery by assaulting the thief, and allowing private citizens to find and punish criminals is the textbook definition of vigilantism. Among those in favor of changing the law, but recognizing the threat hacking back poses are a pair of researchers at the Carnegie Endowment for International Peace, who, in a June, 2017 report, likened the internet to the Gulf of Aden, and argued that passage was only made safe from Somali pirates after vessels started hiring armed private security. However, in the report they advocate for a "spectrum of ACD measures" which excludes hacking back, instead advocating for the use of "digital dye-packs [and] digital beacons"[8], both of which would aid in attribution, while severely limiting defenders' abilities to take destructive action outside their own network.

What Comes Next?

The solution to the growing threat from both state actors and on-state actors is not empowering companies to get into escalating gun fights against opponents they know little to nothing about before confronting them, but neither is is to sit on our hands acting like the state of cybersecurity is fine and

dandy. To return to the analogy of a thief stealing TVs; if there is an increase in the number of break-ins in a neighborhood, the solution isn't to legalize chasing down the thief, but to hire more police to patrol the area, and to advise people to install better security. Neither of those solutions becomes less true in the realm of cybersecurity. In the united states, its estimated that there are more than one million unfilled cybersecurity positions, in both the private and public sector[9], law enforcement agencies don't have the staff, "to respond to and prosecute cybercrime in a timely manner"[3]. It's not just on the FBI however, for the seemly huge number of leaks and hacks reported every year; many firms continue to use out of date, and unpatched software which leaves them vulnerable to known exploits, as is suspected to have happened in the Equifax Breach[10]. Even if neither of these were issues, the flaws in hacking back remain. One of the hardest problems in cybersecurity is that of attribution, a fact that doesn't change when considering how to retaliate to an attack. If it seems like a bad idea to track down a thief, go to their hideout, and try to confront them, without knowing who else is in there, what weapons they have, or even if you have the right address, then why does it seem any less stupid when it's easier to hide your tracks, you may have to break into innocent people's houses to keep following them, and unlike in real life, where it's unlikely that confronting the thief would cause international hostilities, in this case you may very well follow them all the way back to the Kremlin or Pyongyang.

References

[1]*Active Cyber Defense Certainty Act*, vol. 4. https://www.congress.gov/bill/115th-congress/house-bill/4036/text: House of Representatives, 2017.

[2]J. Wolff, "Oh Good, the Worst Idea in Cybersecurity Is Back Again", *Slate Magazine*, 2017. [Online]. Available: http://www.slate.com/articles/technology/future_tense/2017/10/hacking_back_the_worst_idea_in_cybersecurity_rises_again.html. [Accessed: 05- May- 2018].

[3]*Active Cyber Defense Certainty Act*, vol. 2. https://www.congress.gov/bill/115th-congress/house-bill/4036/text: House of Represetnatives, 2017.

[4]J. Wolff, "When Companies Get Hacked, Should They Be Allowed to Hack Back?", *The Atlantic*, 2017. [Online]. Available: https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/. [Accessed: 05- May- 2018].

[5]J. Cox, "FBI Director Tells Companies Not to 'Hack Back' Against Hackers", *Motherboard*, 2017. [Online]. Available: https://motherboard.vice.com/en_us/article/kbyznn/fbi-director-tells-companies-not-to-hack-back-against-hackers. [Accessed: 05- May- 2018].

[6]L. Franceschi-Bicchierai, "Ex-NSA Director Says Companies Should Never Hack Back Because They Could Start Wars", *Motherboard*, 2017. [Online]. Available: https://motherboard.vice.com/en_us/article/a37njb/keith-alexander-nsa-hack-back. [Accessed: 05- May- 2018].

[7]N. Schmidle, "The Digital Vigilantes Who Hack Back | The New Yorker", *Newyorker.com*, 2018. [Online]. Available: https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back. [Accessed: 05- May- 2018].

[8]A. Wyatt Hoffman, "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?", *Carnegie Endowment for International Peace*, 2017. [Online]. Available: http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236. [Accessed: 05- May- 2018].

[9]H. Sheth, "I favor strong cyber defense, but 'hack back' idea is cyber suicide", *TheHill*, 2017. [Online]. Available: http://thehill.com/blogs/congress-blog/technology/336053-i-favor-strong-cyber-defense-but-hack-back-idea-is-cyber. [Accessed: 05- May- 2018].

[10]E. Weise, "How did the Equifax breach happen? Here are some answers and some questions.", *USA TODAY*, 2017. [Online]. Available: https://www.usatoday.com/story/tech/2017/09/12/how-did-equifax-breach-happen-here-some-answers-and-some-questions/658343001/. [Accessed: 05- May- 2018].

Further Reading:

- https://www.law.cornell.edu/uscode/text/18/1030 **(Cornell law library reference for the law that would be modified by the ACDC Act)**
- https://www.csoonline.com/article/3228118/hacking/the-hack-back-is-not-a-defense-strategy.html
- https://www.technologyreview.com/s/609555/hacking-back-makes-a-comeback-but-its-still-a-really-bad-idea/
- https://lawfareblog.com/new-hack-back-legislation-makes-improvements-and-raises-new-questions

Link to power point presentation in google slides:
https://drive.google.com/open?id=1K2lPuGRwzS7BBzVrZGvUEUFFfYuE2WDdZUik5Yf5-2k