Harvard Journal of Law & Technology
Volume 28, Number 1 Fall 2014

MICROSOFT THE BOTNET HUNTER: THE ROLE OF PUBLIC-PRIVATE PARTNERSHIPS IN MITIGATING BOTNETS

*Zach Lerner**

TABLE OF CONTENTS

I. RECOGNIZING THE GROWING BOTNET THREAT AND INDUSTRY

A. Defining Botnet

A botnet is a network of computers coordinated by a single control mechanism, often programmed to complete a set of repetitive tasks.[1] This same distributed computing technique can be used voluntarily and cooperatively to effectively perform a function. When referred to as a botnet, though, this technique signifies a network of

* J.D., Harvard Law School, 2015. Many thanks to Urs Gasser, Greg Nojeim, Taufiq Ramji, and all of the JOLT editors for their support and work in developing and publishing this Note.

[1] *See* T. Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 528 (2010).

zombies — compromised computers, used without the owner's knowledge or permission.[2] Botnet operators — "masters" — often employ botnets to send unsolicited e-mail or spam,[3] create false web traffic for commercial gain through click fraud,[4] or install malware.[5] Masters have used botnets to replace ads with fake infection warnings and manipulate links to redirect users to malicious websites,[6] causing users to download malicious software[7] that can even observe a user's cards in online poker.[8] In fact, a single botnet has the ability to perform all of these functions at once.[9] The most common usage of botnets though is for Distributed Denial of Service ("DDoS") attacks.[10] DDoS attacks seek to make a target website unavailable by overwhelming it with traffic.[11] There are three different types of DDoS attacks — application layer, protocol, and volume-based — but each has the same goal: interrupting or suspending a given website's services from use by legitimate users.[12] Masters have levied botnet-operated DDoS attacks against financial institutions,[13] WordPress,[14] the Church of Scientology,[15] and many others.[16]

[2] *See id.* at 528–29.

[3] *See* Shaun Waterman, *Microsoft XP's Massive Cybersecurity Problem*, POLITICO (Apr. 7, 2014, 8:00 PM EDT), http://www.politico.com/story/2014/04/microsoft-xp-cybersecurity-problem-105451.html?hp=f2.

[4] *See* Tim Bradshaw & Emily Steel, *Hacked PCs Falsify Billions of Ad Clicks*, THE GLOBE AND MAIL, http://www.theglobeandmail.com/report-on-business/international-business/hacked-pcs-falsify-billions-of-ad-clicks/article9958989/ (last updated Mar. 19, 2013, 3:59 PM EDT).

[5] *How Botnets Are Used*, MICROSOFT SEC. INTELLIGENCE REPORT, http://www.microsoft.com/security/sir/story/default.aspx#!botnetsection_installing.

[6] *See, e.g.*, Alexei Kadiev, *End of the Line for the Bredolab Botnet?*, SECURELIST (Dec. 20, 2010, 12:38 PM), https://www.securelist.com/en/analysis/204792152/End_of_the_Line_for_the_Bredolab_Botnet.

[7] *See, e.g.*, Erik Larkin, *Fake Infection Warnings Can Be Real Trouble*, PCWORLD (Feb. 10, 2009, 2:15 PM), http://www.pcworld.com/article/159316/fake_warnings.html.

[8] *See Korean Poker Hackers Arrested*, GAMING SUPERMARKET (July 8, 2010), http://poker.gamingsupermarket.com/news/4660/korean-poker-hackers-arrested.

[9] *See* Yury Namestnikov, *The Economics of Botnets*, SECURELIST (July 22, 2009, 8:52 AM), http://securelist.com/large-slider/36257/the-economics-of-botnets/.

[10] *Botnet DDoS Attacks*, INCAPSULA, http://www.incapsula.com/ddos/ddos-attacks/botnet-ddos.html (last visited Dec. 18, 2014).

[11] *See id.*

[12] *Id.*

[13] *See* Lucian Constantin, *Botnets for Hire Likely Attacked U.S. Banks*, COMPUTERWORLD (Jan. 9, 2013, 3:51 PM PT), http://www.computerworld.com/s/article/9235525/Botnets_for_hire_likely_attacked_U.S._banks.

[14] Dan Goodin, *Huge Attack on WordPress Sites Could Spawn Never-Before-Seen Super Botnet*, ARS TECHNICA (Apr. 12, 2013, 9:10 PM EDT), http://arstechnica.com/security/2013/04/huge-attack-on-wordpress-sites-could-spawn-never-before-seen-super-botnet/.

[15] *See* John Leyden, *US Teen Pleads Guilty over Scientology DDoS Attacks*, THE REGISTER (May 12, 2009, 12:06 PM), http://www.theregister.co.uk/2009/05/12/scientology_ddos_attack_plea/.

[16] Yury Namestnikov, *DDoS Attacks in Q2 2011*, SECURELIST (Aug. 29, 2011, 11:36 AM), https://www.securelist.com/en/analysis/204792189/DDoS_attacks_in_Q2_2011 (citing a 2011 statistical analysis revealing that DDoS attacks were aimed at relatively limited group of sites: 25% at online shopping sites, 20% at gaming sites, 13% at stock exchanges,

Implementing botnets gives the master two main advantages. First, he or she is hard to trace because the actual attacks are launched by the zombies, which are distributed both on the network and geographically.[17] This separation of attacker from attacking devices makes it especially hard to determine the master's location or shut down his or her command-and-control server. Second, the distributed network of zombies permits the master to instigate large scale attacks.[18] Botnets made up of thousands of computers allow the master to send a vast number of emails, collect massive amounts of information, or prevent access to a website quickly and efficiently.

B. The Growing Problem

What began as a niche mechanism used by sophisticated programmers has now developed into a blossoming economic marketplace. At a recent discussion hosted by the Berkman Center for Internet & Society, Dr. Nimrod Kozlovski described this emergence as a paradigm shift in security.[19] He argued that current cyberattacks are different than what experts anticipate and plan for; they are not random hacks by disenfranchised elite hackers, but strategic efforts by governments and an organized marketplace.[20] A recently published study estimates that cyber criminals are outspending the global information security market two-to-one.[21] In addition to the increased funding, botnet masters also benefit from being more agile than those trying to impede their work. Instead of jumping through corporate hoops or wading through convoluted bureaucracy, masters are free to operate without restrictions. A 2014 DDoS Threat Landscape Report indicates that over a ninety-day period, the occurrence of botnet-operated DDoS attacks increased by 240% compared to the same pe-

11% at banks, and the rest at adult content sites, blogs, mass media, and transportation sites).

[17] Guzman, *supra* note 1, at 529.

[18] *Id.*

[19] Nimrod Kozlovski, Prof. for Cyber Studies, Tel Aviv University and Partner, Jerusalem Venture Partners Cyber Labs, Address at The Emerging Cyber Security Paradigm: How New Innovations Meet Unknown Cyber Needs (Mar. 3, 2014); *The Emerging Cyber Security Paradigm: How New Innovations Meet Unknown Cyber Needs*, BERKMAN CTR. FOR INTERNET & SOC'Y, http://cyber.law.harvard.edu/events/2014/03/cybersecurity (last updated Mar. 3, 2014) (describing the event and participants).

[20] *Id.*

[21] Stilgherrian, *Cyber Criminals Are Out-Spending the Defenders Two to One: HP*, ZDNET (Apr. 4, 2014, 4:45 AM GMT), http://www.zdnet.com/cyber-criminals-are-out-spending-the-defenders-two-to-one-hp-7000028056/ (stating that criminals spend roughly $104 billion per year as compared to the defenders' $48 billion).

riod the previous year.[22] This equals over twelve million unique botnet-led DDoS attacks per week.[23]

Furthermore, these advantages have engendered more sophisticated botnets. Recent botnets are showing "familiarity with current DDoS protection methods and the ways in which these methods can be bypassed and overcome."[24] A number of DDoS botnets are spoofing their identities by pretending to be benign bots that are standard in Baidu, Internet Explorer, or Google software.[25] Thus, the newest generation of botnets is composed of more complex agents, often "immune to generic filtering methods . . . ."[26] This combination of increased funding, greater attack volume, and improved techniques is magnified by a developing botnet industry.

The rise of sophisticated botnets has generated profits for both developers and masters. For this reason, while botnets have occasionally been used by the National Security Agency[27] or as a form of protest — most notably by hacktivist groups Anonymous and LulzSec[28] — they are most often exploited for commercial gain. This potential use has generated a rapidly growing and profitable industry composed of actors that build botnets and individuals that use the botnets for subversive purposes.[29] Pointing specifically to the ability for botnets to collect personal data, one security executive states, "It's a huge ecosystem out there, and an economy that's underground and available for hackers."[30] He compares this market to eBay, an environment where the information is readily bought and sold.[31] Groups of criminal hackers can resemble mini-multinationals, paying salaries to staff and hiring marketing directors to advertise their abilities.[32] The capacity to profit has, in turn, generated high demand for the products that can facilitate such illicit schemes: the botnets them-

[22] 2013–2014 DDOS THREAT LANDSCAPE REPORT, INCAPSULA (2014) *available at* http://www.incapsula.com/images/blog/images/2013-14_ddos_threat_landscape.pdf.

[23] *Id.*

[24] *Id.* (revealing that these sophisticated botnets are now able to bypass JavaScript and Cookie challenges, which serve as the most common forms of botnet filtering).

[25] *Id.* at 10–11.

[26] David Braue, *DDoS Botnets Already Smarter, Fiercer in 2014: Imperva Incapsula*, CSO (Apr. 9, 2014, 5:03 PM), http://www.cso.com.au/article/542497/ddos_botnets_already_smarter_fiercer_2014_imperva_incapsula/.

[27] Kevin Poulsen, *NSA Has Been Hijacking the Botnets of Other Hackers*, WIRED (Mar. 12, 2014, 3:45 PM), http://www.wired.com/2014/03/nsa-botnet/.

[28] *See Hackers Inc*, THE ECONOMIST (SPECIAL REPORT: CYBER-SECURITY) (July 12, 2014), *available at* http://media.economist.com/sites/default/files/sponsorships/jl11_checkpoint/20140712_cybersecurity.pdf; *see, e.g.*, Leyden, *supra* note 15.

[29] While these two roles can be filled by the same individual, they can also be performed separately.

[30] Stilgherrian, *supra* note 21 (citing Media Briefing Interview with Arthur Wong, Senior Vice President and General Manager, HP and HP Enterprise Security Services (ESS), in Sydney, Austl. (Apr. 2, 2014).

[31] *Id.*

[32] *See Hackers Inc*, *supra* note 28.

selves. Thus, the same type of marketplace exists for those producing the botnets.

"DDoS for hire" or "rent a botnet" services are commonplace. Masters offer a menu of services that allow for either purchase or rental.[33] The marketplace is replete with advertisements offering botnets for anywhere between $5 and $1000 depending on the number of infected users, their geographical location, and the botnet's ability to evade detection.[34] Some sites allow for use of the botnets by the hour, week, or month, and one even offers a fifteen-minute trial to prove the botnet's efficacy.[35] In addition to marketing wholesale botnets — available at the click of a button — vendors are beginning to engage in more specialized functions. These criminal enterprises are providing tailored and customized services for clients, focusing on individualized encryption to bypass specific security mechanisms at each link in a defense chain.[36]

Producing a botnet that can collect private information is not the only path to economic profit. A botnet capable of DDoS attacks can be exploited as a mechanism of unfair competition or cyberterrorism.[37] For example, a botnet creator can sell its services to an entrepreneur who would benefit from his or her competitor's website becoming inoperable for a short amount of time. In 2011, the owner of ChronoPay, a payment service provider, was charged with organizing a DDoS attack against a competitor in an attempt to secure a lucrative contract for which the two companies were competing.[38] Similarly, a master can use a botnet as a means of extortion, often successfully coercing a fee that is far smaller than the potential economic consequences of a persistent attack. In 2013, two men were convicted and sentenced to five years in prison for using DDoS attacks to extort money from a British online casino.[39] In April 2014, the New York Times reported that the founders of Meetup, Vimeo,

[33] *See* Stilgherrian, *supra* note 21.

[34] *See* Vitaly Kamluk, *The Botnet Business*, SECURELIST (May 13, 2008), https://www.securelist.com/en/analysis/204792003/The_botnet_business?print_mode=1.

[35] *See* Dancho Danchev, *DDoS for Hire Services Offering To 'Take Down Your Competitor's Web Sites' Going Mainstream*, WEBROOT THREAT BLOG (June 6, 2012), http://www.webroot.com/blog/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-sites-going-mainstream/.

[36] *See* Stilgherrian, *supra* note 21.

[37] *See* Namestnikov, *supra* note 9.

[38] Namestnikov, *supra* note 16.

[39] *See* Nick Martin, *Hackers Jailed for Casino Blackmail Attack*, SKY NEWS (Dec. 18, 2013, 6:03 PM), http://news.sky.com/story/1184310/hackers-jailed-for-casino-blackmail-attack; *cf.* Press Release, Sophos, Online Russian Blackmail Gang Jailed for Extorting $4m from Gambling Websites, (Oct. 5, 2006), http://www.sophos.com/en-us/press-office/press-releases/2006/10/extort-ddos-blackmail.aspx (citing that in 2006, members of a Russian gang were arrested for similar efforts, which allegedly led to a profit of over $4 million).

Basecamp, Bit.ly, Shutterstock, and MailChimp all faced similar ransom-based extortion attempts.[40]

The botnet economy is just beginning to mature and has immense opportunity for growth. HP Enterprise Services predicts that "by 2020 there will be another million people working in cybercrime globally."[41] This is not surprising because the cybercrime market encompasses all five indicators of a mature market — accessibility, sophistication, reliability, specialization, and resilience.[42] As a function of the direct links between vendors and buyers, low startup costs, and potential for worldwide distribution, cybercrime is exceedingly accessible.[43] Building a botnet can take less than fifteen minutes[44] and, in order to control one million users, can cost around $150.[45] The market is already showing signs of sophistication and reliability: incorporating usage terms, functionality tracking, and product guarantees.[46] As discussed above, there are already botnet builders offering customization and specialization.[47] Finally, the market is resilient because defensive efforts, such as encryption, simply cause temporary "hiccups" in the market's strength.[48] As such, the rampant surge in botnets is unlikely to decline.

According to the Center for Strategic and International Studies, malicious cyber activity costs the economy somewhere between $300 billion and $1 trillion per year globally and between $24 billion and $120 billion per year in the United States alone.[49] Thus, given the massive costs to both individuals and society as a whole, paired with the apparent avenue for continued growth in the market, steps must be taken to combat botnets.

[40] Nicole Perlroth & Jenna Wortham, *Tech Start-Ups Are Targets of Ransom Cyberattacks*, N.Y. TIMES BLOGS: BITS (Apr. 3, 2014, 4:00 PM), http://bits.blogs.nytimes.com/2014/04/03/tech-start-ups-are-targets-of-ransom-cyberattacks/.

[41] Stilgherrian, *supra* note 21.

[42] *See* Chris Duckett, *Security Black Market as Mature as Any Other Free Market: Juniper*, ZDNET (Mar. 25, 2014, 4:00 AM GMT), http://www.zdnet.com/security-black-market-as-mature-as-any-other-free-market-juniper-7000027660/.

[43] *See id.*

[44] *See* Simon Mullis, *Cybercriminal Intent: How To Build Your Own Botnet in Less than 15 Minutes*, FIREEYE (Aug. 2, 2013, 9:25:08 AM EDT), http://www.fireeye.com/blog/corporate/2013/08/cybercriminal-intent-how-to-build-your-own-botnet-in-less-than-15-minutes.html.

[45] *See* Tim Greene, *Black Hat: How To Create a Massive DDoS Botnet Using Cheap Online Ads*, NETWORK WORLD (Aug. 1, 2013, 3:13 PM PT), http://www.networkworld.com/news/2013/080113-black-hat-ddos-botnets-272447.html.

[46] *See* Duckett, *supra* note 42.

[47] *See* Stilgherrian, *supra* note 21.

[48] *See* Duckett, *supra* note 42.

[49] CTR. FOR STRATEGIC AND INT'L STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 5 (July 2013), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

II. IDENTIFYING THE CURRENT METHODS OF BOTNET ENFORCEMENT

A. Mitigating a Botnet

In response to threats, both the judicial system and military rely on deterrence. Deterrence depends on two elements: punishment and denial.[50] Respectively, these components seek to impose costs that outweigh the adversary's potential gains and negate the opposition's success in order to disincentivize undertaking the action. Prior to 2013, four primary methods were used to prevent, impede, and mitigate DDoS attacks: commercial security software, criminal enforcement, botnet seizure by federal agencies, and private civil action.

Privatized efforts to engender DDoS denial are rooted in creating sophisticated defenses to prevent DDoS attacks before they even happen. This tactic is visible in both infrastructure security and cloud-based application delivery platforms. For example, a leading cloud-based service provider, CloudFlare, offers advanced DDoS protection that "matches the sophistication and scale of [DDoS] threats, and can be used to mitigate DDoS attacks of all forms and sizes . . . ."[51] CloudFlare's sales increased 450% last year,[52] which may be the result of the growing number of DDoS attacks. Akamai, which delivers at least 15% of all web traffic,[53] recently purchased a company that specializes in DDoS protection for $370 million.[54] While these corporate efforts are valuable, they are intrinsically passive and limited by their focus on prevention. Creating stronger walls may keep the enemy out, but it will not eliminate the opponent entirely.

Embracing the goal of deterrence through punishment, the Computer Fraud and Abuse Act ("CFAA") criminalizes the intentional damaging of networked computers.[55] It has been interpreted broadly

[50] COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RES. COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 40 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009), *available at* http://www.nap.edu/catalog/12651/technology-policy-law-and-ethics-regarding-us-acquisition-and-use-of-cyberattack-capabilities.

[51] *CloudFlare Advanced DDoS Protection*, CLOUDFLARE, http://www.cloudflare.com/ddos (last visited Dec. 18, 2014). A competitor, Incapsula, prides itself on its DDoS defense and promises to "[s]ecure your website against all types of DDoS attacks" and "mitigate the largest and smartest DDoS attacks." *Enterprise Plans Datasheet*, INCAPSULA (2014), http://www.incapsula.com/datasheets/enterprise-plans.pdf.

[52] DH Kass, *DDos Security Providers Countering Cyber Attacks on Internet Startups*, THE VAR GUY, (Apr. 7, 2014), http://thevarguy.com/network-security-and-data-protection-software-solutions/040714/ddos-security-providers-countering-cyber-att.

[53] Erik Nygren, Ramesh K. Sitaraman & Jennifer Sun, *The Akamai Network: A Platform for High-Performance Internet Applications*, ACM SIGOPS OPERATING SYS. REV. (Jul 2010), http://www.akamai.com/dl/technical_publications/network_overview_osr.pdf.

[54] Kass, *supra* note 52.

[55] *See* 18 U.S.C. § 1030 (2012).

to prohibit acts such as obstructing voicemail[56] and disseminating computer worms.[57] Violations of the CFAA can warrant either misdemeanor or felony charges depending on the nature of the attack.[58] Felony punishments range from five years to life in prison.[59] However, despite the Act's wide-ranging scope and harsh penalties, CFAA enforcement requires precise knowledge of the defendant's identity, which is often impossible to obtain in DDoS attacks. While the CFAA was successfully used to convict an Arizona resident for selling access to botnets,[60] CFAA prosecution of DDoS masters in foreign countries is impeded by a number of jurisdictional obstacles.[61] Thus, the deterrent effect of the CFAA may be driving botnet masters and developers to operate in foreign countries.

Due to the limitations on criminal prosecution, law enforcement agencies have occasionally altered their focus from punishment to denial: seizing and disabling a botnet rather than prosecuting the master. In 2011, the Federal Bureau of Investigation ("FBI") and the Justice Department ("DOJ") worked in tandem to hijack and eliminate the Coreflood Botnet.[62] The government initiated and won a civil suit in federal court, seeking a temporary restraining order allowing it to replace servers, collect IP addresses, and deliver a disabling command.[63] While some questioned how these actions did not implicate the Fourth Amendment,[64] the court accepted the government's argument that under the "community caretaking" doctrine, a warrant was not required because the disabling command was divorced from detection, investigation, or acquisition of evidence.[65] A similar technique was used less than a year later, but the government did not

[56] *See, e.g.*, Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 301 (6th Cir. 2011).

[57] *See, e.g.*, United States v. Morris, 928 F.2d 504, 510–11 (2d Cir. 1991).

[58] *See* 18 U.S.C. § 1030(c) (2012).

[59] *See id.*

[60] Press Release, U.S. Dep't of Justice, *Arizona Man Sentenced to 30 Months in Prison for Selling Access to Botnets* (Sept. 6, 2012), http://www.justice.gov/opa/pr/arizona-man-sentenced-30-months-prison-selling-access-botnets.

[61] *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 467 (2012).

[62] Kim Zetter, *With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal*, WIRED, http://www.wired.com/2011/04/coreflood/ (last updated Apr. 13, 2011, 7:30 PM).

[63] *Id.*

[64] *See, e.g.*, Ms. Smith, *4th Amendment vs Virtual Force by Feds, Trojan Horse Warrants for Remote Searches?*, NETWORK WORLD (Nov. 9, 2009, 7:57 AM PT), http://www.networkworld.com/article/2221068/microsoft-subnet/4th-amendment-vs-virtual-force-by-feds--trojan-horse-warrants-for-remote-searches-.html.

[65] Complaint at 52, United States v. John Doe, No. 3:11-CV-00561-VLB (D. Conn 2011) *available at* http://www.scribd.com/doc/52965914/Coreflood-Memo. The memo compares the detection of an electronic signal establishing a "break in" of a computer to an "anonymous tip" about a home break in. The complaint analogizes to a cop, who in response to an anonymous tip, comes across an open physical door. In the physical world, the policeman can shut it, so, the argument goes, the government can shut the electronic door as well.

remotely clean the zombies. Instead the FBI posted electronic instructions detailing how individuals could determine if their device was infected and instructed them to "consult a computer professional."[66] While the FBI and DOJ relied on corporate assistance in executing these operations,[67] the judicial actions and mitigation techniques were entirely implemented by the government.

Private citizens and corporations can also seek remediation and punishment independent of the criminal justice system. Although botnet-related crime is a recent phenomenon, many civil legal doctrines charged with thwarting its use are antiquated. The primary cause of action for disruptive network behavior is trespass to chattels. A victim can assert a trespass to chattels claim against a master by alleging intent, interference with a chattel, and actual harm.[68] Businesses have successfully used this tort theory against spammers[69] and to combat repeated scripted access.[70] Additionally, section 1030(g) of the CFAA creates a civil cause of action allowing for compensatory damages or equitable relief.[71] However, as in criminal prosecution, the technological and jurisdictional complications associated with locating and holding masters liable for DDoS attacks hamper the effectiveness of these judicial remedies. Additionally, the value of a civil claim is limited by a master's financial resources, as defendants may be judgment-proof.[72] A civil claim is still useful to large corporations. Uninterested in collecting money or punishing masters, large corporations occasionally used civil remedies to seize and mitigate botnet attacks.[73]

Although not currently sanctioned in the United States, creative alternatives propose shifting liability from the master to intermediary parties. Scholars argue that governments could impose liability on the infected users themselves, the manufacturers of software or hardware,

[66] Gregg Keizer, *Feds Lead Biggest Botnet Takedown Ever, End Massive Clickjack Fraud*, COMPUTERWORLD (Nov. 10, 2011, 6:39 AM PT), http://www.computerworld.com/article/2498686/security0/feds-lead-biggest-botnet-takedown-ever--end-massive-clickjack-fraud.html.

[67] *See, e.g.*, Nick Kolakowsi, *Facebook Assists FBI in Botnet Takedown*, DICE (Dec. 12, 2012), http://news.dice.com/2012/12/12/facebook-assists-fbi-in-botnet-takedown/ (describing how Facebook's security team helped identify the root cause, the perpetrators, and those affected by the Butterfly Botnet).

[68] *See* Restatement (Second) of Torts § 217 cmt. e (1965).

[69] *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017 (S.D. Ohio 1997).

[70] *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071–72 (N.D. Cal. 2000).

[71] *See* 18 U.S.C. § 1030(g) (2012).

[72] *See* Kesan & Hayes, *supra* note 61, at 470.

[73] *See, e.g.*, Tim Cranton, *Cracking Down on Botnets*, MICROSOFT ON THE ISSUES (Feb. 24, 2010), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/02/24/cracking-down-on-botnets.aspx (describing Operation b49 and how Microsoft used a civil complaint in the U.S. District Court of Eastern Virginia to mitigate the Waledac botnet).

or even the Internet service provider.[74] Imposing liability on the latter two would likely cause the affected companies to pass the costs onto consumers, but the former could force zombies to internalize the costs of their actions. Under one such theory, the victim of a DDoS attack could assert a negligence claim against the infected user, averring that the "zombie's failure to secure his computer was the proximate cause of the injuries suffered by the DDoS victim."[75] However, this may not comport with the common law doctrine of intervening and superseding causes, which prevents negligent defendants from being held liable when the harm is caused by a third party's intentional tort.[76]

Another creative alternative is to authorize DDoS victims to strike back against the zombies. This endorsement of self-defense could be accomplished through the recognition of legal privileges[77] or the enactment of a regulatory right to retaliate.[78] Both methods attempt to impose a duty on computer owners, which would generate an incentive to properly secure their computers and networks. However, critics argue this would effectively function as "a tax on ignorance and technophobia," punishing users who are unable to achieve adequate security.[79] Furthermore, retaliatory attacks would likely violate the CFAA and other international cybercrime statutes.[80] Finally, by their very nature, these judicially enforced remedies can only react to past and ongoing attacks and therefore cannot thwart an attack before it happens. Recognizing the inherent flaws in each of these enforcement methods, a public-private partnership was formed in June 2013 to combine criminal enforcement, seizure, and private civil action into one collective effort.

B. The Citadel Botnet

The takedown of the Citadel botnet ("Citadel") demonstrates the potential role for public-private partnerships in locating and mitigating botnets. One of the largest botnets ever documented, Citadel, installed key-logging software onto zombie computers, giving the master the ability to track everything that the infected user typed.[81] Predictions estimate that Citadel logged the keystrokes of over five million users in ninety different countries, leading to more than $500

[74] *See* Kesan & Hayes, *supra* note 61, at 469–70.

[75] Guzman, *supra* note 1, at 548.

[76] Kesan & Hayes, *supra* note 61, at 470–71.

[77] *See* Guzman, *supra* note 1, at 528.

[78] *See* Kesan & Hayes, *supra* note 61, at 475–76.

[79] Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How To Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 47 (2006).

[80] Kesan & Hayes, *supra* note 61, at 444.

[81] Chloe Albanesius, *Microsoft, FBI Take Down 'Citadel' Botnet Targeting Bank Info*, PC MAGAZINE (June 6, 2013, 9:55 AM EST), http://www.pcmag.com/article2/0,2817,2420046,00.asp.

million in losses.[82] An extensive investigation led by Microsoft's Digital Crimes Unit, the FBI, and companies from the financial services and technology sectors began in early 2012 and culminated in the summer of 2013 when Microsoft successfully filed suit against the cybercriminals operating Citadel.[83]

Microsoft's ex parte complaint to the Western District of North Carolina alleged violations of the CFAA, the CAN-SPAM Act, the Electronic Communications Privacy Act, trademark law, the RICO Act, and state computer trespass laws, as well as the common laws of conversion, unjust enrichment, and nuisance.[84] The crux of the Microsoft complaint was that Citadel caused the Windows operating system to cease functioning normally and begin operating as a tool of deception and theft while still bearing Microsoft trademarks.[85] Not only did Citadel harm Microsoft's brands and trademarks, but the botnet also led to customer frustration, which unfairly damaged the company's reputation and goodwill.[86] In addition to these somewhat indirect harms, Microsoft incurred costs in incorporating security features to resist Citadel.[87] The court ruled that unless the defendants were restrained and enjoined, immediate and irreparable harm would occur to both Microsoft and the public.[88] As such, the district court judge granted all three of Microsoft's requests: an emergency temporary restraining order, a seizure order, and a preliminary injunction.[89] In accordance with good cause and the interests of justice, the order was granted without prior warning to the defendants because notice would likely have resulted in the sale, transfer, disposition, destruction, or concealment of the illegal processes.[90] The judge directed the FBI and U.S. Marshals Service to seize, impound, and deliver all of the defendants' computers, servers, storage devices, software, data,

[82] Press Release, Microsoft, Microsoft, Financial Services and Others Join Forces To Combat Massive Cybercrime Ring (June 5, 2013), http://www.microsoft.com/en-us/news/press/2013/jun13/06-05dcupr.aspx.

[83] Albanesius, *supra* note 81.

[84] Brief for Petitioner at 1, Microsoft Corp. v. John Doe, No. 3:13-CV-319, 2013 WL 2728614 (W.D.N.C. 2013).

[85] *Id.* at 27.

[86] *Id.* at 28.

[87] *See id.*

[88] Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, Microsoft Corp. v. John Doe, No. 3:13-CV-319 (W.D.N.C. 2013).

[89] *Id.* Microsoft's lawyers "asked a judge for a temporary restraining order against the spammers, which would require them to show up to a hearing to defend themselves. The spammers, of course, didn't show, which opened the door for Microsoft to 'win by default' . . . ." Jennifer Warnick, *Digital Detectives*, MICROSOFT, http://www.microsoft.com/en-us/news/stories/cybercrime/index.html (last visited Dec. 18, 2014).

[90] Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *supra* note 88, at 8.

and media located in noted facilities.[91] As assurance and collateral, the court ordered Microsoft to post a bond of $300,000.[92]

One week after the ruling, Microsoft employees, escorted by U.S. Marshals in a campaign codenamed Operation b54, collected evidence and seized two data hosting facilities.[93] In doing so, the operation simultaneously cut communications between the 1462 separate botnets operated by Citadel and the millions of computers infected by them.[94] Meanwhile, the FBI coordinated an assault on Citadel in other countries, working with Europol and law enforcement counterparts in more than eighty nations.[95] Microsoft then began a two-step process of disabling the command-and-control centers and cleansing infected users.[96] In phase one, Microsoft used a process called "sinkholing," in which it set up servers "to mimic the botnet command and control centres [*sic*]" and collected IP addresses of the zombies.[97] In phase two, owners of the zombie computers or their Internet service providers were contacted and offered step-by-step instructions on how to remove the botnet.[98] While the coordinated effort did not lead to the arrest of Aquabox, the alleged Citadel master,[99] it did result in the disruption of almost 90% of the Citadel botnet.[100] In the nearly two months following Operation b54, almost 40% of all Citadel-zombies were cleaned.[101]

This public-private cooperation in taking down Citadel represented the first of its kind.[102] While some of the details of Operation b54

[91] *Id.* at 15–16.

[92] *Id.* at 19.

[93] Press Release, Microsoft, *supra* note 82.

[94] *Id.*

[95] Jim Finkle, *Exclusive: Microsoft, FBI Take Aim at Global Cyber Crime Ring*, REUTERS (June 5, 2013, 7:52 PM EDT), http://www.reuters.com/article/2013/06/05/net-us-citadel-botnet-idUSBRE9541KO20130605.

[96] *See Citadel Botnet Takedown (b54 Operation) Enters Phase 2*, HKCERT (June 20, 2013), https://www.hkcert.org/my_url/en/blog/13062001.

[97] *Id.*

[98] *See id.*

[99] Finkle, *supra* note 95.

[100] Lucian Constantin, *Microsoft: Almost 90 Percent of Citadel Botnets in the World Disrupted in June*, PCWORLD (July 26, 2013, 7:25 AM), http://www.pcworld.com/article/2045282/microsoft-almost-90-percent-of-citadel-botnets-in-the-world-disrupted-in-june.html.

[101] Lucian Constantin, *FBI, Microsoft Takedown Program Blunts Most Citadel Botnets*, COMPUTERWORLD (July 26, 2013, 9:42 AM PT), http://www.computerworld.com/article/2484375/cybercrime-hacking/fbi--microsoft-takedown-program-blunts-most-citadel-botnets.html.

[102] Richard Chirgwin, *Microsoft and FBI Storm Ramparts of Citadel Botnets*, THE REGISTER (June 6, 2013, 6:31), http://www.theregister.co.uk/2013/06/06/microsoft_feds_breach_citadel_botnets/. Although the FBI and Justice Department had previously coopted the Coreflood botnet in 2011, the private sector played no direct role in this effort. *See* Zetter, *supra* note 62. Similarly, Microsoft had previously engaged in six botnet mitigation operations, but this was "the first time the company has worked with law enforcement to secure a civil seizure warrant to carry out its plans." Chris Brook, *Microsoft, Authorities Disrupt Hundreds of Citadel Botnets with "Operation b54,"* THREATPOST (June 6, 2013,

remain unknown, it is clear that Microsoft exercised its independent civil authorities and coordinated with the FBI, which served court-authorized search warrants and involved foreign law enforcement in the process.[103] Microsoft's General Counsel Brad Smith praised the coordinated action as a demonstration of "the power of combined legal and technical expertise."[104] FBI executive assistant director Richard McFeely similarly said, "creating successful public-private relationships . . . is the ultimate key to success in addressing cyber threats and is among the highest priorities of the FBI."[105] These sentiments have proven to be more than quotes for the press as Microsoft and the FBI once again cooperated in the takedown of the ZeroAccess botnet in December 2013[106] and the GameOver Zeus botnet in June 2014.[107] These multi-pronged attacks work effectively within the judicial and law enforcement systems to leverage both modern and outmoded legal precedent against a 21st century issue. However, if public-private partnerships represent the future of botnet mitigation, it is necessary to evaluate their legitimacy as a form of regulation.

1:38 PM), http://threatpost.com/microsoft-authorities-disrupt-hundreds-of-citadel-botnets-with-operation-b54/100902.

[103] *FBI Statement on Botnet Operation*, THE FED. BUREAU OF INVESTIGATION (June 5, 2013), *available at* http://www.fbi.gov/news/news_blog/botnets-101/fbi-statement-on-botnet-operation.

[104] Press Release, Microsoft, *supra* note 82.

[105] Albanesius, *supra* note 81. McFeely also said that these "actions represent the future of addressing the significant risks posed to our citizens, businesses, and intellectual property by cyber threats and malicious software."

[106] Press Release, Microsoft, Microsoft, the FBI, Europol and Industry Partners Disrupt the Notorious ZeroAccess botnet (Dec. 5, 2013), http://news.microsoft.com/2013/12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/; Richard Domingues Boscovich, *ZeroAccess Criminals Wave White Flag: The Impact of Partnerships on Cybercrime*, MICROSOFT (Dec. 19, 2013), http://blogs.microsoft.com/blog/2013/12/19/zeroaccess-criminals-wave-white-flag-the-impact-of-partnerships-on-cybercrime.

[107] *See* Richard Domingues Boscovich, *Microsoft Helps FBI in GameOver Zeus Botnet Cleanup*, MICROSOFT (June 2, 2014), http://blogs.microsoft.com/blog/2014/06/02/microsoft-helps-fbi-in-gameover-zeus-botnet-cleanup. The public-private partnership between Microsoft and federal law enforcement agencies extends outside the context of botnets. In November 2013, the company unveiled a new headquarters for fighting cybercrime and in February 2014, hosted a "Cybercrime Enforcement Summit" to develop best practices in protecting users online. *Microsoft Hosts Global Consortium of Experts at Cybercrime Enforcement Summit*, MICROSOFT (Feb. 20, 2014), http://blogs.microsoft.com/firehose/2014/02/20/microsoft-hosts-global-consortium-of-experts-at-cybercrime-enforcement-summit/.

III. The Legitimacy of Public-Private Partnerships in Mitigating Botnets

A. Evaluating Legitimacy

Despite the overwhelming recognition of the threat posed by botnets, "the biggest barrier to defending against cyberattacks is the lack of a legal method . . . that also has a credible deterrent effect on potential attackers."[108] The use of public-private partnerships may offer a legitimate and effective way to mitigate botnet attacks and hold the masters accountable. Microsoft's outside counsel in the Citadel takedown stated that the method is successful because the "goal is not to recover assets, but rather to disable the perpetrator's operation."[109] The method allows both Microsoft and the federal government to effectively leverage their skill sets and legal tools. With real-time intrusion detection systems, some argue that the private sector has access to more advanced cybersecurity technology than the federal government.[110] Conversely, the federal government has access to a wealth of information through its intelligence and law enforcement activities.[111] It was the value of these diverse and complementing skill sets that led President Clinton to call for "intense public-private cooperation" in his 2000 National Plan for Information Systems Protection aimed at preventing cyberattacks.[112]

There are, however, critiques of the public-private partnership casting doubt on its effectiveness in mitigating botnets. First and foremost, there were no arrests made as part of Operation b54.[113] Second, the inherent resilience of a botnet's architecture ensures that "absent a total takeover in any botnet takedown, 'the attacker still has a strong foothold and can easily recover . . . .'"[114] Some critics have

[108] Kesan & Hayes, *supra* note 61, at 421.

[109] Mark Mermelstein, Mary Kelly Persyn & Harry J. Moren, *Strategic Remedies for Cybercrime Victims*, 16 J. INTERNET L. 1, 28 (2013).

[110] *See* Kesan & Hayes, *supra* note 61, at 448–49.

[111] *See* Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 240 (2010).

[112] CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, DEFENDING AMERICA'S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION, iii (2000), *available at* http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf. *But see* Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 361 (2006) (explaining that such attempts have not been successful because "currently most information sharing occurs through informal channels").

[113] *See supra* note 101 and accompanying text. For further discussion of the harm in not making arrests, see *infra* Part III.B.5.

[114] *Botnet Takedowns: Effective or Deceptive?*, INFOSECURITY (Nov. 21, 2013), http://www.infosecurity-magazine.com/view/35730/botnet-takedowns-effective-or-deceptive/.

analogized takedown attempts to "Whack-A-Mole,"[115] and have asserted that they "don't have any lasting impact on end-user safety."[116] SophosLab, an IT security company, found that 51% of the Citadel-run domains were not even identified by Microsoft and 20% of the identified domains were not effectively sinkholed.[117] Finally, Microsoft encountered a trove of negative press regarding collateral damage of the Citadel takedown. Following the takedown, security researchers reported that Operation b54 siphoned off malicious data that they themselves were tracking, thus disrupting their ongoing research efforts.[118] A security researcher who runs the abuse.ch blog's botnet tracking services estimated that 1000 of the 4000 seized domain names were already under the control of research teams using them to monitor and gather data on Citadel.[119]

This was not the first or last time that complaints of this sort have been levied against Microsoft. Its takedown of the Zeus botnet in March 2012 also knocked out researchers' servers[120] and its takedown of 3322.org in September 2012 disrupted a public cloud used by millions of legitimate users.[121] More recently, Microsoft's seizure of twenty-three No-IP domains in June 2014 led to service interruption for ordinary, uninfected users.[122] Microsoft took ownership over the disruption, issuing a statement that "[d]ue to a technical error . . . some customers whose devices were not infected by the malware experienced a temporary loss of service."[123] However, others blamed the disruption on Microsoft's "gross abuse of legal process."[124] Less than a week after the takedown, Microsoft reversed course and returned all

[115] *See* Warwick Ashford, *RSA 2014: Microsoft and Partners Defend Botnet Disruption*, COMPUTERWEEKLY (Mar. 3, 2014, 10:59), http://www.computerweekly.com/news/2240215443/RSA-2014-Microsoft-and-partners-defend-botnet-disruption.

[116] *Botnet Takedowns: Effective or Deceptive?*, *supra* note 114.

[117] James Wyke, *Was Microsoft's Takedown of Citadel Effective?*, NAKED SECURITY (June 12, 2013), http://nakedsecurity.sophos.com/2013/06/12/microsoft-citadel-takedown/.

[118] Ted Samson, *Microsoft Accused of Friendly Fire in Citadel Botnet Takedown*, INFOWORLD (June 10, 2013), http://www.infoworld.com/t/security/microsoft-accused-of-friendly-fire-in-citadel-botnet-takedown-220438.

[119] *See* Constantin, *supra* note 100.

[120] Wyke, *supra* note 117.

[121] Suresh Ramasubramanian, *Microsoft's Takedown of 3322.org — A Gigantic Self Goal?*, CIRCLEID (Sept. 17, 2012, 6:53 AM PST), http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/.

[122] *See* Alex Wilhelm, *Microsoft Goes After Botnet, Tanking No-IP's Dynamic DNS Service for Regular Users in the Process*, TECHCRUNCH (July 2, 2014), http://techcrunch.com/2014/07/02/microsoft-goes-after-botnet-tanking-no-ips-dynamic-dns-service-for-regular-users-in-the-process/.

[123] Mike Masnick, *Microsoft Insists that No-IP 'Outage' Was Due to A 'Technical Error' Rather than Gross Abuse of Legal Process*, TECHDIRT (July 1, 2014), https://www.techdirt.com/articles/20140701/15030927747/.

[124] *See, e.g.*, *id.*

of the domains to No-IP and their original owners.[125] This incident placed Microsoft's takedown practices under a microscope and led experts to question the merits of the Digital Crimes Unit.[126] In Roman Hüssy's opinion, these botnet takedown operations have not had any noteworthy impact on cybercrime and are "nothing more than a PR campaign by Microsoft."[127] No matter its intentions, Microsoft is likely not pleased with the recent press surrounding its cybercrime efforts because following the most recent mishap with No-IP, the hashtag #FreeNoIP was created by technology enthusiasts.[128]

The debated effectiveness of the public-private approach to botnet mitigation demonstrates precisely why authors Robert Baldwin and Martin Cave believe that efficiency should not be used as a "single measuring rod or justification for regulatory decisions."[129] Although not regulation per se, absent the passage of legislation or delegation of power to a federal agency, the public-private partnership appears to be filling a void in botnet enforcement. In fact, "the potential of private regulation and enforcement through tort law as an alternative to public enforcement has increasingly been acknowledged . . . ."[130] Thus, it is necessary to analyze the legitimacy of the roles of both the federal government and Microsoft in implementing this public-private partnership as regulation.

In their book, *Understanding Regulation: Theory, Strategy, and Practice*, Baldwin and Cave offer five key criteria on which to evaluate regulation: legislative authority, accountability, due process, expertise, and efficiency.[131] They emphasize the need to place weight on each of the tests and seek out ways in which to improve on one of the fronts "without material loss on another."[132] Baldwin and Cave do not seek to evaluate the moral correctness or legality of a given regulation, but instead inquire into how deserving it is of public support.[133] Due to the unique public-private style of this regulation and narrow focus on cybersecurity, the application of these five benchmarks will also be shaped by Greg Nojeim's four recommendations for

[125] *See* Natalie Goguen, *Update to Microsoft Takedown — Domains Fully Restored*, NO-IP.COM (July 3, 2014), http://www.noip.com/blog/2014/07/03/update-microsoft-takedown/.

[126] *See, e.g.*, *Microsoft Error Plunged No-IP Punters into Darkness*, INFOSECURITY (July 3, 2014), http://www.infosecurity-magazine.com/view/39149/microsoft-error-plunged-noip-punters-into-darkness/.

[127] *Collateral Damage: Microsoft Hits Security Researchers Along with Citadel*, ABUSE.CH (June 7, 2013), https://www.abuse.ch/?p=5362.

[128] *See* Wilhelm, *supra* note 122.

[129] ROBERT BALDWIN & MARTIN CAVE, UNDERSTANDING REGULATION: THEORY, STRATEGY, AND PRACTICE 77 (Oxford Univ. Press, 1999).

[130] Josephine A.W. van Zeben, *The Untapped Potential of Horizontal Private Enforcement Within European Environmental Law*, 22 GEO. INT'L ENVTL. L. REV. 241, 242 (2010).

[131] *See* BALDWIN & CAVE, *supra* note 129, at 77–82.

[132] *Id.* at 83.

[133] *Id.* at 84.

cybersecurity regulation. Nojeim, senior counsel at the Center For Democracy & Technology, recommends favoring industry standards over mandates, developing incentives for sharing information, relaxing authentication and identification requirements, and ensuring transparency.[134]

B. Baldwin and Cave Factors

1. Legislative Mandate

Baldwin and Cave first inquire into whether legislative authority supports the action, arguing that a regulation deserves support when authorized by a fundamental core of democratic authority.[135] In analyzing the legislative mandate of the public-private partnership, it is helpful to compare it to the 2011 FBI-and DOJ-led Coreflood takedown. It is apparent that the public-private partnership is supported by a clearer legislative mandate, unencumbered by unsettled constitutional and statutory analysis. For example, the government-led seizure required a Fourth Amendment analysis that is not compelled by a private civil action. Although the government successfully argued that a warrant was not required,[136] this represented a significant hurdle to overcome. Removed from Fourth Amendment restrictions, Microsoft's takedown efforts are well-supported by common-law and statutory remedies.

The FBI has a mandate to "investigate all federal criminal violations not specifically assigned by Congress to another federal agency."[137] While investigating cyber-based attacks was not an original emphasis of the FBI, it is now one of its top priorities.[138] The FBI even participates in the National Cyber Investigative Joint Task Force, working specifically to target botnet builders and distributors.[139] The democratic legislative process has granted corporations the right to assert civil protection from botnets and the FBI the right to protect them from a broad range of harms. Therefore, under Baldwin and Cave's framework, the partnership can claim public support, and thus, fulfill the mandate.

However, no single statute articulates the mandate for corporate botnet takedowns. Instead the mandate relies on a patchwork of laws, reshaped to achieve the desired result. Microsoft's ability to mitigate

[134] Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SEC. L. & POL'Y 119, 120 (2010).

[135] BALDWIN & CAVE, *supra* note 129, at 77.

[136] *See supra* notes 64–65 and accompanying text.

[137] *El Paso Division: What We Investigate*, THE FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/elpaso/about-us/what-we-investigate/priorities.

[138] *See id.*

[139] *FBI Statement on Botnet Operation*, *supra* note 103.

botnets is governed by archaic legal formulations, which give them "broad discretions" and require creative interpretation and imaginative argumentation.[140] For example, it is highly unlikely that the Lanham Act was signed into law with visions that its false designation of origin and dilution claims would be invoked to engender an ex parte seizure order to disrupt a zombie network of computers.[141] A July 2014 hearing before the Senate Committee on the Judiciary's Subcommittee on Crime and Terrorism provided insight into such a legislative mandate. The hearing, entitled, "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks," featured representatives from the DOJ, FBI, Microsoft's Digital Crimes Unit, and other private sector employees engaged in the fight against botnets.[142] In his opening statement, Senator Sheldon Whitehouse, Chairman of the Subcommittee, stated, "Congress . . . cannot and should not dictate tactics for fighting botnets; that must be driven by the expertise of those on the front lines of the fight."[143] According to Senator Whitehouse, Congress instead should provide a solid legal foundation for such enforcement along with clear governing standards.[144] While Baldwin and Cave suggest improving the clarity of such a mandate,[145] Nojeim supports such an informal approach as it makes the public-private partnership more efficient and flexible.[146]

2. Accountability

According to Baldwin and Cave, oversight is necessary for an effective regulatory effort. Focus on accountability and control is especially important given the imprecise mandate detailed above. In the public-private partnership to mitigate botnets, there are many forms of oversight; however, the efficacy of this control is debatable. First, the

[140] BALDWIN & CAVE, *supra* note 129, at 78.

[141] In fact, Richard Boscovich only conceived of such a creative approach because he once witnessed the successful use of the Lanham Act in an ex parte proceeding to seize counterfeit t-shirts prior to a rock concert in Miami. Richard Boscovich, Assistant General Counsel, Microsoft Digital Crimes Unit, speech at Microsoft's Innovation and Policy Center (July 24, 2013).

[142] *Taking Down Botnets: Public and Private Efforts To Disrupt and Dismantle Cybercriminal Networks: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 113th Cong. (2014), *available at* http://www.judiciary.senate.gov/meetings/taking-down-botnets_public-and-private-efforts-to-disrupt-and-dismantle-cybercriminal-networks.

[143] *Taking Down Botnets: Public and Private Efforts To Disrupt and Dismantle Cybercriminal Networks: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 113th Cong. (2014) (statement of Sen. Sheldon Whitehouse, Chairman, Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary), *available at* http://www.judiciary.senate.gov/imo/media/doc/07-15-14WhitehouseStatement.pdf.

[144] *Id.*

[145] *See* BALDWIN & CAVE, *supra* note 129, at 83.

[146] Nojeim, *supra* note 134, at 120.

judicial system oversees Microsoft's civil claims. Although there is an inherent trust in the court system, the fact that Microsoft's victory in the Citadel case was ex parte casts doubt on the value of this oversight. This relationship also implicates Nojeim's emphasis on the need for transparency in order to evoke public confidence and trust.[147] Furthermore, Baldwin and Cave are skeptical of judges' abilities to educe control because of their lack of competence in specialized areas.[148] This limitation is especially significant when one considers how little a district judge in North Carolina likely knows about cybersecurity.

Microsoft is also made accountable through the bond it posts as collateral.[149] This assurance guarantees that Microsoft could compensate any individual inadvertently affected by the server seizures.[150] However, $300,000 does not seem sufficient given the scale of the seizures and potential scope of the harm. "A store knocked offline for a day may lose $10,000" in sales alone and may suffer even greater loss in reputational damage.[151] Thus, while a bond serves as an effective form of accountability, increasing the required amount could enhance its efficacy.

Finally, the FBI is overseen by both the executive branch and the public. Yet, when government decisions and techniques are kept secret or made confidential, this control measure is weakened.[152] Once again, this does not comport with Nojeim's insistence on transparency and disclosure. This represents a quintessential trade-off identified by Baldwin and Cave "between accountability and the effective pursuit of regulatory objectives."[153] It seems evident, however, that the public-private partnership would be improved by increased transparency and oversight. To achieve this, Microsoft and federal law enforcement agencies could formally involve security researchers as stakeholders in the process. Security researchers could hold the other actors accountable due to their expertise and preexisting involvement in the botnet mitigation realm. They would be able to advise the court on the suitable scope of the takedown procedure and forewarn Microsoft and the FBI of potential collateral damage. Richard Boscovich, assistant general counsel for Microsoft's Digital Crimes Unit, indicated that his

[147] *Id.*

[148] BALDWIN & CAVE, *supra* note 129, at 79.

[149] *See supra* note 82 and accompanying text.

[150] Ashford, *supra* note 115.

[151] CTR. FOR STRATEGIC AND INT'L STUDIES, *supra* note 49, at 6.

[152] *See, e.g.*, Sean Sundwall, *180solutions Collaborates with FBI To Help Nab International Botnet Crime Ring Suspects*, THEFREELIBRARY (Nov. 3, 2005), http://www.thefreelibrary.com/180solutions+Collaborates+With+FBI+to+Help+Nab+International+Botnet...-a0138256285 (explaining that details of the evidence against botnet suspects remained confidential); *see also* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sep. 13, 2013, 4:17 PM), http://www.wired.com/2013/09/freedom-hosting-fbi/ (describing how the FBI secretly took control of servers in an attempt to rid them of malware).

[153] BALDWIN & CAVE, *supra* note 129, at 79.

team already works hand in hand with leading researchers throughout the takedown process, so implementing a formal accountability system may not be very demanding.[154]

One set of security researchers recently lobbied for such an approach, detailing a procedure similar to the Uniform Dispute Resolution Policy for trademark disputes.[155] Botnet-related disputes would not be settled in a district court, but instead by independent arbitrators. Security researchers could be given a role within the arbitration process, and, at the very least would be made cognizant of the takedown efforts. Alternatively, security researchers could be called upon as expert witnesses to guide the court in tailoring a narrow and effective seizure order.

3. Due Process

Baldwin and Cave believe that if regulation is based on fair, accessible, and open procedures, then public support is merited.[156] In their opinion, it is not just about equality, fairness, and consistency, but also about the levels of participation afforded to the public, consumers, and others affected.[157] Microsoft's role in the public-private partnership innately invokes due process because of its reliance on the judicial system. However, the ex parte proceedings leave a lot to be desired. It is clear why the hearing must be ex parte and why the order must be granted without advanced notice — as otherwise the masters would be able to transfer, dispose, or conceal the botnets. However, the legitimacy of preemptive ex parte seizure orders is highly debated in a number of other technology-related contexts, and the lack of balance in this ex parte process could be easily fixed.[158] In the botnet context specifically, Microsoft was criticized for its takedown techniques with regards to the No-IP domains because "Microsoft never contacted [No-IP] or asked [No-IP] to block any subdomains, even though [No-IP has] an open line of communication with Microsoft corporate executives."[159] Due process should be afforded through additional avenues of participation for other stakeholders affected by the

[154] *See* Samson, *supra* note 118.

[155] Tacin Nadji et al., *Beheading Hydras: Performing Effective Botnet Takedowns*, PROCEEDINGS OF THE ACM CONFERENCE ON COMPUTER AND COMMC'NS SEC. 121, 131 (2013).

[156] BALDWIN & CAVE, *supra* note 129, at 79.

[157] *Id.*

[158] *See* Daniel Grobman, *Preemptive Ex Parte Seizure Orders and Substantive Relief: A Far Cry from Congressional Intent*, 33 CARDOZO L. REV. 1185, 1215 (2012) (documenting grievances about preemptive ex parte seizure orders used to seize domain names and trademark infringing goods).

[159] Natalie Goguen, *No-IP's Formal Statement on Microsoft Takedown*, NO-IP (June 30, 2014), https://www.noip.com/blog/2014/06/30/ips-formal-statement-microsoft-takedown/.

takedowns, such as researchers whose domains are seized along with the masters'.[160]

Microsoft's role in the regulatory scheme can also be criticized for the lack of due process in its collection of IP addresses and manipulation of zombies. In establishing a sinkhole that engages with incoming data and analyzes IP addresses, Microsoft's actions oppose Nojeim's recommendation of preserving user anonymity and protecting the free flow of information by limiting identification and authentication.[161] Additionally, some commentators interpreted its proactive measures to cleanse infected users as remote alterations of an individual's computer.[162] When Microsoft sent out configuration files to remove blocks against antivirus vendors' websites, it changed the set-settings within the users' computers without the consent or knowledge of those users, which "[i]n most countries . . . is violating local law."[163] When the government used similar tactics as part of the Coreflood takedown, a technology director at the Electronic Frontier Foundation called it "extremely sketchy" because "[i]t's other people's computers and you don't know what's going to happen for sure."[164]

Due process ensures proper democratic influence over the regulation, which, in turn, legitimizes the regulatory effort. To burgeon due process in the public-private partnership, Microsoft could commit to involving the research community before obtaining or executing the seizure. Third-party security researchers would provide an independent check on the judicial process while simultaneously adding expertise and insight into the practical effect of seizures, takedowns, and sinkholes. Even providing notice to researchers could resolve the noted accountability concerns. With proper notice, security researchers could help avoid service interruptions and research disruptions. Furthermore, involving third-party researchers would only minimally increase the risk of masters finding out about the impending seizures, and thus would not significantly threaten the effectiveness of botnet takedowns. Thus, this alteration would better achieve due process through increased information flows, participation, and disclosure, as suggested by Baldwin and Cave.[165]

4. Expertise

Implementing regulation often requires the exercise of expert judgment. Baldwin and Cave assert that the public must be wary of

[160] *See supra* notes 119–28 and accompanying text.

[161] *See* Nojeim, *supra* note 134, at 120.

[162] *See, e.g.*, Samson, *supra* note 118.

[163] *Collateral Damage*, *supra* note 127.

[164] Zetter, *supra* note 62 (internal quotation marks omitted).

[165] BALDWIN & CAVE, *supra* note 129, at 83.

regulatory efforts that are justified through the invocation of trust rather than reason.[166] For the most part, Microsoft's dependency on the judicial system protects it from charges of making decisions without explanation or validation. While the proceedings are ex parte and the judges lack a level of expertise in the field, Microsoft must present a cogent and well-researched legal argument in support of its actions.

Conversely, the public places a large amount of trust in the expertise of law enforcement. It is difficult for the public to accurately assess whether the FBI's decisions and decision-making processes are appropriate or effective. This is especially true in the cybercrime context because measuring the success of a botnet takedown is only possible through estimation. There is no reliable manner of measuring the size of a botnet, so it is necessary to speculate and make presumptions.[167] Independent security researchers would serve as the greatest check on this authority. For this reason, involving security researchers in the process incorporates Nojeim's second suggestion: to incentivize sharing in the regulatory process. The public should not automatically trust that, "when freed from the duties of explanation," an expert will come to the best decision.[168] Thus, the public-private approach should better incorporate security researchers as a check on the decision-making process, appropriately balancing the trust in law enforcement with the articulated reason of Microsoft.

5. Efficiency

Baldwin and Cave identify two possible claims that can be made in support of a regulation's efficiency. The first demands approval based on the legislative mandate.[169] However, Operation b54 is not explicitly supported by a mandate. Thus, the public-private approach must turn to the alternative claim, urging support based on efficiency as judged by an independent set of criteria measuring allocative and dynamic efficiency.[170]

Allocative efficiency refers to the regulation's ability to redistribute in order to make one consumer better off without making another consumer worse off.[171] The public-private partnership efficiently exploits the diverse and complementing skill sets of both corporate and governmental agencies.[172] In this way, the regulation embraces

[166] *Id.* at 80.

[167] *See* Daniel Plohmann, Elmar Gerhards-Padilla & Felix Leder, *Botnets: Detection, Measurement, Disinfection & Defence*, EUR. NETWORK & INFO. SEC. AGENCY 1, 117 (2011), http://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/forschungsbereiche/botnets-detection-measurement-disinfection-defence.pdf.

[168] BALDWIN & CAVE, *supra* note 129, at 80.

[169] *Id.* at 81.

[170] *Id.*

[171] *Id.*

[172] *See supra* notes 110–12 and accompanying text.

Nojeim's endorsement of increasing the distribution of information and is able to achieve economies of scope. Adding additional participation for security researchers would create additional allocative efficiency by ensuring that the mitigation techniques do not harm consumers.

Dynamic efficiency denotes the ability for a regulatory system to encourage flexibility and innovation.[173] The public-private partnership maintains a high level of dynamic efficiency as it mandates very little rigidity. Unlike the traditional command-and-control regulation style, established through standards, duties, and prohibitions,[174] this approach is based on a non-prescriptive set of common-law precedents and reshaped statutory claims. This amalgamation leads to a lack of complexity and delay in regulation because if a legal claim or law enforcement tactic fails, Microsoft can simply employ a different method. Not only does this regulatory approach encourage desirable innovation and flexibility, it also encourages properly aligned incentives as Microsoft shares the same goal as the public in stopping botnet-related attacks. For example, Microsoft will work hard to implement other technical innovations that could supersede the need for these civil claims at all. Microsoft is properly incentivized to develop the most cost-effective solution and will not be complacent in its attempt to mitigate the problem.

However, the public-private method is also subject to the criticism noted above regarding ineffective results and collateral damage.[175] Reports indicate, "Microsoft [was] not sorry for swallowing researchers' work in [the] Citadel takedown," because, in its opinion, researchers should go beyond mere observation and work harder at prevention.[176] Microsoft defended its course of attack stating that it has consistently accomplished its primary objective: "disrupt, disrupt, disrupt."[177] The implemented techniques "not only help to clean people's computers, but they help take the very infrastructure the botnet needs to be impactful and profitable away from the cyber criminals . . . ."[178] Microsoft and the FBI "[do] not expect to fully eliminate" these botnets, but rather set a goal "to protect people by cleaning the computers infected with the malware so they [can] no longer be

[173] BALDWIN & CAVE, *supra* note 129, at 81.

[174] van Zeben, *supra* note 130, at 246.

[175] *See supra* notes 113–28 and accompanying text.

[176] Liam Tung, *Microsoft Not Sorry for Swallowing Researchers' Work in Citadel Takedown*, CSO (June 11, 2013, 10:12), http://www.cso.com.au/article/464267/microsoft_sorry_swallowing_researchers_work_citadel_takedown/.

[177] Terry Zink, *Microsoft Disrupts the Zeus Infrastructure*, CIRCLEID (Mar. 26, 2012, 12:09 PM PST), http://www.circleid.com/posts/20120326_microsoft_disrupts_the_zeus_infrastructure/ (internal quotation marks omitted).

[178] Alastair Stevenson, *Arresting Hackers More Effective than Botnet Takedowns for Tackling Cybercrime*, V3 (Feb. 10, 2014), www.v3.co.uk/2327200.

used for harm."[179] Thus, they find comfort in the fact that "financial partners reported between 86% and 98% reduction in fraud" after the Citadel takedown.[180] Additionally, Microsoft struck a blow to its critics when, in response to its civil suit against the ZeroAccess botnet, the masters abandoned their zombie network entirely.[181]

Furthermore, Microsoft only represents half of the approach. It is also important to consider the value in successful criminal prosecutions of botnet builders and masters. Arresting the masters is important because "[s]ystems don't rebuild themselves" without the master.[182] In fact, arrests of two botnet masters in the past three years "led to a huge and almost immediate halt in the use of those malicious creations."[183] Although Operation b54 did not result in any arrests, the FBI's ambition to investigate and pursue those in charge cannot be ignored. Even if the FBI's involvement does not conclude in arrests, it leads to greater international awareness and cooperation with regards to botnet investigation and prosecution.

Baldwin and Cave believe that a primary limitation in measuring the efficiency of regulation is the inability to know whether alternative systems would offer superior performance.[184] For example, it is impossible to know whether Microsoft's role in the partnership is necessary. Maybe the FBI would be more efficient if it strictly focused on tracking botnet masters rather than serving search warrants and sharing resources. Maybe new legislation would be passed if corporate efforts ceased. Roman Hüssy subscribes to both of these beliefs, arguing that takedowns are ineffective and trigger countermeasures. He compares botnet takedowns to seizing the baseball bat from a habitual home invader.[185] He believes that the criminal will just buy a new bat, or even worse, buy a gun, making him more dangerous in the future. "[I]t's obvious that the criminals using Citadel won't stop doing cybercrime."[186] In his opinion, the seizures merely result in cybercriminals updating their software and improving their defense mechanisms. Thus, Hüssy believes that coordinated law enforcement and new legislative measures are the keys to mitigating botnets and that corporate efforts should be discontinued.[187]

[179] Boscovich, *supra* note 106.

[180] Ashford, *supra* note 115.

[181] Boscovich, *supra* note 106.

[182] Stevenson, *supra* note 178.

[183] *Id.* (describing how the arrest of the Blackhole Exploit Kit and DNS Changer perpetrators led to immediate results).

[184] BALDWIN & CAVE, *supra* note 129, at 81.

[185] *See Collateral Damage*, *supra* note 127.

[186] *Id.*

[187] *Id.*

IV. CONCLUSION

The public-private partnership between Microsoft and the FBI formed to combat botnets represents a legitimate, layered approach to solve a complicated problem. Leveraging the diverse skill sets and legal devices available to corporate entities and law enforcement, the partnership reduces harm quickly through the seizure of servers, and prevents future attacks, through investigations and arrests. While the partnership approach is not supported by an explicit legislative mandate, it favors flexible industry standards over concrete obligations. It incorporates multiple steps of control, but could be improved through increased transparency and accountability. The regulatory method comports to judicial standards of due process but should integrate additional means of participation. In some respects, the emphasis on expertise is supported, but would be reinforced by increased information sharing with third parties. Finally, while the effectiveness of the regulation is up for debate, the incentives are properly aligned to ensure dynamic efficiency, eventually leading to an efficient solution. In order to improve the public-private partnership approach, security researchers should be included in the process. Currently, takedowns are performed in an ad-hoc manner with limited public oversight. For this reason, the research community is unable to properly assist in the efforts. This lack of coordination and supervision has led to the sinkholing of researcher-owned domains, court orders filed under seal, and the grant of subsequent cleanup actions. Involving security researchers in the process would increase its accountability, due process, expertise, and effectiveness. No matter the solution, it is clear that botnets are a growing problem and that a regulatory solution must be established in the near future.