# INVESTING IN A CENTRALIZED CYBERSECURITY INFRASTRUCTURE: WHY "HACKTIVISM" CAN AND SHOULD INFLUENCE CYBERSECURITY REFORM

*Brian B. Kelly*[*]



*This Note recommends that Congress draft cybersecurity reform legislation in line with President Obama's May 2011 Cybersecurity Legislative Proposal, rather than the House Republican Cybersecurity Task Force's October 2011 Proposal. The former proposal's emphasis on centralized regulation under the*

[*] J.D. Candidate, 2013, Boston University School of Law; B.A. Political Science, 2009, University of California, Santa Barbara. I gratefully thank Beau Barnes for his steady guidance and passion in all things cybersecurity, Mary Herman for her patience in the development of this Note, the *Boston University Law Review* Note Selection Committee for taking an interest in my topic, my parents Betsy and John Kelly for encouraging me to accept new challenges, and Olivia Russell for inspiring me in all my pursuits.

*Department of Homeland Security (DHS) more accurately accounts for the nature of threats posed in cyberspace, including hacktivist groups like the online hacker collective Anonymous who have become the most prominent actors in cyberspace over the last few years. This Note advocates that Congress expressly account for Anonymous in drafting cybersecurity legislation because doing so will deliver an array of otherwise-desirable policy goals.*

*In arriving at these conclusions, this Note explores in detail the history of hacking, hacktivism, and Anonymous. Additionally, it briefly surveys the panoply of current legal mechanisms governing cyberspace. Finally, this Note will advocate for the inclusion of several key elements in any cybersecurity reform legislation, whether or not Congress chooses a DHS-centric model.*

## INTRODUCTION

Of the many topics President Obama was expected to address head-on in the opening stage of his presidency, only political and industry insiders could have guessed that cybersecurity would be one. Surely, President Obama's self-designated mandate upon taking office – "Change" – pertained to the tanking global economy and the prolonged wars in Iraq and Afghanistan. Attention to those gargantuan problems, the American public might have thought, should prevent talk of just about anything else.

Nevertheless, in late May 2009, barely four months after taking his presidential oath, Obama delivered a blunt, urgent speech on securing our nation's cybersecurity network.[1] Partially spurred into action after becoming a victim of a cyberattack himself,[2] President Obama stated that cyberattacks[3] constitute "one of the most serious economic and national security challenges we face as a nation."[4] The President also made clear a belief that has been widely agreed upon by commentators for nearly two decades: "We're not as

[1] *See generally* Press Release, The White House, Office of the Press Sec'y, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (describing the twenty-first century as a "transformational age" but warning that the risks associated with cyberspace create "great peril").

[2] *See id*. ("I know how it feels to have privacy violated because it has happened to me and the people around me. It's no secret that my presidential campaign harnessed the Internet and technology to transform our politics. What isn't widely known is that during the general election hackers managed to penetrate our computer systems. . . . [H]ackers gained access to emails and a range of campaign files, from policy position papers to travel plans. . . . It was a powerful reminder: In this Information Age, one of your greatest strengths – in our case, our ability to communicate to a wide range of supporters through the Internet – could also be one of your greatest vulnerabilities.")

[3] For the purpose of this Note, the term "cyberattack" will be construed broadly to mean any unauthorized access to a cyber network, system, or database, whether or not material damage to that network, system, or database actually occurs.

[4] *See* Press Release, The White House, Office of the Press Sec'y, *supra* note 1.

prepared as we should be, as a government or as a country [for a cyberattack]. . . . This status quo is no longer acceptable – not when there's so much at stake. We can and we must do better."[5]

These statements beg the question: Three years later, has the status quo changed? Are we better equipped in 2012 than we were in 2009 to protect the United States from cyberattacks? Even an optimistic reader of recent news headlines would answer, "No."

Consider the following stories. In December 2010, hackers prevented user access to PayPal – a leading online global payment company – for a four-day period by executing a distributed denial of service (DDoS) attack on the PayPal website.[6] The hackers who took credit for the attack announced that PayPal deserved retribution for its wrongful suspension of WikiLeaks' donation account following the latter's online release of highly classified U.S. State Department documents.[7]

In April 2011, Sony's PlayStation Network – an online gaming community for the company's top-selling video game console – was the victim of a more intrusive cyberattack.[8] Hackers breached security safeguards to steal data from each of the PlayStation Network's seventy-seven million individual user accounts, including birthdates and credit card numbers.[9] Upon discovering the

---

[5] *Id*.

[6] *See* Press Release, U.S. Dep't of Justice, Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks (July 19, 2001), *available at* http://www.justice.gov/opa/pr/2011/July/11-opa-944.html (detailing the history of the PayPal attack in the wake of the arrests of the responsible hackers). DDoS attacks are "attempts to render computers unavailable to users through a variety of means, including saturating the target computers or networks with external communications requests, thereby denying service to legitimate users." *Id*.

[7] *See id*. ("The San Jose indictment alleges that in retribution for PayPal's termination of WikiLeaks' donation account, a group calling itself Anonymous coordinated and executed distributed denial of service (DDoS) attacks against PayPal[]. . . . According to the indictment, Anonymous referred to the DDoS attacks on PayPal as 'Operation Avenge Assange.'").

[8] Jason Schreier, *PlayStation Network Hack Leaves Credit Card Info at Risk*, WIRED (Apr. 26, 2011, 4:43 PM), http://www.wired.com/gamelife/2011/04/playstation-network-hacked/ ("Sony thinks an 'unauthorized person' now has access to all PlayStation Network account information and passwords, and may have obtained the credit card numbers of the service's 70 million users.").

[9] *See id*. ("The PlayStation maker said it believes hackers now have access to customers' vital information, including names, birthdates, physical and e-mail addresses, and PlayStation Network/Qriocity passwords, logins, handles and online IDs."). Shortly after the April attacks, hackers infiltrated another branch of Sony's online web services: Sony Online Entertainment (SOE). Jason Schreier, *Sony Hack Probe Uncovers 'Anonymous' Calling Card*, WIRED (May 4, 2011, 2:08 PM), http://www.wired.com/gamelife/2011/05/sony-playstation-network-anonymous/ ("The intruders in the SOE breach compromised information on 24.6 million users, as well as 20,000 credit card and bank account numbers. Sony discovered the SOE breach on Sunday [May 1, 2011] while investigating an earlier

breach,[10] Sony promptly shut down the PlayStation Network for more than a month in order to conduct a thorough security and damage assessment.[11] Sony estimated that the cyberattack caused approximately $170 million in losses for the company.[12] In the weeks preceding the cyberattack, the hackers alleged to be responsible had taken to the blogosphere to declare war on Sony for its decision to sue a hacker in January 2011 for publishing the PlayStation 3 console code obtained from reverse-engineering the device.[13]

In August 2011, Bay Area Rapid Transit (BART) – the San Francisco Bay Area's public transportation system – shut down cell phone service in its subway tunnels to prevent mobile communication between protestors seeking to halt movement of subway trains.[14] Hackers swiftly denounced BART's

attack that compromised information on 77 million accounts from Sony's PlayStation Network and Qriocity services in April.").

[10] Martyn Williams, *PlayStation Network Hack Will Cost Sony $170M*, NETWORK WORLD (May 23, 2011, 7:11 AM), http://www.networkworld.com/news/2011/052311-playstation-network-hack-will-cost.html (explaining that Sony hired several computer security companies to rebuild the security system and run forensic auditing tests); *see also* Liana S. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS, Apr. 26, 2011, *available at* http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426 (citing a statement a by research director of the SANS institute, a computer security organization, that the attack may be the single largest identity data information theft to date).

[11] Keir Thomas, *Sony Makes It Official: PlayStation Network Hacked*, PCWORLD (Apr. 23, 2011, 7:35 AM), http://www.pcworld.com/article/226128/sony_makes_it_official_playstation_network_hacked.html (explaining that due to the intrusive nature of the cyberattack, "Sony has to trace every corner of their systems affected by the hacker and repair it or restore files. It's like removing a rodent infestation from a house – there's no quick and easy fix.").

[12] Kim Zetter, *FBI Arrests U.S. Suspect in LulzSec Sony Hack; Anonymous Also Targeted*, WIRED (Sept. 22, 2011, 5:51 PM), http://www.wired.com/threatlevel/2011/09/sony-hack-arrest/ (explaining that the $170 million figure includes expenses for protecting against future attacks as well).

[13] Matt Peckham, *Anti-Sony Hackers Attacking Employee Families and Children*, PCWORLD (Apr. 5, 2011, 5:49 AM), http://www.pcworld.com/article/224267/antisony_hackers_attacking_employee_families_and_children.html. Specifically, the hackers accused Sony that its lawsuit amounted to an "unforgivable offense against free speech and internet freedom." *Operation Payback Brings You #OpSony*, ANONNEWS, http://anonnews.org/?p=press&a=item&i=787 (last visited Aug. 13, 2012).

[14] Michael Cabanatuan, *BART Admits Halting Cell Service to Stop Protests*, S.F. CHRON. (Aug. 13, 2011), http://www.sfgate.com/default/article/BART-admits-halting-cell-service-to-stop-protests-2335114.php ("Benson Fairow, BART's deputy police chief, said he decided to switch off the service out of concern that protesters on station platforms could clash with commuters, create panicked surges of passengers, and put themselves or others in the way of speeding trains or the high-voltage third rails."). The purpose of the protest was to voice criticism over a fatal July 2011 shooting of a knife-wielding man by BART police. *Id*.

action, condemning it as a violation of civil rights,[15] and executed a series of cyberattacks on BART websites as retribution.[16] Simultaneously, the hackers orchestrated a live protest with like-minded Bay Area residents in BART stations, causing the complete closure of two downtown San Francisco subway stations during rush hour.[17]

Unsurprisingly, all three cyberattacks originated from a single online hacker collective that first emerged in 2003: Anonymous.[18] Illustrated by the examples above, Anonymous is not defined as, and does not intend to be defined as, the traditional cast of voiceless, faceless hackers. Rather, Anonymous publicly leads the "hacktivism" movement,[19] "the nonviolent use

[15] *This Is a Message from Anonymous to the Bay Area Rapid Transit System (BART)*, YOUR ANON NEWS (Aug. 12, 2011, 11:14 PM), http://youranonnews.tumblr.com/post/8850132926/this-is-a-message-from-anonymous-to-the-bay-area-rapid ("We will not tolerate censorship. We will do everything in our power (we are legion) to parallel the actions of censorship that you have chosen to engage in. We will be free to speak out against you when you try to cover up crimes, namely on behalf of those who have engaged in violence against a mostly unarmed public. . . . People of San Francisco, join us Every Monday at 5pm for a peaceful protest at Civic Center station to illustrate the solidarity with people we once knew and to stand up for your rights and those of your fellow citizens. We will be wearing 'blood' stained shirts for remembrance to [sic] the blood that is on the hands of the BART police."); *see also OpBART*, ANONNEWS, http://anonnews.org/?p=press&a=item&i=1068 (last visited Oct. 7, 2012) ("[BART] violated the people's right to assembly and prevented other bystanders from using emergency services by blocking cell phone signals in order to stop a protest against the BART police murders.").

[16] *Two BART Stations Closed, 10 Protestors Arrested*, INT'L BUS. TIMES (Aug. 23, 2011, 10:23 AM), http://sanfrancisco.ibtimes.com/articles/202507/20110823/anonymous-two-bart-stations-closed-10-protesters-arrested-san-francisco.htm ("On Aug. 14 . . . [hackers launched a cyberattack on] the BART Web site, leaking 2,001 names of users as well as their passwords. The addresses and phone numbers of BART users were also released. . . . On Aug. 17, the group hacked into the BART police website in San Francisco, publishing 102 police officers' personal information, including their home addresses and email accounts and passwords.").

[17] *Id*. ("Another BART protest broke out during the rush-hour on Monday evening, which led to closure of two BART stations.").

[18] Scott Neuman, *Anonymous Comes Out in the Open*, NPR (Sept. 16, 2011), http://www.npr.org/2011/09/16/ 140539560/anonymous-comes-out-in-the-open (describing Anonymous as a "cyberguerilla" group).

[19] Anonymous describe themselves as "a decentralized network of individuals focused on promoting access to information, free speech, and transparency." *About Us*, ANONYMOUS ANALYTICS, http://anonanalytics.com/ (last visited July 21, 2012); *see also* Quinn Norton, *Anonymous 101: Introduction to the Lulz*, WIRED (Nov. 8, 2011, 5:30 AM) [hereinafter *Anonymous 101: Part I*], http://www.wired.com/threatlevel/2011/11/anonymous-101/all/1 ("Anonymous is a nascent and small culture, but one with its own aesthetics and values, art and literature, social norms and ways of production, and even its own dialectic language."); Quinn Norton, *Wired.com Embeds with #Occupy and Anonymous*, WIRED (Oct. 18, 2011, 6:27 PM), http://www.wired.com/threatlevel/2011/10/quinn-norton-occupy/ ("Anonymous .

of illegal or legally ambiguous digital tools in pursuit of political ends."[20] Even under the discrete umbrella of hacktivism, however, Anonymous has a distinct make-up: a decentralized (almost nonexistent) structure, unabashed moralistic/political[21] motivations, and a proclivity to couple online cyberattacks with offline protests.[22]

Against this backdrop of frequent and highly publicized cyberattacks, Congress is in the midst of considering a bevy of legislative proposals aimed squarely at cybersecurity. The last two years have seen at least twenty-two different cybersecurity-related legislative proposals in the form of Congressional bills, executive proposals, and formal recommendations from a Republican House of Representatives task force.[23] This overwhelming number

. . [is an] example[] of a new kind of hybrid entity, one that breaks the boundaries between 'real life' and the internet, creatures of the network embodied as citizens in the real world.").

[20] Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation 1-2 (Sept. 2004) (unpublished Ph.D. dissertation, Harvard University), *available at* http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf (explaining that hacktivism is "the marriage of political activism and computer hacking . . . combin[ing] the transgressive politics of civil disobedience with the technologies and techniques of computer hackers"). The Department of Homeland Security currently defines hacktivism as a "cyber exploitation or [an act by an] attack actor whose intent is driven by a social, religious, political, or religious ideology." DEP'T OF HOMELAND SEC., NAT'L CYBERSECURITY & COMMC'NS INTEGRATION CTR., DHS BULL. NO. A-0020-NCCIC, ASSESSMENT OF ANONYMOUS THREAT TO CONTROL SYSTEMS (2011) [hereinafter DHS 2011 BULLETIN], *available at* http://www.wired.com/images_blogs/threatlevel/2011/10/NCCIC-AnonymousICS.pdf.

[21] For the purpose of this Note, "political," when referenced in the context of hacktivism, will be defined broadly to represent any kind of morally grounded action, rather than connoting partisanship as it often does in current events.

[22] *See infra* notes 73-74, 90 and accompanying text (describing frequent cyber attacks against the United States government as well as private, religious institutions such as the Church of Scientology).

[23] *See* Identifying Cybersecurity Risks to Critical Infrastructure Act of 2012, H.R. 6221, 112th Cong. (2012); Cybersecurity Act of 2012, S. 3414, 112th Cong. (2012); Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 3342, 112th Cong. (2012); Federal Information Security Amendments Act of 2012, H.R. 4257, 112th Cong. (2012); Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 2151, 112th Cong. (2012); Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012); Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness (PRECISE) Act of 2011, H.R. 3674, 112th Cong. (2011); Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2012); Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011); International Cybercrime Reporting and Cooperation Act, S. 1469, 112th Cong. (2011); Data Security Act of 2011, S. 1434, 112th Cong. (2011); Data Breach Notification Act of 2011, S. 1408, 112th Cong. (2011); Secure and Fortify Electronic (SAFE) Data Act, H.R. 2577, 112th Cong. (2011); Cybersecurity Enhancement Act of 2011, S. 1152, 112th Cong. (2011); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Cybersecurity Enhancement

of proposals alone signals Washington's recognition of the importance of cybersecurity.

Thus, the question is not *if* cybersecurity reform will be passed, but *when* and *in what form*.[24] This Note will primarily analyze and discuss the merits of

Act of 2012, H.R. 2096, 112th Cong. (2012); Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011); Cybersecurity and Internet Safety Standards Act, S. 372, 112th Cong. (2011); Cyber Security and American Cyber Competitiveness Act of 2011, S. 21, 112th Cong. (2011); Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. (2011); EXEC. OFFICE OF THE PRESIDENT, LEGISLATIVE LANGUAGE: LAW ENFORCEMENT PROVISIONS RELATED TO COMPUTER SECURITY (2011) [hereinafter OBAMA PROPOSAL], *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf; HOUSE REPUBLICAN CYBERSECURITY TASK FORCE, RECOMMENDATIONS 4 (2011), *available at* http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf [hereinafter REPUBLICAN TASK FORCE PROPOSAL]. For a consolidated list of all twenty-two proposals, see *Cybersecurity Legislation Tracker*, CIPHERLAW GROUP, https://www.cipherlawgroup.com/legislation (last updated Sept. 13, 2012).

[24] On November 16, 2011, Senate Majority Leader Harry Reid stated: "[I]t is my intent to bring comprehensive cyber security legislation to the Senate floor for consideration during the first Senate work period of next year." Gautham Nagesh, *Reid Says Senate Will Take up Cybersecurity Bill Next Year*, THE HILL (Nov. 17, 2011, 11:52 AM), http://thehill.com/blogs/hillicon-valley/technology/194245-senate-will-take-up-cybersecurity-bill-next-year. Expedient consideration and passage of cybersecurity legislation has received bipartisan support, as several prominent Senate Independents, Republicans, and Democrats – Joe Lieberman (I-Conn.), Susan Collins (R-Me.) and Tom Carper (D-Del.), respectively – echoed Majority Leader Reid's declaration in their November 17, 2011, statement: "Every day Congress fails to strengthen the cybersecurity of the nation's critical infrastructure is another day of unacceptable risk for our country. . . . Hackers, criminals, and antagonistic foreign powers are maliciously probing our cyber defenses every day on an unprecedented scale, and it is no secret they have found our defenses to be vulnerable." *Id*.

As of the time of this Note's publication, the Lieberman/Collins-introduced Cybersecurity Act of 2012 was the closest Congress has come to passing comprehensive legislative reform. On August 2, 2012, however, the Act fell eight votes short of the required sixty in the Senate. *See* Ramsey Cox & Jennifer Martinez, *Cybersecurity Act Fails Senate Vote*, HILL (Aug. 2, 2012, 11:36 AM), http://thehill.com/blogs/hillicon-valley/technology/241851-cybersecurity-act-fails-to-advance-in-senate [hereinafter Cox & Martinez, *Cybersecurity Act Fails*]. The Cybersecurity Act of 2012 was endorsed by the White House and, as explained in further detail below, fell closer to a direct-regulation model rather than a market-incentive model for legislative reform, albeit in substantially diluted form, to appease Republican detractors. *Id*.; *see also* Ramsey Cox & Jennifer Martinez, *Senate Sets Up Cyber Vote for Thursday, Lawmakers Still Working on Amendments*, THE HILL (July 31, 2012, 7:31 PM), http://thehill.com/blogs/floor-action/senate/241457-senate-fails-to-reach-agreement-on-cyber-amendments-vote-to-proceed-scheduled-for-thursday (listing concessions made by the bill's sponsors, including, most importantly, removing a provision that allowed federal regulators to make voluntary cybersecurity benchmarks mandatory for critical infrastructure operators). The Act's failure, coming just a few months before the 2012 Presidential election and the day before Congress's annual August recess, "likely kills any legislative

just two of the many recent proposals: President Obama's May 2011 legislative proposal (the "Obama Proposal")[25] and the October 2011 House Republican Cybersecurity Task Force ("Task Force") legislative recommendations (the "Republican Task Force Proposal").[26]

These two proposals originate from highly incentivized political actors within the Democratic and Republican parties. President Obama has had a strong political incentive to take credit for potential comprehensive cybersecurity reform, especially due to the fact that he addressed the need for change in the opening months of his presidency.[27] Similarly, the members of the House Republican Cybersecurity Task Force, which was formed in June 2011 by Speaker John Boehner and Majority Leader Eric Cantor, have had an equally strong incentive to ensure their own reelection, retain control of the House, and deliver a political blow to President Obama.[28] Additionally, elements of each bill represent (popularly believed, but perhaps clichéd) normative tendencies of the two parties: Democratic-favored direct regulation versus Republican-favored market incentives. Therefore, due to the proposals' links to incentivized party leaders, the final version of cybersecurity reform will likely embody major elements from one of these two proposals.

Ultimately, many factors will shape cybersecurity reform[29]: government resources (both financial and personnel), international coordination, particular external national security threats, among others. In analyzing the Obama and Republican Task Force Proposals and advocating for one over the other, this Note will also seek to answer the following questions: Why should legislators specifically consider hacktivists in shaping reform, especially when hacktivists, compared to other types of cybercriminals, may not pose the greatest absolute threat to the U.S. economy or national security? How well do the Obama Proposal and Republican Task Force Proposal account for the unique problems created by hacktivism? How can legislators expect to deter cybercrime that is politically or philosophically motivated? Finally, will

action on cybersecurity this year, punting efforts to 2013." Cox & Martinez, *Cybersecurity Act Fails*, *supra*.

[25] *See* Press Release, The White House, Office of the Press Sec'y, Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal [hereinafter Obama Proposal Fact Sheet].

[26] *See* REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23.

[27] *See supra* text accompanying note 1.

[28] Josh Smith, *House Republicans Propose Cybersecurity Incentives over Regulation*, NAT'L J. (Oct. 5, 2011, 4:22 PM), http://www.nationaljournal.com/tech/house-republicans-propose-cybersecurity-incentives-over-regulation-20111005.

[29] *See* REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 4 ("Cybersecurity is a complex set of issues involving legal, economic, and national security considerations."); Nagesh, *supra* note 24 (describing Majority Leader Reid's mandate for reform as "comprehensive" rather than reform merely aimed at, for instance, data breach notification regulations).

addressing hacktivism through legislative reform provide collateral benefits that alleviate or prevent other major cybersecurity concerns?

Part I explains the current state of cybersecurity, hacktivism, and the pertinent law. This Part will demonstrate that hacktivism, and particularly the hacktivist group Anonymous, present unique problems in the cybersecurity realm which current law is ill-equipped to handle. Part II proceeds to introduce the substance of the Obama Proposal and Republican Task Force Proposal, highlighting similarities and differences. Part III concludes by endorsing, in large part, the Obama Proposal. This Part argues that the Obama Proposal's emphasis on the central role to be played by the Department of Homeland Security (DHS) in regulation, policing, and enforcement better accounts for both the nature of cybersecurity threats generally and hacktivism specifically. In addressing the latter concern, this Note posits that the Obama Proposal's quest to counter hacktivism also yields considerable collateral benefits to other cybersecurity concerns.

## I. CYBERCRIME, HACKTIVISM, AND THE LAW

### A. *The Current State of Cybercrime*

To understand the proper scope of reform, it is essential to first comprehend three key elements of cybercrime: who is being harmed, the magnitude of the harm, and the origin of harm. The notion that cybercrimes today predominantly take the form of email scams that can be prevented by pre-installed anti-virus software on a home desktop computer is utterly naïve, no matter how many of those pesky spam messages swarm our inboxes.[30] Modern hackers use increasingly sophisticated methods[31] to attack a variety of

[30] *See* Terrence Berg, *The Changing Face of Cybercrime: New Internet Threats Create Challenges to Law Enforcement*, MICH. B.J., June 2007, at 18, 18 ("Cybercrime generally includes any crime carried out primarily by means of a computer or the Internet. Examples include hacking into or damaging a computer network; accessing and stealing electronic data or trade secrets without authorization; fraud in connection with an Internet auction; spam (false or misleading bulk commercial e-mail); e-mail threats of violence or extortion (cyberstalking); stealing credit card information through a phony website log-in page (phishing); soliciting minors for sexual activity or trading child pornography or other contraband over the Internet; and distributing pirated music, movies, and software via file-sharing networks (or warez sites), just to name some of the most common." (internal quotation marks omitted)). This is not to say, however, that unsolicited spam email is no longer prevalent; as of December 2006, it accounted for ninety percent of all email. *Id*. at 20. The point is that while spam email has not subsided, the more significant harm associated with other kinds of cybercrime has seeped into the public consciousness.

[31] For instance, Sony characterized the nature of the SOE and PlayStation Network hacks as a "very carefully planned, very professional, highly sophisticated criminal cyber attack." Patrick Seybold, *Sony's Response to the U.S. House of Representatives*, PLAYSTATION.BLOG (May 4, 2011), http://blog.us.playstation.com/2011/05/04/sonys-response-to-the-u-s-house-of-representatives/. In the wake of these cyberattacks, Sony hired an online security firm,

targets that occupy nearly every corner of our society: private persons;[32] corporations;[33] religious institutions;[34] and governmental entities, including

whose chief technology officer reiterated the same assessment. Jesse Emspak, *Anonymous Launches DDoS Attack on Sony*, INT'L BUS. TIMES (Apr. 6, 2011), http://www.ibtimes.com/articles/131421/20110406/anonymous-launches-ddos-attack-on-sony.htm ("Prolexic's chief technology officer, Paul Sop, noted that most people think a DDoS is a simple flood of data. But they can often be much more sophisticated than that, sometimes involving only a few kilobits rather than megabytes worth of requests to a targeted machine.").

[32] In one cyberattack, more than 26,000 private persons' email and password log-in information to pornographic websites was published online by hackers. Stephen Chapman, *26,000 Email Addresses and Passwords Leaked. Check This List to See if You're Included*, ZDNET (June 12, 2011, 10:03 PM), http://www.zdnet.com/blog/btl/26000-email-addresses-and-passwords-leaked-check-this-list-to-see-if-youre-included/50424. A few days later, the same hackers leaked an additional 62,000 email/password combinations of private persons. Stephen Chapman, *LulzSec Leaks 62,000 Emails and Passwords, Also Targets CIA*, ZDNET (June 16, 2011, 7:24 AM), http://www.zdnet.com/blog/btl/lulzsec-leaks-62000-emails-and-passwords-also-targets-cia/50831 [hereinafter Chapman, *62,000 Emails*].

[33] Excluding those already mentioned above, prominent corporate targets have included Amazon, Visa, MasterCard, Nintendo, Fox, Bethesda Software, and PBS. *See* Stephen Chapman, *United States Senate Has Been Hacked by Lulz Security*, ZDNet (June 13, 2011, 5:47 PM), http://www.zdnet.com/blog/btl/united-states-senate-has-been-hacked-by-lulz-security/50542; Tim Lohman, *Hacktivism: The Fallout from Anonymous and LulzSec Part 1*, COMPUTERWORLD (Oct. 11, 2011, 7:11 PM), http://www.computerworld.com/s/article/9220760/Hacktivism_The_fallout_from_Anonymous_and_LulzSec_Part_1; Neuman, *supra* note 18. Troublingly, national-security-related firms, like military defense contractors, that are perceived as bastions of secure, confidential information, have not been immune to cyberattacks either. *See* Fahmida Y. Rashid, *Pentagon Admits Major Data Breach as It Unveils Defensive Cyber-Strategy*, EWEEK (July 14, 2011), http://www.eweek.com/c/a/Security/Pentagon-Admits-Major-Data-Breach-as-It-Unveils-Defensive-CyberStrategy-869009/ ("A foreign government was behind a March [2011] cyber-attack against military computers that led to 24,000 files being stolen from a defense contractor, the Department of Defense said. The intruders were after files related to missile tracking systems, unmanned aerial vehicles and the Joint Strike Fighter.").

[34] In 2008, Anonymous publicly sparred with the Church of Scientology over the Church's efforts to require Internet websites to remove an unflattering video of Tom Cruise describing his Scientologist faith. Ryan Singel, *War Breaks Out Between Hackers and Scientology – There Can Be Only One*, WIRED (Jan. 23, 2008, 11:16 AM), http://www.wired.com/threatlevel/2008/01/anonymous-attac/. More recently, Anonymous launched a cyberattack, albeit a mild one, on the website of the oft-criticized Westboro Baptist Church, well known for its inflammatory, anti-gay protests against the U.S. military, including at the funerals of fallen soldiers. *See* Joe Coscarelli, *Anonymous Hackers Take Westboro Baptist Church Website, Briefly, Just to Show They Can*, VILLAGE VOICE (Feb. 24, 2011, 1:25 PM), http://blogs.villagevoice.com/runninscared/2011/02/anonymous_hacke_4.php.

local police units,[35] industrial and utility systems,[36] and major federal agencies and legislative bodies.[37]

For instance, in November 2011 a two-year FBI investigation codenamed "Operation Ghost Click" concluded with the arrest of six Estonian nationals who infected millions of computers globally, shutting down victims' antivirus software to divert profits from Internet advertisements, yielding them a $14 million windfall.[38] Among the computers infected were those belonging to individuals, businesses, and government entities.[39] An FBI agent who worked on the case was quoted as saying, "[The cybercriminals] were organized and operating as a traditional business but profiting illegally as the result of the

[35] In the largest cyberattack against law enforcement, in 2011 Anonymous released ten gigabytes of sensitive data from more than fifty U.S. police departments. *See* Paul Suarez, *AntiSec Hackers Steal, Post Police Data*, PCWORLD (August 6, 2011, 1:31 PM), http://www.pcworld.com/article/237459/antisec_hackers_steal_post_police_data.html (explaining that sensitive data included "more than 300 mail accounts; personal information for more than 7000 individuals including home addresses, phone numbers, and Social Security numbers; online police training files; a snitch list compilation; and server passwords"). Anonymous member "Voice" announced that the group's widespread assault on law enforcement agencies was intended to "demonstrate the inherently corrupt nature of law enforcement . . . as well as result in possibly [sic] humiliation, firings, and possible charges against several officers . . . [and] disrupt and sabotage their ability to communicate and terrorize communities." *Shooting Sheriffs Saturday: Official Release Statement*, PASTEBIN.COM (Aug. 5, 2011), http://pastebin.com/iKsuRkUj. Commentators, however, speculate that the cyberattack was a direct response to the recent arrests of several prominent Anonymous members. *See* Suarez, *supra* (referencing the arrest of Jake Davis, codenamed "Topiary," leader of a viable Anonymous subgroup).

[36] Perhaps the most famous attack to a utility system came in 2010, when an Iranian nuclear facility was the victim of a highly evolved cyberworm nicknamed "Stuxnet." *See* Ron Rosenbaum, *The Triumph of Hacker Culture*, SLATE (Jan. 21, 2011, 11:55 AM), http://www.slate.com/articles/life/the_spectator/2011/01/the_triumph_of_hacker_culture.single.html (reporting that the Stuxnet malware, comprised of more than 15,000 lines of code, caused the self-destruction of 1000 carefully selected uranium-refining centrifuges in Iran's Natanz nuclear facility).

[37] Some of the high-profile targets have included the CIA and U.S. Senate websites, both attacked in 2011. *See* Chapman, *62,000 Emails*, *supra* note 32 (reporting that hackers crashed the CIA.gov website server); Chapman, *supra* note 33 (reporting that hackers accessed and stole a "considerable amount of data pertaining to the internal server structure of Senate.gov" and that "amongst the pile of data [was] the email address of a server administrator"). Cyberattacks against government entities have not been confined to U.S. targets, as other victims have included "government sites in Algeria, Chile, Colombia, Egypt, Libya, Iran, Spain and New Zealand." David Jolly & Raphael Minder, *Spain Detains 3 in PlayStation Cyberattacks*, N.Y. TIMES (June 10, 2011), http://www.nytimes.com/2011/06/11/technology/11hack.html.

[38] *Operation Ghost Click: International Cyber Ring that Infected Millions of Computers Dismantled*, FBI (November 9, 2011), http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911.

[39] *Id*.

malware. . . . There was a level of complexity here that we haven't seen before."[40]

The damage of these cyberattacks is alarming. Consider the following statistics from 2010. In a sample of fifty larger-sized U.S. companies[41] that were victims of cyberattacks, the median annual cost of harm inflicted from those attacks was $5.9 million.[42] So while not every corporation should expect to spend upwards of $170 million like Sony to shore up its networks,[43] neither can it expect to go unscathed. In the public sector, the number of reported cyberattacks for the year numbered more than 40,000.[44] Fragmented down to the lowest level, the average cost per compromised record in a malicious or criminal data breach cyberattack was $318.[45] Extrapolated out to the broadest level, the cost of cyberattacks on private citizens worldwide, when accounting for both the direct financial harm and time lost due to recovery, totaled $388 billion.[46] If this figure seems large, it should. $388 billion amounts to more

[40] *Id*.

[41] PONEMON INST., SECOND ANNUAL COST OF CYBER CRIME STUDY: BENCHMARK STUDY OF U.S. COMPANIES 1 (2011), *available at* http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf (defining "larger-sized" as companies with more than 700 enterprise seats).

[42] *Id*. at 4, 6 (explaining that each of the companies from the survey experienced 1.4 successful cyberattacks per week in fiscal year 2011, a forty-four percent increase over the same figure from a year before). The $5.9 million figure does not account for cyberattack prevention, which, if included, would surely inflate the overall cost of each cyberattack. *Id*. at 4 (indicating that the study's cost measure included the costs of "responding to cyber crime incidents" but not the "plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations"). The report defines "cyberattacks" as including "stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country's critical national infrastructure." *Id*. at 1. Condensed even further, the average cost per compromised record of a malicious or criminal data breach cyberattack in the United States was $318 in 2010. PONEMON INST., 2010 ANNUAL STUDY: U.S. COST OF A DATA BREACH 4 (2011), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf (surveying fifty-one U.S. companies from fifteen different industry sectors, that experienced cybersecurity data breaches in 2010).

[43] *See supra* note 12. Since the average expenditure was $5.9 million, one can infer that Sony's $170 million expenditure was not a common occurrence.

[44] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-137, INFORMATION SECURITY: WEAKNESSES CONTINUE AMID NEW FEDERAL EFFORTS TO IMPLEMENT REQUIREMENTS 4 (2011), *available at* http://www.gao.gov/assets/590/585570.pdf (stating that the 41,776 incidents in fiscal year 2010 marked a 650% increase over a five-year period). The GAO Report defined "incident" as any cyberattack which "placed sensitive information at risk." *Id*.

[45] PONEMON INST., *supra* note 42, at 4.

[46] *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually*,

than the global black market for marijuana, cocaine, and heroin combined.[47] Statistics aside, the magnitude of harm posed by a major cyberattack was eloquently summarized in 2003 by Richard A. Clarke, former Special Advisor on Cyberspace Security to President George W. Bush, in his testimony before Congress:

> The threat is really very easy to understand. If there are major vulnerabilities in the digital networks that make our country run, then someday, somebody will exploit them in a major way doing great damage to the economy. What could happen? Transportation systems could grind to a halt. Electric power and natural gas systems could malfunction. Manufacturing could freeze. 911 emergency call centers could jam. Stock, bond, futures, and banking transactions could be jumbled. If that major attack comes at a time when we are at war, it could put our forces at great risk by having their logistics system fail.[48]

Equally inaccurate as the general perception that cybercrime is mostly benign is the mainstream portrait of the cybercriminal as an isolated, rebellious, American male in his late teens or early 20s.[49] In April 2011, the Director of DHS's Office of Cyber Security and Communications testified before Congress that common cybercriminals include "nation states, terrorist networks, organized criminal groups, and individuals located here in the United States."[50] These actors' motives include, among others, "intelligence

---

SYMANTEC (Sept. 7, 2011), http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (reporting that $274 billion of $388 billion lost included "time lost due to [the victims'] cybercrime experiences").

[47] *Id*.

[48] *Cyber Security: The Challenges Facing Our Nation in Critical Infrastructure Protection: Hearing before Subcomm. on Tech., Info. Policy, Intergovernmental Relations and the Census of the H. Comm. on Gov't Reform*, 108th Cong. 13 (2003) (statement of Richard A. Clarke, former Special Advisor to the President for Cyberspace Security) [hereinafter Clarke Testimony].

[49] *See* Berg, *supra* note 30, at 20 ("The profile of the typical cybervillain has also matured in dangerous ways. Unlike the lone hacker of the past, cybercriminals today are becoming more organized, profit-driven, group-oriented, and technologically advanced in their craft."). Some commentators believe that the loner-as-hacker archetype began with the popular 1983 film *War Games*, starring Matthew Broderick as a relatable teen whose hacking unwittingly brings the United States to the brink of World War III. *See, e.g.*, Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 388 (2011). This description, however, is not far off the mark of the group of sixteen hacktivists arrested in a nationwide FBI raid on July 19, 2011. *See* Jana Winter, *16 Suspected "Anonymous" Hackers Arrested in Nationwide Sweep*, FOXNEWS.COM, July 19, 2011, http://www.foxnews.com/scitech/2011/07/19/exclusive-fbi-search-warrants-nationwide-hunt-anonymous/. All those arrested were male and their average age was twenty-six, the youngest aged sixteen and the oldest forty-two. *Id*.

[50] *See The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical*

collection, intellectual property or monetary theft, or disruption of commercial activities."[51] Again, the common theme in cybercrime is that there is no common theme.

Thus, when accounting for the variety of both perpetrators and targets of cybercrime along with the magnitude of harm, the urgent concern of legislators for securing our nation's cybersecurity becomes obvious. This evidence shows how vast any reform effort must be.

### B. *Defining Hacktivism and Anonymous's Place Within the Movement*

#### 1. Hacking and Hacktivism

While the ensemble of cybercriminals varies in resources and affiliation, this Note focuses exclusively on a particular subset of cybercriminals – hacktivists – and within that subset, a single hacktivist group – Anonymous – as the current embodiment of the subset's ideal. Before addressing either hacktivism or Anonymous in depth, however, it is worthwhile to briefly assess the history and nature of hackers generally.

In 1984, Steven Levy, a pioneering technology journalist, coined the term "hacker ethic" to describe a manifesto of sorts running deep across the hacker community.[52] Even early on in the age of the personal computer, many computer users performed "hacks": legal or illegal computer manipulations (e.g., access, defacement, redirects) of computer systems/networks "imbued with innovation, style, and technical virtuosity."[53] Additionally, the "hacker ethic" contained seven core tenants: (1) access to computers should be totally unrestricted; (2) hackers should always honor the "Hands-On Imperative";[54] (3) information should be free; (4) hackers should distrust authority and promote decentralization; (5) hackers should judge their peers only by their hacking, rather than any educational or professional pedigree; (6) it is possible to create beauty and art within the confines of a computer; and (7) computers can better a person's life.[55] Thus, hackers in general have always shared a philosophical approach – perhaps, a sense of purpose – to their Internet presence. Yet despite a common identity, hackers have historically rejected a

*Infrastructure: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Prot., & Sec. Techs. of the H. Comm. on Homeland Sec.*, 112th Cong. 8 (2011) (statement of Sean P. McGurk, Director, Nat'l Cybersecurity & Commc'ns Integration Ctr., Dep't of Homeland Sec.) ("Malicious actors in cyberspace, including nation states, terrorist networks, organized criminal groups, and individuals located here in the United States, have varying levels of access and technical sophistication, but all have nefarious intent.").

[51] *Id.*

[52] STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 27-36 (1984).

[53] *Id.* at 10.

[54] The "Hands-On Imperative" stands for the principle that "essential lessons can be learned about the systems – about the world – from taking things apart, seeing how they work, and using this knowledge to create new and more interesting things." *Id.* at 27.

[55] *Id.* at 27-36.

highly centralized, close-knit sense of community and instead opted for a non-clustered meritocracy.[56]

The leap in ideology from hacking culture generally to politically minded hacktivism is therefore not a large one since hacking can be seen as inherently political given its philosophical roots.[57] However, when hacking becomes explicitly political – i.e., becomes hacktivism – it is reframed from technical feats with an implied philosophical underpinning to the explicit "pursuit of attention for worthy and perhaps neglected issues"[58] in order to shift public discourse, raise awareness, and create public pressure.[59]

Within the "hacker ethic," then, hacktivists share a more fine-tuned set of beliefs: "tolerance for legal risk, naming practices, scale of collective action and propensity for multinational cooperation."[60] These beliefs contain two subtle yet important changes from hacking in general. First, hacktivists engage more frequently in illegal, rather than legal,[61] computer activity. Second, hacktivists more frequently form a collective – an unsurprising result since hacktivists target singular issues rather than merely fragmented pockets of data or code.[62] Yet, despite hacktivists' sense of collectivity behind any particular motive for a hack, individual hacktivist operations are primarily "conducted by

[56] *See id*. at 29-30.

[57] *See* Samuel, *supra* note 20, at 41-42 (explaining that the hacker's "quest for knowledge" promotes a worldview of transparency, access, and openness that directly conflicts with the propriety or confidential nature of many government and private corporation activities). For an alternative characterization of hackers, see Peter T. Leeson & Christopher J. Coyne, *The Economics of Computer Hacking*, 1 J.L. ECON. & POL'Y 511, 512 (2005) (categorizing hackers into three subclasses based on economic motivation: (1) "good hackers," who break into computer systems but then voluntarily reveal the security weaknesses to the system administrator; (2) "bad hackers," who seek fame and status by attacking vulnerable systems and causing disruption; and (3) "greedy hackers," who are driven by profiting from their cyber-exploits and can be characterized as either "good" or "bad" depending on their ulterior motivation).

[58] Samuel, *supra* note 20, at 55.

[59] *Id*. at 73 ("Performative hacktivists are very much oriented to the public eye, and see their activities as a way of challenging corporate and media domination of public discourse. Their hacktions are aimed at shifting that discourse by raising awareness and creating public pressure – not at directly affecting outcomes.").

[60] *Id*. at 48.

[61] An example of a legal hack is "trolling" – obtaining readily available (or poorly protected) Internet data to do any combination of the following: "telephone pranking, having many unpaid pizzas sent to the target's home, DDoSing, and most especially, splattering personal information, preferably humilating [sic], all over the Internet." E. Gabriella Coleman, *Anonymous: From the Lulz to Collective Action*, NEW EVERYDAY (Apr. 6, 2011), http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action.

[62] *See infra* notes 76-77 and accompanying text.

solo or small-group hackers, with little or no apparent coordination of the overall campaign."[63]

2. Anonymous

Neat labels elude those commentators who have sought to categorize Anonymous as an entity. With little consistency, commentators have referred to Anonymous as hackers, activists, vigilantes, a movement, etc.[64] Perhaps then, Anonymous itself is the best authority on what Anonymous is. On its website, Anonymous describes itself as "an internet gathering" rather than a "group."[65] Moreover, Anonymous states that it has "a very loose and decentralized command structure that operates on ideas rather than directives."[66]

"Very loose" might be an understatement. The group is open to anyone[67] and is often rife with dissent over its messages and operations,[68] which is unsurprising given that Anonymous does not utilize formal procedures for conducting its operations. In August 2011, an Anonymous member spoke to the media about this process:

> With any given operation there are always some [Anonymous members] who agree and some who disagree. . . . Annoymous [sic] allows each person individually to vote on each operation, a yes vote means they participate, a no vote means they do not. Anyone is allowed to create an

[63] Samuel, *supra* note 20, at 52.

[64] *See* Joe Dysart, *The Hacktivists*, A.B.A. J., Dec. 2011, at 40, 42 ("What's new is a public bravado and political stance taken by the new vigilantes, or hacktivists, as some call them."); *Anonymous 101: Part I*, *supra* note 19 ("Hacker group, notorious hacker group, . . . pimply-faced, basement-dwelling teenagers, an activist organization, a movement, a collective, a vigilante group, online terrorists, and any number of other fantastical and colorful terms. None of them have ever really fit.").

[65] *ANON OPS: A Press Release*, ANONNEWS (Dec. 10, 2010), http://anonnews.org/?p=press&a=item&i=31.

[66] *Id*.

[67] *See* Coleman, *supra* note 61 ("Technically, Anonymous is open to all and erects no formal barriers to participation.").

[68] *See ANON OPS: A Press Release*, *supra* note 65. Perhaps the best example came in August 2011 when a splinter group within Anonymous threatened to "destroy" Facebook. *See* Adrien Chen, *Hacker Plot to "Kill Facebook" Is All a Terrible Misunderstanding*, GAWKER (Aug. 10, 2011, 5:15 PM), http://gawker.com/5829659/hacker-plot-to-kill-facebook-is-all-a-terrible-misunderstanding ("The internet is quaking with the news that the hacktivist collective Anonymous plans to 'destroy' Facebook on November 5th."). Immediately after the proclamation, a large swell within Anonymous's ranks responded that this operation was not officially endorsed by Anonymous. *Id*. ("After a stunning burst of media coverage, a number of popular Anonymous twitter [sic] accounts and news sources distanced themselves from Operation Facebook, claiming it was a hoax.").

> [operation] and if others vote yes it will get traction and something may be accomplished.[69]

This system seems to allow for the frequent possibility of minority-led projects since there is no minimum approval from the collective required to initiate and execute an operation. If members of Anonymous are interested in executing a cyberattack, they will, even if they constitute a small fraction of the group's overall membership.

So is there anything definitive to be learned from the operations of such a dispersed, seemingly unorganized group? Prior to 2008, perhaps the answer would have been "no." Until that point in time, Anonymous had been most notable for the spread of harmless, humorous Internet pranks like the "rickroll"[70] and "lolcats."[71]

A clash with the Church of Scientology in January 2008 changed that perception, however, shedding light on who (or what) Anonymous is today. The group began a campaign against the Church of Scientology after the Church tried to suppress Internet media outlets' publication of a notorious video of movie star Tom Cruise speaking fanatically (and incoherently) about the religion.[72] What differentiated this Anonymous campaign from its prior attacks was its seriousness and breadth. More than 6000 participating members of the operation, dubbed "Project Chanology," donned Guy Fawkes masks[73] and protested in the streets of ninety cities worldwide, spanning North

---

[69] Kelly Hodgkins & Sam Biddle, *Anonymous to Destroy Facebook on November 5th (Update: Well, Probably Not)*, GIZMODO (Aug. 10, 2011, 12:00 AM), http://gizmodo.com/5829353/anonymous-to-destroy-facebook-on-november-5th (quoting a member of Anonymous).

[70] Being "rickrolled" is a common Internet prank where users are redirected automatically to an un-closeable browser window playing the 1987 Rick Astley song *Never Going to Give You Up*. *See Anonymous 101: Part I*, *supra* note 19 ("The rickroll began as a tool of the /b/tard/Anonymous raid, before spreading so far into the culture that the Oregon legislature and even the US Speaker of the House were rickrolling the world.").

[71] "Lolcats" are simply pictures of cats accompanied by ironic, humorous text. *See Lolcat*, WIKIPEDIA, http://en.wikipedia.org/wiki/Lolcat (last modified Aug. 13, 2012, 6:40 AM).

[72] *See Anonymous 101: Part I*, *supra* note 19 ("A video of a disturbingly manic Cruise leaked out of Scientology in January 2008, and the notably litigious church tried to force hosting services and Gawker to take it down with legal nastygrams.") The Tom Cruise video was still available online as of the time of publication of this Note. Aleteuk, *Tom Cruise Scientology Video – ( Original UNCUT )*, YOUTUBE (Jan. 17, 2008), http://www.youtube.com/watch?v=UFBZ_uAbxS0.

[73] Guy Fawkes was a Englishman who unsuccessfully attempted to blow up the English House of Lords in 1605. Mark Nicholls, *Fawkes, Guy*, OXFORD DICTIONARY OF NATIONAL BIOGRAPHY, http://www.oxforddnb.com/view/article/9230 (last visited May 14, 2012) (recounting the story of the "Gunpowder Plot"). A mask in his likeness was worn by the antihero protagonist "V" in the 1982 comic book series *V for Vendetta*, which was made into a movie in 2006. Tom Lamont, *Alan Moore – Meet the Man Behind the Protest Mask*,

America, Europe, Australia, and New Zealand.[74] Meanwhile, online members raided Scientology websites and prevented the Cruise video from altogether disappearing from the Internet.[75] The Church of Scientology had done nothing to initially provoke Anonymous, but Anonymous members took issue with the Church's litigious history and attempted suppression of free speech on the Internet.[76] The Church's refusal to break stance over the Cruise video triggered Anonymous's now hallmark tone of moral retribution.[77] One Anonymous member recently stated:

> Scientology tried to fuck with our internet, attempting to shut down the Cruise video. It was punished, hard, and continues to be punished nearly four years later. . . . Anonymous was born out of a need to exact retribution. . . . The targets may have broadened but the essential message is the same.[78]

Thus, in the wake of its battle against Scientology, some key characteristics of Anonymous emerged: (1) an unrelenting moral stance on issues and rights, regardless of direct provocation; (2) a physical presence that accompanies online hacking activity; and (3) a distinctive brand.[79] Those characteristics were evident in several of Anonymous's 2011 cyberattacks. "OpBART," mentioned in the Introduction of this Note, contained all three elements, while the attacks on Visa, Mastercard, and Paypal (dubbed "Operation Avenge Assange") exhibited the same, minus the physical presence element.[80]

In 2011, Anonymous also began increasingly targeting governments and government entities, giving its cyberattacks an overtly political flavor. This trend began early in the year when a Tunisian marketplace vendor set himself

---

GUARDIAN (Nov. 26, 2011, 3:05 PM), http://www.guardian.co.uk/books/2011/nov/27/alan-moore-v-vendetta-mask-protest ("A sallow, smirking likeness of Guy Fawkes – created by Moore and the artist David Lloyd for their 1982 series *V for Vendetta*. It has a confused lineage, this mask: the plastic replica that thousands of demonstrators have been wearing is actually a bit of tie-in merchandise from the film version of *V for Vendetta*, a Joel Silver production made (quite badly) in 2006."). The mask was a staple for protesters during the 2011 Occupy Movement protests. *Id*.

[74] *See* Coleman, *supra* note 61.

[75] *See Anonymous 101: Part I*, *supra* note 19; Quinn Norton, *Anonymous 101 Part Deux: Morals Triumph over Lulz*, WIRED (Dec. 30, 2011, 6:00 AM), http://www.wired.com/threatlevel/2011/12/anonymous-101-part-deux/all/1 [hereinafter *Anonymous 101: Part II*].

[76] *See Anonymous 101: Part I*, *supra* note 19.

[77] *See Anonymous 101: Part II*, *supra* note 75.

[78] *Id*.

[79] Some of Anonymous's branding elements include its logo (a nondescript suited man with either no head or a question mark instead of a head), videos narrated by a lifeless computer voice, naming schemes for its operations (like Operation Payback, or "OpPayback"), and, of course, the Guy Fawkes masks. *See id*.

[80] *See id*.

on fire after the dictatorship seized his goods.[81] Anonymous caught wind of the event and after investigating the dictatorship in greater depth, determined the Tunisian government was guilty of widely suppressing its citizens' access to the Internet, or at least portions of the Internet that contained unfavorable (but truthful) stories.[82] Anonymous then conducted cyberattacks against several Tunisian government websites and provided Tunisian citizens with software to circumvent the dictatorship's censorship blocks.[83] Within a month, President Zine El Abidine Ben Ali, the country's dictator, fled after the Arab Spring protests escalated.[84]

Anonymous also targeted U.S. federal and state government entities regularly in 2011. CIA.gov and Senate.gov were the victims of DDoS attacks.[85] BART, target of the aforementioned cyberattack, had to rely on riot police to fend off protesters.[86] In June 2011, after civil rights advocates expressed outrage over Arizona S.B. 1070, an immigration law that has drawn considerable criticism from civil rights commentators,[87] Anonymous quickly launched a series of cyberattacks on the Arizona Department of Public Safety.[88] Separately, in a leaked "For Official Use Only" 2011 bulletin, DHS made clear that it believes Anonymous to be displaying an increased interest in targeting critical infrastructure.[89] A successful cyberattack on, for instance, an

[81] Rania Abouzeid, *Bouazizi: The Man Who Set Himself and Tunisia on Fire*, TIME (Jan. 21, 2011), http://www.time.com/time/magazine/article/0,9171,2044723,00.html.

[82] *See* Quinn Norton, *2011: The Year Anonymous Took On Cops, Dictators and Existential Dread*, WIRED (January 11, 2012, 6:00 AM), http://www.wired.com/threatlevel/2012/01/anonymous-dicators-existential-dread/all/1 [hereinafter *Anonymous 101: Part III*].

[83] *Id*. (quoting an Anonymous member as stating, "We also distributed a care package containing stuff to workaround privacy (restrictions in Tunisia), including . . . script to avoid proxy interception by the Tunisian government on Facebook users.").

[84] *Id*.

[85] *Id*. (stating that Lulzsec, an Anonymous "spinoff group," launched a DDoS attack on CIA.gov and "hacked Sony six times, the U.S. Senate website twice, and an FBI contractor once, getting account data and releasing it onto the web").

[86] *See id*.

[87] *After SB1070: Adios Arizona*, ECONOMIST, Nov. 27, 2010, at 39.

[88] *Hackers Claim Third Attack on Arizona Police*, FOXNEWS.COM, July 2, 2011, http://www.foxnews.com/scitech/2011/07/01/anonymous-hackers-claim-third-attack-on-arizona-police/.

[89] NAT'L CYBERSECURITY & COMMC'NS INTEGRATION CTR., DEP'T OF HOMELAND SEC., BULL. NO. A-0020-NCCIC, ASSESSMENT OF ANONYMOUS THREAT TO CONTROL SYSTEMS (2011), *available at* http://info.publicintelligence.net/NCCIC-AnonymousICS.pdf ("The loosely organized hacking collective known as Anonymous has recently expressed an interest in targeting industrial control systems (ICS)."); *see also* Kim Zetter, *DHS: Anonymous Interested in Hacking Nation's Infrastructure*, WIRED (Oct. 17, 2011, 8:36 PM), http://www.wired.com/threatlevel/2011/10/hacking-industrial-systems/. ICS is a derivative of the term "critical infrastructure," first defined in the USA PATRIOT Act as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or

electrical grid serving hundreds of thousands of urban residents, would bring Anonymous closer toward the "crime" side of the cyberattack spectrum and further away from mere cyber thrill-seeking. Finally, Anonymous was an early participant and public supporter of the Occupy Movement in the fall of 2011, and had a direct hand in launching the Occupy protest in Boston.[90]

Thus, in just one year's time, Anonymous launched cyberattacks on American government entities, threatened to take on the nation's critical infrastructure, and acted as a key participant in a large public protest that famously seeks to uproot the American establishment. And as the frequency of Anonymous's cyberattacks has increased (and spilled over into a physical presence), the group's penchant for disaggregation has given way to what some investigators believe is a coherent structure with ad hoc leaders who delegate tasks, select targets, and reprimand disobedient members.[91]

Simply put, Anonymous has come a long way from "lolcats."[92]

---

destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (2006). There are eighteen ICS sectors, as defined by DHS pursuant to Homeland Security Presidential Directive 7: (1) Agriculture and Food; (2) Banking and Finance; (3) Chemical; (4) Commercial Facilities; (5) Critical Manufacturing; (6) Dams; (7) Defense Industrial Base; (8) Drinking Water and Water Treatment Systems; (9) Energy; (10) Government Facilities; (11) Information Technology; (12) National Monuments and Icons; (13) Nuclear Reactors, Materials, and Waste; (14) Postal and Shipping; (15) Public Health and Healthcare; (16) Telecommunications; (17) Transportation Systems; and (18) Emergency Services. *See* Directive on Critical Infrastructure Identification, Prioritization, and Protection, 39 WEEKLY COMP. PRES. DOC. 1816, 1818, 1821 (Dec. 17, 2003); *see also Critical Infrastructure*, U.S. DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/critical-infrastructure (last visited Sept. 9, 2012).

[90] *Anonymous Joins #OCCUPYWALLSTREET*, ADBUSTERS (Aug. 23, 2011), http://www.adbusters.org/blogs/adbusters-blog/anonymous-joins-occupywallstreet.html; *Anonymous 101: Part III*, *supra* note 82 ("Occupy Wall Street was not an Anonymous plan, but Anonymous came out in support of it in late August, and drew more media attention to it. . . . As occupations spread, anons were there at each step, encouraging. 'I think it was some Anonymous people who saw my tweets, said I should start Occupy Boston,' said Occupy Boston founder Robin Jacks, 'and I thought, I think I will.'").

[91] *See* Coleman, *supra* note 61 ("If one spends time examining the political wings of Anonymous, it is clear that they have enough coherence, history, and ethical substance to separate them in some fashion from some other facets of [fringe internet sites such as] 4chan or troll culture. . . ."); John Cook & Adrian Chen, *Inside Anonymous' Secret War Room*, GAWKER (Mar. 18, 2011, 2:00 PM), http://gawker.com/5783173/inside-anonymous-secret-war-room ("They demonstrate that contrary to the repeated claims of Anonymous members, the group does have ad hoc leaders, with certain members doling out tasks, selecting targets, and even dressing down members who get out of line.").

[92] *See* Dysart, *supra* note 64, at 46 ("Long term, the real worry over Anonymous may hinge on whether the group's increasing predilection to lend its tech skills to popular causes morphs into its core identity. There was nothing funny about the Anonymous decision to attack Visa, PayPal and MasterCard in connection with the WikiLeaks data release, at least

### C. *Current Cybersecurity Law*

Current U.S. cybersecurity law is already a vast, complicated web, involving four categories: (1) federal statutes, both criminal and civil, and regulations; (2) national defense systems; (3) state statutes and monitoring systems; and (4) international coalitions. The initial reaction, and a completely rational one, upon reading this list is: *If current cybersecurity law already encompasses this diverse array of legal channels, why are politicians nevertheless bent on more legislation*? The answer is not immediately apparent, but is discernible upon closer examination.

#### 1. Federal Statutes

In 1986, Congress took its first stab at legislating to protect against cybercrime in passing the Computer Fraud and Abuse Act (CFAA).[93] Under the statute, Congress appointed the Secret Service as the chief investigatory authority of computer crime.[94] The CFAA broadly prohibits (1) "knowingly caus[ing] the transmission of a program, information, code, or command, and . . . intentionally caus[ing] damage . . . to a protected computer" and (2) "intentionally access[ing] a protected computer without authorization, and . . . recklessly caus[ing] damage."[95] Currently, however, the CFAA's definition of protected computers is "narrow and applies mainly to those used by the federal government and financial institutions."[96] The law also provides for civil actions against violators by "[a]ny person who suffers damage or loss by reason of a violation of this section."[97] In the years since its enactment, the CFAA has been updated several times. Each time, Congress strengthened the statute by "creating new crimes, lowering the required level of intent, and increasing the penalties."[98]

---

for those on the receiving end. Instead of simply goofing around, Anonymous has caused real damage in the name of ideological belief."). In April 2012, Anonymous was named one of *TIME*'s "100 Most Influential People in the World." Barton Gellman, *The 2012* TIME *100: Anonymous*, TIME (Apr. 18, 2012), http://www.time.com/time/specials/packages/article/0,28804,2111975_2111976_2112122,00.html; Courtney Palis, *Anonymous Makes the* TIME *100 2012 List, but Places Much Lower Than on the Reader Poll*, HUFFINGTON POST (Apr. 18, 2012, 6:36 PM), http://www.huffingtonpost.com/2012/04/18/time-100-voters-love-anonymous-time-editors-dont_n_1435461.html.

[93] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2006).

[94] *Id*. § 1030(d)(1).

[95] *Id*. § 1030(a)(5)(A)(i)-(ii).

[96] REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 14; *see also* CHARLES DOYLE, CONG. RESEARCH SERV., 97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 1 (2010), *available at* http://www.fas.org/sgp/crs/misc/97-1025.pdf.

[97] 18 U.S.C. § 1030(g).

[98] Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH L.J. 909, 911 (2003).

Separately, the Federal Information Security Management Act of 2002[99] (FISMA) governs the federal government's information security program for its own computers.[100] The statute was created to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets" and "provide a mechanism for improved oversight of Federal agency information security programs."[101] High-ranking bureaucrats have recently criticized the statute's effectiveness in auditing cybersecurity practices and outcomes.[102]

Although not explicitly applicable to computer crimes, the Racketeer Influenced and Corrupt Organizations (RICO) Act,[103] passed in 1970, was Congress's response to the increasing "influence of organized crime on the American economy, which it sought to eliminate through criminal sanctions and civil remedies."[104] As the statute is currently written, computer crimes (e.g., hacking) are not offenses falling within the scope of the bill.[105]

2. National Defense Systems

The federal government partially guards its computers and networks with an intrusion detection system nicknamed "Einstein."[106] Now in its third iteration, the Einstein software is designed to conduct real-time surveillance on, make

[99] 44 U.S.C. § 3541 (2006).

[100] *See* REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23 ("FISMA is the main law governing the federal government's information security program.").

[101] 44 U.S.C. § 3541.

[102] *See* Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116, 145 (2011) ("Recently, the Department of Transportation's CIO [(Chief Information Officer)] questioned the effectiveness of FISMA audits in securing government systems. The former CIO of the Departments of Air Force and Energy echoed this concern, as he opined that the flaws such audits reveal are not always viewed in the perspective of the agencies' overall cybersecurity scheme.").

[103] 18 U.S.C. §§ 1961-1968 (2006).

[104] Eric Lloyd, *Making Civil RICO "Suave": Congress Must Act to Ensure Consistent Judicial Interpretations of the Racketeer Influenced and Corrupt Organizations Act*, 47 SANTA CLARA L. REV. 123, 123 (2007).

[105] *See* 18 U.S.C. § 1961(1)(B) (defining "racketeering activity" in such a way as to exclude computer crimes).

[106] Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SECURITY L. & POL'Y 119, 123 (2010) ("Einstein 2 will be deployed at participating federal agency Internet access points. The first full implementation was at DHS. As of March 15, 2010, nine other agencies and the Executive Office of the President were also using Einstein 2." (footnotes omitted)); *see also* EXEC. OFFICE OF THE PRESIDENT, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE (2008), *available at* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf ("DHS is deploying, as part of its EINSTEIN 2 activities, signature-based sensors capable of inspecting Internet traffic entering Federal systems for unauthorized accesses and malicious content.").

threat-based decisions on, and provide an intrusion prevention system for any activity taking place in certain federal government computer networks.[107] In performing these functions, Einstein shares information and cooperates with federal departments and agencies, including DHS and the National Security Agency (NSA).[108] Thus, currently within its own network, the federal government closely coordinates among departments, wipes personally identifiable information from shared cybersecurity data, and operates on a real-time response basis. The value of these specific tasks will be discussed in Part III.

3. State Monitoring Systems

The increasing frequency and severity of cyberattacks has prompted state legislatures to pass a litany of statutes ranging from identity theft and trade secrets legislation to data breach notification laws.[109] Out of this legislative activity, states with prominent cyber-related industries have dedicated substantial resources to preventing and enforcing cybercrime.[110]

In September 2009, Massachusetts Attorney General Martha Coakley announced the opening of a state-of-the-art, Boston-based Computer Forensics Lab.[111] The new unit, part of Coakley's Cyber Crime Initiative, receives its funding from the U.S. Department of Justice and seeks to develop a

[107] EXEC. OFFICE OF THE PRESIDENT, *supra* note 106 ("This approach, called EINSTEIN 3, will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving these Executive Branch networks. . . . It will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense.").

[108] *Id*. ("The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with Federal Departments and Agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and, when deemed necessary by DHS, to send alerts that do not contain the content of communications to the National Security Agency . . . so that DHS efforts may be supported by NSA exercising its lawfully authorized missions."); *see also* Nojeim, *supra* note 106, at 123.

[109] *See* Pinguelo & Muller, *supra* note 102, at 150 ("Also listed are statutes that deal with identity theft, trade secrets, and providing notifications to consumers upon IT data breaches, since each go hand-in-hand with the activities of cybercriminals."). This Note does not consider a large number of other computer-related laws that have been passed on issues such as online child pornography, cyberbullying, cyberstalking, child protection registry acts, and other morality-based computer laws. *See id*. For an exhaustive list of every state law on cybercrime through early 2011, see *id*. at 151.

[110] *See infra* notes 111-117 and accompanying text.

[111] Jeff Bone, *Massachusetts Attorney General Announces Opening of New Computer Forensics Lab*, FOLEY HOAG LLP (Sept. 22, 2009), http://www.securityprivacyandthelaw.com/2009/09/articles/cybersecurity-cybercrime/massachusetts-attorney-general-announces-opening-of-new-computer-forensics-lab/.

cybercrime information sharing program within the state.[112] Two years later in 2011, Massachusetts opened its Advanced Cyber Security Center, an entity that brings together stakeholders in cybersecurity from the government, industry, and academia.[113] Private sector participants claim that the largest benefits of the Security Center are collaboration, cooperation, and coordination.[114] One participating private sector executive even stated that data breach notification laws have not gone far enough to mitigate the damage of cyberattacks, and that for any positive change to be made, companies would need to share information with one another on every intrusion they face.[115]

Meanwhile, in December 2011, California – home of Silicon Valley – created a new eCrime Unit under its Justice Department to combat technology crimes.[116] Significantly, the unit well-resourced, being comprised of twenty investigators and prosecutors charged with investigating, among other things, identity theft.[117] As explained earlier, identity theft often constitutes primary or collateral damage in hacktivist and non-hacktivist cyberattacks.[118]

4. International Coalitions

Because cyberattacks can be carried out from anywhere on the planet with an Internet connection, global cybersecurity experts have begun coordinating international defenses and strategies in the past decade. In 2001, the Council of Europe – a coalition of forty-seven European states organized in 1949 for the purpose of promoting human rights, democracy, and the rule of law throughout Europe – drafted the Budapest Convention on Cybercrime, which is open to accession by any country.[119] The only international treaty to standardize cybercrime investigation, defense, and coordination tactics amongst its members, the Convention entered into force on July 1, 2004, and has since been ratified by thirty-seven countries, including the United States.[120]

---

[112] *Id*.

[113] Rodney H. Brown, *New Cyber Security Center Launches to Help Halt Hackers*, MASS HIGH TECH (Sept. 20, 2011), http://www.masshightech.com/stories/2011/09/19/daily21-New-Cyber-Security-Center-launches-to-help-halt-hackers-.html.

[114] *Id*. ("At panels throughout the day, the theme of cooperation was hammered home. [One panel leader] brought up the point that, while regulations have forced companies to disclose successful attacks against their IT infrastructure, knowing that won't suffice. Companies need to tell each other about every attempted intrusion, to be able to learn about the methods being tried and to counter them, [the panel leader said].").

[115] *Id*.

[116] Steven Musil, *California Unveils New Unit to Fight Cybercrime*, CNET (Dec. 13, 2011, 10:25 PM), http://news.cnet.com/8301-1009_3-57342718-83/california-unveils-new-unit-to-fight-cybercrime/?tag=cnetRiver.

[117] *Id*.

[118] *See supra* note 10 and accompanying text.

[119] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, 41 I.L.M. 282 (2002).

[120] *See Convention on Cybercrime*, TREATY OFFICE, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=EN

Most recently, in November 2011, sixteen EU member states and the United States, including representatives from DHS, planned and participated in Cyber Atlantic 2011, a simulated cyberattack on EU security agencies and critical infrastructure.[121] The simulation contained two comprehensive, complex drills: a stealth attack attempting to extract and publish online secret EU member state information from their respective cybersecurity agencies, and a disruption of several power plants' data acquisition systems.[122]

## II. CURRENT REFORM PROPOSALS

### A. *Obama Proposal*

Upon taking office in January 2009, President Obama declared that cybersecurity was a pressing issue.[123] By May of that year, the White House had completed a sixty-day Cyberspace Policy Review.[124] While the lengthy report may not have triggered the kind of public awareness that the President and other government officials had hoped for, it certainly initiated a steady stream of activity on Capitol Hill. More than fifty cybersecurity-related legislative proposals in two years prompted Democratic Senate Majority Leader Harry Reid to request guidance from President Obama in early 2011.[125]

On May 12, 2011, Obama released his Cybersecurity Legislative Proposal[126] (previously and hereinafter referred to as the "Obama Proposal"), which is primarily composed of four parts: (1) "Protecting the American People"; (2) "Protecting the Nation's Critical Infrastructure"; (3) "Protecting Federal

G (last visited Sept. 9, 2012); John Leyden, *UK Finally Ratifies Cybercrime Convention During Obama Visit*, REGISTER (May 25, 2011, 2:19 PM), http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/ ("The convention, which embodies a commitment to harmonise national cybersecurity laws, has been ratified by 30 countries including the US and many European states since it came into force in 2004."). The treaty has been criticized, however, for failing to gain the participation of China and Russia, two countries from which cyberattacks often emanate. *Id*.

[121] Jennifer Baker, *Simulated Cyberattack Unites EU and US Security Experts*, PCWORLD (Nov. 3, 2011, 12:40 PM), http://www.pcworld.com/businesscenter/article/243103/simulated_cyberattack_unites_eu_and_us_security_experts.html; Lee Rock, *United States and European Union Hold First-Ever Joint Cyber Tabletop Exercise*, DEP'T OF HOMELAND SECURITY (Nov. 3, 2011, 5:42 PM), http://blog.dhs.gov/2011/11/united-states-and-european-union-hold.html.

[122] Baker, *supra* note 121 ("The first was a targeted, stealth APT (advanced persistent threat) attack aimed at extracting and publishing online secret information from EU member states' cybersecurity agencies. . . . The second simulation focused on the disruption of supervisory control and data acquisition . . . systems in power generation infrastructures.").

[123] EXEC. OFFICE OF THE PRESIDENT, CYBERSPACE POLICY REVIEW, at iii (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[124] *Id*.

[125] *See* Obama Proposal Fact Sheet, *supra* note 25.

[126] OBAMA PROPOSAL, *supra* note 23.

Government Computers and Networks"; and (4) a "Framework to Protect Individuals' Privacy and Civil Liberties."[127]

Part one – Protecting the American People – includes data breach reporting requirements and criminal provisions related to computer crimes.[128] Data breach reporting laws already exist in forty-seven states,[129] and though those laws vary in particulars, they mostly require private businesses to notify consumers after a cyberattack so that consumers can take steps to protect their personal information or at least mitigate the damage if their information has been compromised.[130] The Administration's hope is that cybersecurity legislative reform will simplify and harmonize state laws so that businesses, especially those with a physical presence in several states or a presence in the online marketplace, can streamline their reporting obligations.[131] With regard to criminalization provisions, the Obama Proposal recommends that Congress implement harsher sentencing and/or monetary penalties for cyberattacks.[132] The proposal specifically recommends amending the RICO statute to include cybercrimes.[133]

Part two of the Obama Proposal – Protecting the Nation's Critical Infrastructure – contains the real substantive bulk. The Administration recommends that Congress give DHS statutory authority to provide both pre- and post-cyberattack assistance to private businesses that request it.[134] Moreover, private businesses, local government entities, and even states would be encouraged to voluntarily share information with DHS so that the volunteering participant and DHS would work together to troubleshoot or prevent cyberthreats.[135] Finally, DHS would coordinate with critical

[127] *See* Obama Proposal Fact Sheet, *supra* note 25.

[128] *Id*.

[129] *Id*. ("State laws have helped consumers protect themselves against identity theft while also incentivizing businesses to have better cybersecurity, thus helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers' personal information. The Administration proposal helps businesses by simplifying and standardizing the existing patchwork of 47 state laws that contain these requirements.").

[130] *Id*.

[131] *Id*. ("The Administration proposal helps businesses by simplifying and standardizing the existing patchwork of 47 state laws that contain these requirements.").

[132] *Id*. ("The Administration proposal thus clarifies the penalties for computer crimes, synchronizes them with other crimes, and sets mandatory minimums for cyber intrusions into critical infrastructure.").

[133] *Id*.

[134] *Id*. ("However the lack of a clear statutory framework describing DHS's authorities has sometimes slowed the ability of DHS to help the requesting organization. The Administration proposal will enable DHS to quickly help a private-sector company, state, or local government when that organization asks for its help. It also clarifies the type of assistance that DHS can provide to the requesting organization.").

[135] *Id*.

infrastructure operators, whose systems are increasingly being managed online as a result of market forces,[136] to spot the most significant cyberthreats and vulnerabilities. The critical infrastructure operators, after their initial consultation with DHS, would then independently develop their own frameworks for addressing those threats and vulnerabilities and make those frameworks subject to a third-party commercial auditor's risk assessment.[137] Should this process fail to yield adequate frameworks in the opinion of DHS, then DHS would retain the authority to modify and strengthen the arrangement.[138]

Part three of the Obama Proposal – Protecting Federal Government Computers and Networks – outlines the Administration's recommendation that DHS formalize its role as chief manager of cybersecurity for the federal government's civilian computers and networks.[139] Additionally, the proposal would allocate resources and funding to DHS for the purpose of recruiting and hiring cybersecurity personnel.[140] Finally, this part seeks to permanently authorize DHS to oversee cyber-intrusion prevention systems for federal executive branch computers.[141]

Finally, part four – a Framework to Protect Individuals' Privacy and Civil Liberties – ensures that entities that choose to voluntarily share information with DHS under part two of the proposal receive immunity for any incriminating information contained within the cybersecurity disclosure.[142] The Administration would require that DHS seek the approval of the Attorney General before any disclosed information is used by DHS or other criminal law enforcement agency for non-cybersecurity-related purposes against the disclosing entity.[143]

### B. *Republican Task Force Proposal*

Just as the Obama Proposal draws strength from the political status of its author, the Republican Task Force Proposal is prominent because it is backed by more political capital than other cybersecurity proposals, at least on the right side of the aisle. The twelve-member Task Force was organized by

[136] *Id*.

[137] *Id*.

[138] *Id*.

[139] *Id*.

[140] *See id*. ("The recruitment and retention of highly-qualified cybersecurity professionals is extremely competitive, so we need to be sure that the government can recruit and retain these talented individuals.").

[141] *Id*.

[142] *Id*.

[143] *Id*. ("All monitoring, collection, use, retention, and sharing of information are limited to protecting against cybersecurity threats. Information may be used or disclosed for criminal law enforcement, but the Attorney General must first review and approve each such usage.").

House Speaker Boehner and is led by Texas Congressman Mac Thornberry, the first member of Congress to advocate for the creation of the Department of Homeland Security.[144]

The October 2011 Task Force Proposal is split into four issues: (1) "Critical Infrastructure and Incentives"; (2) "Information Sharing and Public-Private Partnerships"; (3) "Updating Existing Cybersecurity Laws"; and (4) "Legal Authorities".[145] Issue one – Critical Infrastructure and Incentives – recommends that Congress adopt "a menu of voluntary incentives to encourage private companies to improve cybersecurity,"[146] including tax breaks, grant funding, and compliance waivers upon the creation of standards within the business.[147] The Task Force prefers the incentive-based approach to a regulation-based approach, stating that Congress should only consider "*carefully targeted* directives for *limited* regulation of *particular* critical infrastructures to advance the protection of cybersecurity at these facilities using *existing* regulators."[148] Thus, even within the high-risk realm of critical infrastructure the Task Force proposes piecemeal, rather than sweeping changes.[149]

Issue two – Information Sharing and Public-Private Partnerships – suggests that a new, non-governmental "clearing house" should be created to facilitate active sharing between private entities and the government.[150] The non-governmental agency would "improve security and . . . expand information

[144] *Biography*, U.S. CONGRESSMAN MAC THORNBERRY, http://thornberry.house.gov/Biography/ (last visited Sept. 9, 2012). Interestingly, Thornberry proposed the creation of DHS more than six months before the September 11, 2001, terrorist attacks. *Id*. Of course, the legislation which in fact created DHS – the Homeland Security Act – was not enacted until a year after 9/11. *See Creation of the Department of Homeland Security*, DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/creation-department-homeland-security (last visited Sept. 9, 2012).

[145] *See* REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 4.

[146] *Id*. at 7.

[147] The hope here is that Congress would allow businesses and industries that adopt cybersecurity standards to receive a waiver for any overlapping (or nearly overlapping) privacy and security requirement under other laws, like Sarbanes-Oxley Act of 2002, the Health Information Portability and Accountability Act of 1996, or the Gramm-Leach-Bliley Act. *See id*. at 8 ("Congress could require the Administration to coordinate with critical infrastructure sectors to develop strong performance standards that, if a company was found compliant with the new standard, would satisfy the information security/privacy protections of [other laws]. A company would be encouraged to implement stronger security standards by allowing it to save money and time by avoiding multiple audits from multiple regulators.").

[148] *Id*. at 9 (emphasis added).

[149] The Task Force cites nuclear power, electricity, chemical plants, and water treatment facilities as specific types of critical infrastructure where additional direct regulation may be warranted. *Id*.

[150] *Id*. at 10.

sharing to detect and mitigate cyber attacks in real time before they reach their target."[151] The Task Force prefers a non-governmental agency, as opposed to DHS, in the information-sharing role because "[t]here is substantial and understandable concern with the government monitoring private networks," insofar as that monitoring could lead to unintended liability for the private entities and, more abstractly, represent an unwarranted encroachment of government into the private sphere.[152] The proposal additionally states: "Change occurs so fast in this area that attempts to directly regulate a specific cybersecurity solution will be outdated by the time it is written."[153] Similar to the Obama Proposal, any private entities that ultimately share information with the non-governmental clearing house would receive immunity from liability for the information shared beyond the cybersecurity capacity.[154]

Issue three – Updating Existing Cybersecurity Laws – targets FISMA, the CFAA, and RICO as federal statutes that must be updated if cybersecurity reform is to be achieved.[155] The Task Force believes that FISMA should be changed from its current form, which is little more than an "inefficient checklist" that focuses on procedure rather than outcomes and often produces legally compliant but "extremely poor" cybersecurity practices.[156] The Task Force would extend the scope of the CFAA to include at least critical infrastructure networks – an interpretation that has only been informally applied by courts – or even all private network computers with varying levels of criminal penalties attached.[157] Finally, the Task Force would make the same changes to RICO as the Obama Proposal. It would include computer crimes within the scope of RICO's organized crime activities.[158]

Issue four – Legal Authorities – does not offer any concrete recommendations, but rather poses critical questions to be answered by Congress in enacting legislation.[159] Some of the more pertinent questions

[151] *Id*.

[152] *See id*. at 11.

[153] *Id*. at 6.

[154] *Id*. ("For those private sector entities that voluntarily participate in this new entity, Congress should provide some level of liability protection from lawsuits that result from an action to address malicious activity based upon information received as a member of the entity."); *see also* OBAMA PROPOSAL, *supra* note 23, at 28.

[155] REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 13.

[156] *Id*.

[157] *Id*. at 16.

[158] *Id*. at 14 ("Congress should also change . . . RICO . . . to include computer fraud within the definition of racketeering; provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information; expand penalties for conspiracies to commit computer fraud and extortion attempts involving threats to access computers without authorization; provide for forfeiture of property used to commit computer fraud; and require restitution for victims of identity theft and computer fraud.").

[159] *Id*.

include, "What is the responsibility and/or authority of the federal government to defend a private business when it is attacked in cyberspace?" and "How should we use the full range of instruments of national power and influence to discourage bad actors in cyberspace?"[160]

The Task Force concludes by making tertiary recommendations similar to those of the Obama Proposal, such as providing for elevated attention to recruitment, retention, and training of government cybersecurity talent, and increasing overall research and development investments.[161]

## III. THE CYBERSECURITY REFORM SOLUTION

### A. *Similarities in the Reform Models*

In order to be effective in either the short- or long-term, any cybersecurity reform legislation must contain some key elements. Fortunately, both the Obama Proposal and the Task Force Proposal contain many of these provisions, including those related to criminalization, data breaches, personnel recruitment, and liability protections.[162]

#### 1. Amending Criminal Statutes

Both proposals endorse an update of two federal criminal statutes: the CFAA and RICO.[163] The CFAA, again, is the primary statute under which computers connected to a federal interest (whether directly or tangentially) are protected by criminal law from "trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud."[164] The Task Force Proposal recommends that the definition of protected computers "should be extended to cover critical infrastructure with attached criminal penalties . . . [and] could also be expanded to cover all private sector computers with differing criminal penalties."[165] The Task Force Proposal placates the critics of CFAA expansion[166] by stating that the CFAA should be "narrowly focused to avoid unintended liability beyond computer hacking."[167] Meanwhile, the

[160] *Id.*

[161] *Id.*

[162] *See generally* OBAMA PROPOSAL, *supra* note 23; REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23.

[163] *See* OBAMA PROPOSAL, *supra* note 23, at 2; REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 14.

[164] *See* DOYLE, *supra* note 96, at 1 ("It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision; instead it fills cracks and gaps in the protection afforded by other state and federal criminal laws.").

[165] *See* REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 14.

[166] *See generally* Skibell, *supra* note 98 (criticizing Congress for failing to draw a clear line between serious and petty computer crimes in increasing criminal penalties).

[167] *See* REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 14.

Obama Proposal takes a more explicit stance on these issues. The Administration would excise the jurisdictional provisions from the CFAA, which requires that the crimes be against computers affecting interstate or foreign commerce, or alternatively, used by or for the federal government.[168] Thus, under the Obama Proposal, the CFAA amendments would extend the statute to cover private sector computers as well.[169] The Obama Proposal also increases the sentencing guidelines for related offenses.[170]

Ultimately, both proposals seem comfortable making one CFAA-related recommendation: expanding the scope of crimes that currently constitute CFAA violations. In the first few iterations of the CFAA, the jurisdictional element – that the computers affected by the crime had to be either engaged in interstate or foreign commerce, or used by or for the federal government – was a practical result of the fact that a large percentage of private computers lacked an Internet connection, making computer use generally more personal in nature.[171] With the expansion of the Internet however, every person who purchases songs from iTunes can be said to be engaging in interstate commerce. Thus, the expansion in scope of the CFAA simply reflects the growing interconnectedness of computer use. The changes in this regard of both the Task Force Proposal and the Obama Proposal are welcome.[172]

However, only the Obama Proposal takes the further step of explicitly endorsing increased criminal penalties for CFAA violations. While increased criminal penalties may be solely justified by a retributive punishment theory due to the historical increase in damage of the average cyberattack,[173] they can also be solely justified on a deterrence theory.[174] Currently, hacking behavior

---

[168] *See* OBAMA PROPOSAL, *supra* note 23, at 2.

[169] *Id*.

[170] *Id*. at 3 (proposing increasing fraud-related penalties from ten to twenty years, one to three years, and five to ten years).

[171] *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1565 (2010) (explaining that the 1986 expansion of CFAA liability to computers with a "federal interest" did not have a major practical effect because "when use of the Internet remained in its infancy, few crimes would be included in [the Act's] reach").

[172] *See* Skibell, *supra* note 98, at 934 ("The likelihood of being prosecuted under the CFAA is so remote that higher penalties will not sufficiently impact the decision calculus of foreign crackers[, who are one of the two groups, along with cyber-terrorists,] least likely to be influenced by the [USA PATRIOT Act] changes.").

[173] Matthew Haist, *Deterrence in a Sea of "Just Deserts": Are Utilitarian Goals Achievable in a World of "Limiting Retributivism"?*, 99 J. CRIM. L. & CRIMINOLOGY 789, 890-91 (2009) ("Retributivists . . . base the degree of punishment solely on the desert of the wrongdoer. Minor wrongdoing warrants only minor punishment, grave wrongdoing warrants grave punishment.").

[174] *Id*. at 891 (explaining that, as opposed to a retributive theory of punishment which looks to the seriousness of the crime, a deterrence-based theory of punishment would set a high criminal penalty for jaywalking in a jurisdiction where the incident of jaywalking was frequent, and would alternatively set a low criminal penalty for jaywalking in a jurisdiction

is characterized by a laissez-faire attitude toward liability and legality.[175] Stigmatizing illegal computer activity with harsher sentencing and broader enforcement may change those behavioral norms in the long run.[176] Combining this normative argument with the fact that the damage done by cyberattacks individually and cumulatively continues to increase should persuade Congress to adopt the Obama Proposal's stance on the CFAA.

Additionally, both the Task Force and Obama Proposal recommend making computer crimes predicate offenses to RICO violations.[177] This change is both a helpful and necessary one for cybersecurity reform, and it would surely help target Anonymous. Though Anonymous both brands itself and has been characterized as a disaggregated collection of individuals, recent investigative reports have shown that its meritocracy-based culture necessarily means that some members elevate in reputation over time and inherit a pseudo-leadership authority over more casual, less-skilled members of the group.[178] Thus, even Anonymous begins to resemble the kind of criminal organization that traditionally falls within RICO's statutory purview. Certainly then, more organized cybercrime groups, like small bands of individuals working in close physical proximity to one another, would be liable as well.

2. Data Breach Notification

Both the Obama and Task Force Proposal recommend that the patchwork of state data breach notification laws be harmonized under a federal standard.[179] While most of this Note and the two proposals cover cybersecurity as it pertains to proprietors and violators of computer networks, any comprehensive cybersecurity reform must also contain a consumer-protection element. This

where the incident of jaywalking is infrequent).

[175] Derek E. Baumbauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1097 (2011) ("The term hacker . . . connotes not only technical skill, but also a disregard for rules and, at times, a malicious enjoyment in finding flaws and wreaking havoc.").

[176] *See* Skibell, *supra* note 98, at 936 (recognizing that "[o]ne explanation for the unabated increase in computer crime is that not enough time has passed to see the effects of deterrence on computer criminals . . . [and thus,] it is unfair to assess the success or failure of substantial penalties until a generation has matured under them").

[177] *See* OBAMA PROPOSAL, *supra* note 23, at 2; REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 14.

[178] *See* Coleman, *supra* note 61; *see also Anonymous 101: Part III*, *supra* note 82 (stating that a private security consultant, who claimed that the members of Anonymous "secretly obeyed" a group of leaders that he had identified, had "walked into Anonymous' Vatican and declared their Virgin Mary a whore").

[179] *See* OBAMA PROPOSAL, *supra* note 23, at 18 ("The provisions of this title shall supersede any provision of the law of any State, or a political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data . . . ."); REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 12 ("Congress should address data breach notification legislation that simplifies compliance for businesses and protects the sensitive personally identifiable information of individuals.").

element is directly embodied in data breach notification laws.[180] This change is logical insofar as an ever-increasing number of American companies (especially those that would be targets of cyberattacks by Anonymous or cyberterrorists) conduct business online in greater volume, and therefore are subject to the laws of many states.[181] Simply put, it no longer makes sense to have forty-seven different standards in a single marketplace.[182]

3. Personnel Recruitment

Both proposals emphasize the need for the federal government to broaden its cybersecurity personnel recruitment efforts. Fortunately, much has already been done. In May 2009, President Obama established the National Institute for Cybersecurity Education (NICE).[183] NICE, co-led by DHS, the Department of Education, the Office of Science and Technology Policy, the Office of Personnel Management, the Department of Defense, and the Office of the Director of National Intelligence, launched a four-prong strategy to "build a cyber savvy nation through training, awareness, Kindergarten through post-graduate educational programs, and professional development for federal security professionals."[184] NICE has consistently pursued this mission since its inception. For example, DHS held its eighth annual National Cyber Security Awareness Month in October 2011, a main goal of which was "to train the next generation cyber workforce."[185] To meet that goal, DHS targeted a wide array of the population as prospective employees: K-12 students, college students, and private sector partners.[186] Additionally, the U.S. Cyber Challenge – a coalition formed by the Department of Defense with the Air Force Association, Center for Internet Security, and National Collegiate Cyber Defense Competition – hosted a series of computer-skills contests in 2011 to identify talented cybersecurity prospects.[187]

---

[180] See *supra* Part II.

[181] From 2007 to 2011, holiday-season online-shopping sales have increased by nearly fifty percent, from $16 billion to $30 billion. *See* Kate Gibson, *Holiday-Season Online Sales Up 15% from Year Ago*, WALL ST. J. (Dec. 18, 2011), http://articles.marketwatch.com/2011-12-18/industries/30730828_1_free-shipping-promotions-comscore-holiday-season; Amy Hoak, *Holiday Online Spending up 18%*, WALL ST. J. (Dec. 16, 2007), http://articles.marketwatch.com/2007-12-16/news/30786568_1_online-spending-comscore-chairman-online-sales.

[182] *See supra* notes 129-131 and accompanying text.

[183] *See National Initiative Cybersecurity Education (NICE)*, NAT'L INST. OF STANDARDS & TECH., http://www.nist.gov/itl/csd/nice.cfm (last updated May 25, 2012).

[184] *Id*.

[185] *National Cyber Security Awareness Month*, DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/files/programs/gc_1158611596104.shtm (last visited Sept. 9, 2012).

[186] *See Shaping the Future of Cybersecurity Education and Workforce Development*, DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/files/programs/cyber-education-workforce-development.shtm (last visited July 28, 2012).

[187] *See generally Welcome to U.S. Cyber Challenge*, NAT'L BOARD INFO. SECURITY

Any cybersecurity reform legislation should make these arrangements permanent. The Secretary of Homeland Security should be given the authority and resources to initiate new recruitment and education campaigns and extend the scope of existing ones. The rationale for this investment is two-fold. First, in a world of ever-increasing connectivity, more cybersecurity will be needed to manage that connectivity, so there will be a parallel increase in demand for cybersecurity jobs. Second, through enhancing its presence in recruitment and education, the federal government can attract those individuals to fill cybersecurity jobs who might otherwise have joined the ranks of Anonymous or other hacker groups. Granted, persons who are anti-government or even apathetic towards government may not be persuaded by the government's recruitment efforts. But for those young people who exhibit exceptional computer skills and seek a community that utilizes and appreciates those skills, the recruitment and education campaigns will certainly aid the federal government in its mission.

4. Liability Protection

Both the Task Force and Obama Proposal contain liability protections for any private entities sharing cybersecurity information with the government.[188] Without these protections, a private entity might resist voluntary information-sharing out of concern that the benefits to be gained by cybersecurity aid from the government would not cover the cost of liability resulting from incriminating evidence contained within the disclosure. Thus, the most practical solution, recognized by both proposals, is to provide civil liability immunity to those private entities that share cybersecurity information with the federal government.[189]

### B. *Differences in the Reform Models*

The differences between the Task Force Proposal and Obama Proposal are few but significant. First, the Task Force Proposal reveals a hesitation to endorse any legislative package that contains more than a modest level of federal government involvement in cybersecurity.[190] This hesitation is primarily motivated by two beliefs: (1) the need for fiscal savings;[191] and (2)

EXAMINERS, https://www.nbise.org/uscc/ (last visited July 28, 2012).

[188] *See* OBAMA PROPOSAL, *supra* note 23, at 28; REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 9-11.

[189] *See* Nojeim, *supra* note 106, at 128 ("Currently, companies have little incentive to report network vulnerability information to the government. Who, after all, would voluntarily tell anyone that the lock on their back door is broken? Thus, additional measures should be considered to encourage the sharing of vulnerability information. . . . Companies could receive immunity from liability if they disclose vulnerabilities.")

[190] *See supra* text accompanying notes 146-48.

[191] *See* REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 5 ("With the current fiscally constrained environment, any new or expanded programs and initiatives need to

the superiority of market incentives over direct regulation for private entities.[192] This approach contrasts sharply with the Obama Proposal, which envisions considerable investment in cybersecurity infrastructure coupled with directly mandated cybersecurity benchmarks for the private market.

Second, the Task Force Proposal would create a non-governmental agency to establish cybersecurity standards for private entities, where the Obama Proposal would delegate that authority to DHS.[193] Moreover, while the Task Force Proposal standards would be voluntary, the standards promulgated by DHS under the Obama Proposal would be mandatory for covered entities.[194]

### C. *The Rationale for Charting a DHS-Centric Course for Reform*

So long as legislators are in agreement that the threat of cyberattacks is real and imminent, a DHS-centric reform model is warranted for several reasons. First, insofar as the recent wave of cyberattacks has undermined consumers' and businesses' confidence in the web,[195] the government should take a proactive role in restoring that confidence. This proactive role is a proper one for the federal government to take so long as the American people continue to believe that the government is responsible for addressing major economic vulnerabilities. Voluntary incentives are decidedly less proactive than direct regulation, therefore legislators might fail to persuade consumers and businesses to remain in the online marketplace if the Task Force Proposal is adopted in large part.[196]

---

reflect fiscal realities.").

[192] "Legislative packaging and vehicles must, of course, be decided by Leadership, but we are generally skeptical of large, 'comprehensive' bills on complex topics . . . ." *Id*. at 5. "We believe Congress should adopt a menu of voluntary incentives to encourage private companies to improve cybersecurity." *Id*. at 7. "There may be instances where additional direct regulation of an industry that is already highly regulated (nuclear power, electricity, chemical plants, water treatment) may be warranted. [But] Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity at these facilities using existing regulators." *Id*. at 9.

[193] *See* OBAMA PROPOSAL, *supra* note 23, at 19-32 (detailing the new powers the proposal would grant to DHS); REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 7 (indicating that the proposal favors reliance on the National Institute of Standards and Technology to help create non-binding standards through a public-private partnership).

[194] *See* OBAMA PROPOSAL, *supra* note 23, at 21-26; REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 7-8.

[195] Larry Dignan, *LulzSec, Anonymous and Hacktivism: Crappy Security Has Caught Up with Us*, ZDNET (June 16, 2011, 8:03 AM), http://www.zdnet.com/blog/security/lulzsec-anonymous-and-hacktivism-crappy-security-has-caught-up-with-us/8777 ("What happens when the CIA, Senate, various gaming sites, Citibank and a bevy of others are hacked on a regular basis by various groups with one-liners on Twitter and no formal organization? You lose confidence in the Internet and the data passing through it.").

[196] *See* Nicole Perlroth, *Even Big Companies Cannot Protect Their Data*, N.Y. TIMES BITS (Jan. 17, 2012, 9:02 PM), http://bits.blogs.nytimes.com/2012/01/17/even-big-compan

Second, Congress has, in the past, shown a willingness to handle matters of national security through direct regulation rather than market incentives. In the wake of 9/11, it created an entire federal agency – the Department of Homeland Security – to secure the safety of the country,[197] and with it sub-agencies like the Transportation Security Administration (TSA).[198] Congress did not leave improvements in airport security to market incentives; rather, Congress promulgated and provided for the enforcement of new standards.[199] Presumably, two considerations motivated that decision: (1) a need for immediate change in security practices; and (2) a need to restore confidence in security. Of course, there has been no cyberattack that approaches the magnitude of 9/11,[200] but both of these concerns are present in the cybersecurity arena.

Third, market-incentive-based legislation like the Task Force Proposal is better suited for early-adoption scenarios and not immediate-change scenarios; the former model is dependent upon voluntary, rather than mandatory, participation in the regulatory scheme. Voluntary legislative schemes produce slower adoption rates (or at least slower than those of mandatory regulation) and slower adoption rates necessarily yield weaker cybersecurity in the interim. Weak cybersecurity for any length of time moving forward is an undesirable result if there is a consensus that the threat of a harmful cyberattack is real and imminent.

As it so happens, most are in agreement on that point. One prominent voice is Michael Chertoff, the former Secretary of Homeland Security under President George W. Bush. Chertoff recently wrote that the need for cybersecurity would soon outstrip the need for more traditional

ies-cannot-protect-their-data/ (quoting a member of the National Cyber Security Task Force as stating, "There are a lot of people that are going to seriously reconsider before they purchase anything else on the Internet").

[197] *Creation of the Department of Homeland Security*, *supra* note 144.

[198] *Our History*, TRANSP. SECURITY ADMIN., http://www.tsa.gov/research/tribute/history.shtm (last visited July 28, 2012).

[199] Francine Kerner & Margot Bester, *The Birth of the Transportation Security Administration: A View from the Chief Counsel*, 17 AIR & SPACE LAW. 1, 21 (2002) ("[The Aviation and Transportation Security Act] grants TSA comprehensive powers to protect transportation security. TSA has the authority to . . . oversee the implementation and adequacy of security measures at airports and other transportation facilities.").

[200] While there has yet to be a cyberattack rivaling the impact of 9/11, politicians have begun alluding to the possibility of such an attack in an effort to drum up support for expedient passage of legislation. *See Securing America's Future: The Cyber Security Act of 2012: Hearing on S. 2105 Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 112th Cong. (2012) (statement of Sen. Joseph Lieberman, Chairman, S. Comm. on Homeland Sec. and Gov't Affairs) (unprinted prepared opening statement available at http://www.hsgac.senate.gov/download/?id=aef223b5-a625-4215-ae01-ff3e7d0f6390) ("To me it feels like Sept. 10, 2001. The question is whether we will act to prevent a cyber 9/11 before it happens instead of reacting after it happens.").

counterterrorism efforts on behalf of the federal government.[201] Moreover, in a few specific instances, weak cybersecurity has been a primary justification used by Anonymous in selecting the victims of its cyberattacks.[202] Thus, the Task Force Proposal would fail to expedite wholesale improvements in cybersecurity and may induce more cyberattacks from hacktivists than would a direct-regulation reform model.

Some commentators, however, see an uncomfortable parallel between the doomsday rhetoric surrounding calls for cybersecurity reform and past instances in which the American public has been led to believe that great danger lurked around every corner. Jerry Brito and Tate Watkins argue that cybersecurity rhetoric since 2008 mirrors the "weapons of mass destruction" (WMD) rhetoric employed by the Bush administration circa 2001, and therefore the lawmakers and the public alike should be hesitant to rush to ill-advised conclusions.[203]

While it is true that politicians have used apocalyptic language both then[204] and now[205] to describe the potential for attacks, the analysis of Brito and

---

[201] *Securing America's Future: The Cyber Security Act of 2012: Hearing on S. 2105 Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 112th Cong. (2012) (statement of Michael Chertoff, former Sec'y of the Dep't of Homeland Sec.) (unprinted prepared opening statement available at http://www.hsgac.senate.gov/download/cybersecurity-support-statement-former-dhs-secretary-michael-chertoff) [hereinafter Chertoff Statement] ("In my opinion, these cyber threats represent one of the most seriously disruptive challenges to our national security since the onset of the nuclear age sixty years ago."). In his statement, Chertoff quotes the Director of National Intelligence, the nation's most senior intelligence advisor to the President, and the Director of the FBI as subscribing to the same belief. *See id.* ("The Director of National Intelligence Jim Clapper, our nation's most senior intelligence advisor to the President, elevated the discussion of cyber space in his recent testimony on the worldwide threat assessment calling it 'one of the most challenging [threats] we face.'"). Chertoff's former role as the Secretary of Homeland Security under President Bush should eliminate any Republican-fueled conspiracy theories that the playing up of cybersecurity reform is yet another instance of Democratic politicians' desire to increase federal bureaucracy and spending. Chertoff's testimony lends support to the notion that the need for urgent cybersecurity reform is a non-partisan issue.

[202] *See* Dysart, *supra* note 64, at 42 (detailing how Anonymous hacked into the computer networks of HBGary, a company specializing in computer security, and published their contents on the web, thereby exposing the company's hypocrisy and mocking its lack of actual cybersecurity).

[203] Jerry Brito & Tate Watkins, *Loving the Cyber Bomb?: The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L. SECURITY J. 39, 40-55 (2011).

[204] *See* Vice President Dick Cheney, Remarks by the Vice President to the Veterans of Foreign Wars 103d National Convention (Aug. 26, 2002), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2002/08/20020826.html ("But we now know that Saddam has resumed his efforts to acquire nuclear weapons. . . . Simply stated, there is no doubt that Saddam Hussein now has weapons of mass destruction. There is no doubt he is amassing them to use against our friends, against our allies, and against us.").

[205] *See* RICHARD A. CLARKE & ROBERT K. KNAVE, CYBER WAR 67-68 (2010) (asserting

Watkins suffers from four serious defects. First, history revealed the Bush Administration was wrong, and perhaps intentionally so, about its assertion that Saddam Hussein possessed weapons of mass destruction immediately after 9/11. Thus, the Brito and Watkins benefit immensely from hindsight and reader sympathy in choosing that example as the most apt comparison for the current cybersecurity debate.

Second, the range of responses to each threat – weapons of mass destruction and cyberattacks – inherently differ. Post-9/11, the belief that Saddam Hussein possessed weapons of mass destruction was used to conclude that the United States should preemptively invade Iraq, overthrow its government, and attempt to bring stability to an unruly region. In contrast, the belief that a faceless enemy may launch a cyberattack to cripple the US economy and critical infrastructure is used to conclude that our government should consider strengthening its cybersecurity defenses. Responding to the latter is primarily defensive in nature, while the U.S. response to the former was offensive.[206]

Third, the source of the rhetoric in each scenario is significant. The Bush Administration, primarily Vice President Dick Cheney, was at the forefront of the WMD campaign.[207] The Obama Administration has certainly endorsed the need for greater cybersecurity; however, it is not the only voice in the debate. Rather, President Obama is joined by a chorus of bipartisan commentators in calling for reform.[208]

Last, and most important, Brito and Watkins attempt but ultimately fail to overcome credible evidence that the tools to launch a crippling cyberattack in fact exist and have already been used. Brito and Watkins are correct to cite the Stuxnet cyberattack[209] on Iranian uranium enrichment facilities as an example of infrastructure-disabling cyber capabilities,[210] yet they insist that it is "simply one data point" and "tells us nothing about the probability that such weapons could or would be used."[211] The logic of this argument could be used compel the conclusion that the United States should not have worried or continue to

that a serious cyberattack could quickly lead to famine, powerless hospitals, and train crashes nationwide).

[206] Furthermore, there was a logical gap for the Bush Administration between its rhetorical justification – ridding Iraq of WMDs – and its (unstated) foreign policy end goal – bringing democracy to Iraq through an invasion followed by a military occupation. In the cybersecurity debate, on the other hand, the rhetoric and the policy goals are one and the same: strengthening our nation's cybersecurity.

[207] *See* Dick Cheney, *supra* note 204.

[208] *See, e.g.*, REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 4.

[209] *See* Rosenbaum, *supra* note 36 ("Stuxnet exhibited virtual superpowers last fall by penetrating, taking control of, and jamming into self-destruction some 1,000 precisely calibrated uranium-refining centrifuges in Iran's Natanz nuclear facility.").

[210] Brito & Watkins, *supra* note 203, at 55-56.

[211] *Id.* at 55-56 (dismissing the hazards posed by Stuxnet-like attacks in the United States).

worry about nuclear weapons because the bombing of Hiroshima and Nagasaki at the end of World War II was "simply one data point" – the fact that others possess nuclear weapons indicates nothing about the United States' potential exposure to or need to prepare for a nuclear attack.

Separately, there are several reasons to believe that the Task Force Proposal's limited regulation model may be more about toeing partisan lines than measured policy judgments. Three pieces of evidence support this conclusion. First, for politically cynical observers, the Task Force Proposal was drafted on the heels of the hard-fought, rhetorically loaded, and often petty July 2011 battle between Democrats and Republicans over increasing the national debt ceiling.[212] For rank-and-file Republicans at the time, supporting any legislative proposal with new spending, like the Obama Proposal with its DHS-oriented focus, was a politically disfavored, even taboo, move. Pieces of rhetoric in the Task Force Proposal hint at this sentiment: "With the current fiscally constrained environment, any new or expanded programs and initiatives need to reflect fiscal realities. We must keep in mind the potential fiscal impact on both the public and private sectors."[213] It is difficult to remember any similar overt hesitation to pass national-security-based legislation due to cost post-9/11, notwithstanding the different economic climate.[214]

Second, in one major Republican-led cybersecurity bill proposed after the October 2011 Task Force recommendations, the Promoting and Enhancing Cybersecurity Information Sharing Effectiveness Act (PrECISE Act),[215] DHS's role in reform would be increased beyond that in the Task Force Proposal, though still short of its role in the Obama Proposal. The PrECISE Act is faithful to the Task Force Proposal in one respect – it "stops short of mandating new security standards for sectors deemed critical to national security."[216] Those standards must be voluntarily initiated by critical

---

[212] Carl Hulse & Helene Cooper, *Obama and Leaders Reach Debt Deal*, N.Y. TIMES (July 31, 2011), http://www.nytimes.com/2011/08/01/us/politics/01FISCAL.html?pagewanted=all (detailing the agreement reached between the parties concerning the debt ceiling increase); Ed O'Keefe, *How Much Did Last Year's Debt Fight Cost Taxpayers?*, WASH. POST, (July 24, 2012, 6:00 AM), http://www.washingtonpost.com/blogs/2chambers/post/how-much-did-last-years-debt-fight-cost-taxpayers/2012/07/23/gJQAD5I94W_blog.html ("The debt fight prompted Standard & Poor's to drop the nation's AAA credit rating and blame 'political brinkmanship' for making the U.S. government's ability to manage its finances 'less stable, less effective and less predictable.'").

[213] *See* REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 5.

[214] *See, e.g.*, Kerner & Bester, *supra* note 199, at 21 (detailing the powers granted to the TSA despite the impact on the government fisc).

[215] H.R. 3674, 112th Cong. (2011). The bill was sponsored by House Cybersecurity Subcommittee Chairman Daniel Lungren (R-Cal.) and was cosponsored by nine more Republican Representatives and a lone Democrat. *Id.*

[216] Gautham Nagesh, *House Cybersecurity Bill Would Establish Federal Overseer*, THE HILL (Dec. 16, 2011, 12:31 PM), http://thehill.com/blogs/hillicon-valley/technology/1999

infrastructure industry members themselves.[217] However, the bill would put DHS in charge of assessing and defending against critical infrastructure cybersecurity risks and determining the best way to mitigate them.[218] In doing so, the bill's authors have more closely aligned themselves with the White House vision for an active DHS, despite leaving it "unclear how much authority DHS would have to enforce its security standards."[219] Regardless of the specifics, if DHS has the authority to enforce standards under the PrECISE Act, then the bill marks an important departure from the Task Force Proposal's incentive-based and purely voluntary model. This departure is made more significant by the timing of the bill, which arrived after the recommendations of the Task Force, and the sponsors' party affiliations; ten of its eleven sponsors are Republican.[220]

Third, the Republican aversion to direct regulation may be partially driven by a misunderstanding of what cybersecurity standards and requirements would look like in practice. This point is underscored by provisions of a more recent cybersecurity bill, the Cybersecurity Act of 2012, produced by a bipartisan coalition of senior members from the Senate Committees on

29-house-members-introduce-cybersecurity-bill ("Like the other cybersecurity bills offered by the House GOP, the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness (PrECISE Act) encourages private firms to share information on cyber threats but stops short of mandating new security standards for sectors deemed critical to national security.").

[217] H.R. 3674 § 226(a)(1) (indicating that the Secretary can only act "upon request" and "in consultation with" agencies and private entities).

[218] *Id*. ("[T]he Secretary shall develop and conduct risk assessments for Federal systems . . . that may include threat, vulnerability, and impact assessments and penetration testing, or other comprehensive assessment techniques."). The PrECISE Act states that the Secretary of DHS shall "establish, in coordination with the Director of the National Institute of Standards and Technology and the heads of other appropriate agencies, benchmarks and guidelines for making critical infrastructure information systems more secure." *Id*. § 226(a)(7). Further, the Secretary shall "acquire, integrate, and facilitate the adoption of new cybersecurity technologies and practices in a technologically and vendor-neutral manner to keep pace with emerging . . . cybersecurity threats . . . including . . . making such technologies available to governmental and private entities that own or operate critical infrastructure information systems." *Id*. § 226(a)(3). Contrast this with the Task Force Proposal, which states: "Congress should encourage participation in the development of voluntary cybersecurity standards and guidance through non-regulatory agencies, such as the National Institute of Standards and Technology (NIST), to help the private sector improve security." REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 7. Thus, while the PrECISE Act envisions DHS to be, at the very least, a fifty percent co-participant in establishing cybersecurity standards and also authorized to update private critical infrastructure entities on emerging cyberthreats, the Task Force Proposal leaves DHS out of the picture completely.

[219] *See* Nagesh, *supra* note 216.

[220] *Id*.

Commerce, Homeland Security and Governmental Affairs, and Intelligence.[221] Sections 103 and 104 of the Act would endow the Secretary of Homeland Security with the authority to set "risk-based cybersecurity performance requirements" for designated critical infrastructure entities.[222]

These provisions should alleviate Republican concerns about a direct-regulation reform for two reasons. First, even though the Cybersecurity Act of 2012 envisions a direct-regulation model, the Act specifically requires the Secretary of Homeland Security to work hand-in-hand with private sector critical infrastructure entities in designating which entities are to be subject to the standards and also in establishing cybersecurity standards.[223] Second, the standards to be enumerated under the Act are risk-based performance requirements, rather than regulatory mandates.[224] Put another way, under the Act the Secretary of Homeland Security could not simply tell a covered critical structure entity the way in which it must reduce its cybersecurity risk, the Secretary could only require the entity to reduce its cybersecurity risk to a certain acceptable level based on outcomes. This approach avoids the undesirable (and awkward) result of the federal government "telling Microsoft and Apple how to upgrade their" their operating systems[225] and affords private entities flexibility in meeting benchmarks.[226] Former Homeland Security

[221] U.S. SENATE COMM. ON HOMELAND SEC. AND GOV'T AFFAIRS, THE CYBERSECURITY ACT OF 2012, S. 2105 – SUMMARY (2012), *available at* http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105_-summary.

[222] S. 2105, 112th Cong. §§ 103-104 (2012).

[223] *Id*. §§ 102-04.

[224] *Id*. § 104 ("The Secretary . . . shall identify or develop . . . risk-based cybersecurity performance requirements . . . [that] do not permit any Federal employee or agency to [regulate or require specific products or designs].").

[225] Paul Rosenzweig, *The Cybersecurity Carve Out – Revisited*, LAWFARE (Feb. 16, 2012, 1:29 PM), http://www.lawfareblog.com/2012/02/the-cybersecurity-carve-out-revisited/.

[226] Kenneth Corbin, *McCain, GOP Vow Alternative Cybersecurity Bill*, PCWORLD (Feb. 17, 2012, 9:38 AM), https://www.pcworld.com/businesscenter/article/250196/mccain_gop_vow_alternative_cybersecurity_bill.html ("[T]he oversight framework is narrowly drawn and gives industry players significant flexibility in achieving compliance, and [ensures] a baseline level of security in areas of critical infrastructure such as utilities the financial services sector is a decidedly pro-business stance."). Despite the flexible nature of the risk-based performance requirements in the Cybersecurity Act of 2012, some prominent Republicans have been unwilling to temper their criticism of any legislation utilizing a direct-regulation model. *See id*. (quoting Senator John McCain as stating, "If the legislation before us today were enacted into law, unelected bureaucrats at the DHS would promulgate prescriptive regulations on American businesses, . . . stymie job creation, blur the definition of private property rights and divert resources from actual cybersecurity to compliance with government mandates"). Though Republicans may lack credence to their criticisms of the Act on regulatory compliance grounds, they would still have credible reason to oppose the bill on principal of cost, at least when compared to the Republican Task Force's market-incentive model.

Secretary Michael Chertoff wrote in support of the approach taken in the Cybersecurity Act of 2012, stating that risk-based security standards for critical infrastructure and information sharing are two elements that should be emphasized in any reform package.[227] This detailed explication of the risk-based security standards mirrors the philosophy of the Obama Proposal.[228]

Fourth, the Task Force's belief that the private sector will hesitate to share sensitive information is likely overstated. Reexamining the details of the Massachusetts Advanced Cyber Security Center's opening confirms this theory. For the Center, disclosure of sensitive information was both a means to and an end of the public/private sector collaboration.[229] If competitors in Massachusetts' private sector, which is predominated by highly competitive biotech and software firms whose financial success relies upon the secrecy of intellectual property and business strategies, feel comfortable sharing information amongst each other, why would they not feel equally comfortable sharing that information with a federal agency under the agreed condition that any such shared information would be given immunity?[230] Moreover, leading technology companies, including Microsoft, Oracle, and Cisco, have come out in support of the Cybersecurity Act of 2012's direct-regulation model.[231] Their support certainly signals a willingness to share sensitive information with the federal government. More importantly, DHS itself has expressed no interest in unmitigated monitoring of the private sector, and recently voiced its desire to

[227] *See* Chertoff Statement, *supra* note 201, at 3 ("There are three areas that I believe should be emphasized as a part of any comprehensive cybersecurity legislation: (1) risk-based security standards for our critical infrastructure, (2) information sharing, and (3) liability protections.").

[228] *See supra* notes 136-37 and accompanying text.

[229] *See supra* notes 114-15 and accompanying text.

[230] *See supra* note 142 and accompanying text.

[231] *See Securing America's Future: The Cybersecurity Act of 2012: Hearing on S. 2105 Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 112th Cong. (2012) (unprinted written testimony of Scott Charney, Corporate Vice President, Trustworthy Computing, Microsoft Corp. available at http://www.hsgac.senate.gov/download/2012-02-16-charney-testimony-cyber-security) ("It is my view that the current legislative proposals provide an appropriate framework to improve the security of government and critical infrastructure systems and establish an appropriate security baseline to address current threats. Furthermore, the framework is flexible enough to permit future improvements to security – an important point since computer threats evolve over time."); Letter from Blair Christie, Senior Vice President and Chief Mktg. Officer, Cisco Systems, Inc., to Senator Harry Reid, Majority Leader, U.S. Senate (Feb. 14, 2012) (available at http://www.hsgac.senate.gov/do wnload/cybersecurity-support-letter-cisco-oracle) (sup-porting the idea that information sharing is critical to long-term cybersecurity). For a longer list of public- and private-sector supporters of the Cybersecurity Act of 2012, see Press Release, U.S. Senate Comm. on Homeland Sec. & Gov't Affairs, IT Industry, National/Homeland Defense Leaders Lend Support to Cybersecurity Act (Feb. 15, 2012), http://www.hsgac.senate.gov/media/majority-media/it-industry-national/homeland-defense-leaders-lend-support-to-cyberecurity-act.

"provide liability protections to private sector entities for sharing cybersecurity information."[232]

Fifth, by the Task Force's own rationale, direct DHS involvement in the private sector would yield benefits. The Task Force Proposal states in its "Observations" section: "We face a wide range of threats – from vandalism and petty crime to, potentially, cyber warfare and cyber terrorism, but we may not be able to tell which it is at the moment of attack."[233] This language strengthens the argument that the federal government needs to prepare for cyberattacks of all shapes and sizes. So long as both parties agree that in the future the United States stands to face a cyberwarfare attack, it would be helpful in the interim to use the private sector as training grounds, so to speak, for differentiating between and preventing relatively "harmless" attacks and more serious ones. It is conceivable that a cyberterrorist – or a hacker with intentions more serious than a "typical" hacktivist – would use rudimentary tools, such as the DDoS made popular by Anonymous, to disguise a more damaging cyberattack. Even if Anonymous's activities never escalate to cyberterrorism and instead continue to target DHS-supervised computer networks, it will be a useful exercise for DHS to distinguish between cyberthreats that are and are not acts of war.

So, in the end, what basis is there to think that DHS's involvement in cybersecurity will lead to suboptimal or inefficient standards? It cannot be that DHS is fundamentally incapable of tailoring its regulation and enforcement to particularized industries. DHS currently is the ad hoc manager of the federal government's computer networks, spanning agencies from a wide variety of economic sectors, including environmental (Environmental Protection Agency), transportation (TSA), energy (Department of Energy), and education (Department of Education).[234] Thus, the federal government has at least some experience in tailoring its cyber-standards and -monitoring to different fields, and any shortcomings in fulfilling those duties may be the result of a lack of resources and guidance from Washington on the proper scope its authority. This is the position that the Government Accountability Office (GAO) took in its December 2011 report.[235] There, the GAO found that while DHS is the lead

[232] DEP'T OF HOMELAND SEC., BLUEPRINT FOR A SECURE CYBER FUTURE 12 (2011), *available at* http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

[233] REPUBLICAN TASK FORCE PROPOSAL, *supra* note 23, at 6.

[234] William Jackson, *Industry Needs Government Help to Protect Infrastructure, GAO Study Says*, GOV'T COMPUTER NEWS (Jan. 10, 2012), http://gcn.com/Articles/2012/01/10/Critical-infrastructure-protection-GAO.aspx?admgarea=TC_SECCYBERSSEC&Page=1 ("DHS is the lead agency for both government and private-sector cybersecurity and is responsible for developing national critical infrastructure protection plans, helping the private sector in development and promotion of best security practices, and providing assistance when requested.").

[235] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-92, CRITICAL INFRASTRUCTURE PROTECTION: CYBERSECURITY GUIDANCE IS AVAILABLE, BUT MORE CAN BE DONE TO

agency responsible for public- and private-sector cybersecurity protection plans, its plans have not identified key guidance and standards in a sector-specific way, leaving plan participants confused at times over which guidelines and standards to follow.[236] The GAO recommended, therefore, that "more could be done to identify guidance and standards applicable to entities within the sectors and to promote their implementation."[237] The Obama Proposal would provide DHS with the clear-cut authority to promulgate sector-specific guidelines and standards that are currently lacking. Thus, with the backing of personnel and funding resources in a reform package, DHS will be able to improve upon its arrangement with federal government networks and forge a new working relationship with the private sector.

### D. *Why Congress Should Account for Hacktivism in Reform*

Explicitly targeting hacktivists in cybersecurity legislative reform yields two important results. First, doing so solves some underlying problems tied to the cybersecurity debate, without reference to which legislative model is passed. Second, targeting hacktivism lends direct support to the DHS-centric reform model endorsed in the Obama Proposal.

Targeting hacktivism in reform efforts will most obviously minimize a threshold problem in the larger cybersecurity debate: the large disparity between Congressional activity and public discourse. Since 2009, more than fifty cybersecurity-related bills have been proposed in Congress.[238] However, beyond easily relatable pieces of legislation, like those focusing narrowly on cyberbullying or data privacy, public awareness of the larger cybersecurity legislative effort has been largely absent.[239] As of the date of publication of this Note, neither President Obama nor his challenger Governor Mitt Romney have made cybersecurity – at least to the lay observer – into a central issue of their campaigns in the same way that national security was a central issue of the 2004 presidential election.

Perhaps the problem is that cybersecurity reform is too complex an issue to gain mainstream traction with the public. But politicians could overcome this problem if they seized upon the public's familiarity with Anonymous and Anonymous-led cyberattacks. Just as the mafia was once singled out as the

PROMOTE ITS USE (2011), *available at* http://www.gao.gov/assets/590/587529.pdf.

[236] *Id*. at 23.

[237] *Id*.

[238] *See supra* note 125 and accompanying text.

[239] Sean Lawson, *Where is the "Public Awareness" in the Cyber Security Public Awareness Act?*, FORBES (Apr. 26, 2011, 1:34 PM), http://www.forbes.com/sites/seanlawson/2011/04/26/where-is-the-public-awareness-in-the-cyber-security-public-awareness-act/ (arguing that the "poor quality of public discourse" on cybersecurity is due to "1) the lack of clear definitions of key terms and problems, 2) the inconsistent use and quality of evidence backing claims of serious cyber threats, and 3) the lack of transparency by both government and industry").

face of organized crime,[240] politicians should capitalize on Anonymous's visibility when discussing cybersecurity with the general public. This singling-out of Anonymous would not be unwarranted. According to a 2012 report published by Verizon, hacktivists (generally) overtook cybercriminals as the group responsible for the largest amount of damage resulting from cyberattacks in absolute dollar figures.[241] Moreover, Anonymous specifically has high public recognition due its reliance on social media (Twitter feeds, YouTube pages, and websites), branding mechanisms (iconic Guy Fawkes masks and naming practices), and politically-charged viewpoints in the course of conducting cyberattacks on high-profile victims. Undoubtedly, sizable sectors of the American public followed or were affected by the PayPal/Visa/MasterCard cyberattacks, the Sony outage, and the Occupy Movement protests. There is no reason why politicians should refrain from singling out a group that is already actively attracting attention to itself. Capitalizing on the public's familiarity with Anonymous when discussing cybersecurity would be a prudent strategy for politicians to stress the urgent need for cybersecurity reform and gauge the public's policy preferences toward it. Increased public awareness is especially important considering that one of the major differences between the two proposals is the amount of taxpayer money to be spent on reform.

Moreover, focusing on hacktivists will aid recruitment of talented individuals with hacking skills – a goal shared by both the Obama Proposal and Task Force Proposal.[242] While not all hacktivists in Anonymous's ranks are young, many of them are,[243] suggesting that they might be subject to ideological capture. Without a substantial recruitment effort by the federal government, there is an obvious lack of an alternative hacking "career path," so to speak, for those young persons looking for an outlet for their computer skills. Additionally, increased recruitment efforts might even help persuade those who already have joined hacktivist endeavors to work for the government. Hacktivism's roots in moralistic/political philosophy[244] yield the possibility that the federal government could enlist the help of hacktivists to

---

[240] Lesley Suzanne Bonney, *The Prosecution of Sophisticated Urban Street Gangs: A Proper Application of RICO*, 42 CATH. U. L. REV. 579, 583 (1993) ("As the Mafia obtained authority and the ability to exert control over legitimate business by virtue of its financial position, the creators of RICO hoped to finally create a means by which to diminish the role of the Mafia and organized crime within the United States by impairing the financial bases of the nation's criminal organizations.").

[241] VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 18-19 (2012), *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (stating that of the 174 million records compromised resulting from cybercrimes that were tracked in 2011, 100 million of those compromised records were the product of hacktivist-orchestrated attacks).

[242] *See supra* Part III.A.3.

[243] *See supra* note 49 and accompanying text.

[244] *See supra* Part I.B.1.

help thwart, defend, or even counterattack a common political enemy. One such enemy would be foreign government hackers.[245] For example, China, a prominent source of foreign hacking operations, is known for its censorship of the Internet and speech[246] – two characteristics detested by Anonymous's ranks.[247] Ideally, therefore, the national cybersecurity recruitment effort would be framed in the language of "national defense."

Only one of the proposals would successfully lend itself to such a recruitment campaign. It is unlikely that the Republican Task Force Proposal, while outwardly professing the benefits of increased cybersecurity recruitment, would deliver the same results as the Obama Proposal. Under the Task Force Proposal, DHS would have no role in establishing or enforcing cybersecurity guidelines with key private sector entities.[248] The obvious question posed by this approach is who is the intended beneficiary of the Task Force Proposal's recruitment push? Under the decentralized reform model, the only logical solution offered by the Task Force Proposal would be private-sector companies.

Interestingly, the same capitalism/market-efficiency rationale that pervades the Task Force Proposal, would also lead to the conclusion that private companies already allocate the optimal level of resources toward cybersecurity. That is to say, should a private company subjectively believe itself to be lacking in cybersecurity protections and personnel, it would invest in additional protection and personnel absent any legislative intervention, whether that intervention is a direct-regulation model or a market-incentive-based model. Thus, framing the recruitment effort in the necessary "national defense" rhetoric would yield no extra benefit for the Task Force Proposal. It makes no sense to say that a private company is simultaneously deemed to be inadequate in its cybersecurity standards and presumed to be appropriately allocating resources toward hiring and training cybersecurity personnel to achieve those standards.

The Obama Proposal on the other hand has identified the key beneficiary of recruitment efforts: the federal government, and more specifically, DHS. This approach is the wiser one for several reasons. First, it converts a niche,

---

[245] *Internet Censorship in China*, N.Y. TIMES, http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html (last updated Mar. 22, 2010) (detailing the Chinese government's March 2011 cyberattack on Google's servers).

[246] *Id*. ("Internet censorship in China is among the most stringent in the world. The government blocks Web sites that discuss the Dalai Lama, the 1989 crackdown on Tiananmen Square protesters, Falun Gong, the banned spiritual movement, and other Internet sites. As revolts began to ricochet through the Middle East and North Africa in 2011, and homegrown efforts to organize protests began to circulate on the Internet, the Chinese government tightened its grip on electronic communications, and appeared to be more determined than ever to police cellphone calls, electronic messages, e-mail and access to the Internet in order to smother any hint of antigovernment sentiment.").

[247] *See supra* notes 13, 76 and accompanying text.

[248] *See supra* notes 150-51 and accompanying text.

technical job into a public service career. The initial reaction to this result is that such a conversion will deter some cybersecurity talent from choosing a career with DHS over a large technology company such as Google. While some recruits will surely choose the private sector for no other reason than more handsome compensation, some patriotic-minded recruits will opt for a DHS career imbued with service to country, in the same way that many young persons with engineering skills enlist in the armed forces out of a desire to serve their country. Second, making DHS the direct beneficiary of increased cybersecurity recruitment matches the public nature of cybersecurity – a dynamic that Anonymous has underscored better than any other actor in cyberspace. Despite the obvious flaws in the comparison, Anonymous is the public face of hacking in the same way that Al Qaeda has been the public face of international terrorism since 9/11. Anonymous has shown a proclivity for utilizing social media, news outlets, and public protests to communicate its goals.[249] Again, under the Task Force's decentralized reform model, it is hard to understand how a young, talented cybersecurity recruit would find as high a level of gratification in thwarting hacktivists and other public-oriented hackers by opting for private sector work over a career in public service.

Recruitment aside, it would be naïve for legislators pondering reform to expect hacktivist cyberattacks to remain "benign"[250] since hacktivism is rooted in moralistic and quasi-political motivations.[251] Rather, cyberattacks could certainly come from domestic or foreign hacktivists whose political mission is the dismantling of the American government or its critical infrastructure, rather than the brief interruptions of website service typical of Anonymous's trademark, and comparatively harmless, DDoS attacks.[252] In February 2012, NSA Director General Keith Alexander informed the White House just that that within the next two years Anonymous would be able to launch a cyberattack on the United States' electric grid.[253] If the United States should be worried that Anonymous's cyberattacks are becoming increasingly destructive, then a strong DHS would more realistically align prevention of current attacks and prospective attacks.

The Obama Proposal's emphasis on centralized regulation more accurately perceives the nature of cyberthreats in the country's immediate and distant future. Presume for a moment that cyberthreats exist along a spectrum of

---

[249] *See supra* notes 14-15, 79 and accompanying text.

[250] Use of the term "benign" refers to cyberattacks such as those on the Senate, CIA, and BART websites where the websites were shut-down and some personal-identifying information may have been stolen, but no long-term infrastructure or fiscal damage was done to the victim.

[251] *See supra* Part I.B.

[252] *See supra* note 89 (describing DHS's concerns that Anonymous may begin targeting critical infrastructure in the United States).

[253] Eric Chabrow, *Anonymous Set to Do Real Damage*, GOV INFO SECURITY (Feb. 22, 2012), http://www.govinfosecurity.com/blogs.php?postID=1203.

seriousness/damage, with "benign" DDoS-like cyberattacks on the low end of the spectrum and full-fledged cyberwarfare on the high end. Assume also, as is actually the case, that legislators and government officials believe that cyberwarfare is inevitable. Any indication that cyberthreats are potentially or in fact moving upward along the spectrum warrants a more centralized (i.e., direct governmental) approach due to the fact that cyberwarfare would certainly be a matter of national security involving the federal government. Anonymous, already the most publicly visible actor within the cybersecurity arena, has shown the ability and will to escalate the seriousness of its cyberattacks.[254] Thus, it would be unwise to make private industry alone shoulder the burden of investment and prevention when cyberattacks could – and eventually will – become a matter of national security. Using Anonymous as but one reference point, Congress should realize that empowering DHS now is an investment in future prevention against cyberspace actors inimical to the very existence of our government.

Finally, to the extent that Anonymous has conducted its activities internationally, the federal government should realize that preparing for and defending against Anonymous attacks will help prepare for what politicians fear is the "inevitable" cyberwarfare era among nation-states.[255] The FBI has already been successful in a few instances of tracking down and arresting Anonymous hackers internationally with the help of foreign governments and law enforcement agencies.[256] This work should continue, as it will forge strong relationships with international partners – bolstered by broader coordination efforts like Cyber Atlantic 2011 – and train the U.S. government's cybersecurity personnel to think and operate on a global scale.

Overall, many, if not all, of the arguments for why Congress should account for hacktivism in cybersecurity reform tend to favor a direct regulation model as embodied in the Obama Proposal, rather than the Task Force Proposal's more limited, market-incentive-based approach.

---

[254] *See supra* Part I.B.2.

[255] *See supra* note 200 and accompanying text; *see also* Helen A.S. Popkin, *NSA Chief Fears Anonymous Could Hit Power Grid: Report*, NBCNEWS.COM TECHNOLOG (Feb. 21, 2012), http://www.nbcnews.com/technology/technolog/nsa-chief-fears-anonymous-could-hit-power-grid-report-157724 (reporting that countries with the capability to destroy part the U.S. electric grid, such as China and Russia, lack incentive to do so, while other states, such as North Korea and Iran, have incentive but lack the capability).

[256] *See* Eyder Peralta, *FBI Arrests 14 in Connection to Cyberattack on PayPal*, NPR (July 19, 2011, 6:20 PM), http://www.npr.org/blogs/thetwo-way/2011/07/19/138522991/fbi-arrests-14-in-connection-to-cyber-attack-on-paypal?ps=rs; Brendan Sasso, *Interpol Arrests Alleged Anonymous Hackers*, THE HILL (Feb. 29, 2012, 11:13 AM), http://thehill.com/blogs/hillicon-valley/technology/213275-interpol-arrests-alleged-anonymous-hackers.

## CONCLUSION

The threat of cyberattacks against the United States is serious and imminent. The good news is that U.S. politicians and legislators are in the midst of a heated debate over how best to improve cybersecurity. The bad news is the debate has been ongoing since 2009 and there is no enacted, comprehensive legislation to show for it.

Since President Obama's speech some three years ago, hacktivists, led by the online collective Anonymous, have become a dominant force in the cyber arena. Anonymous has taken hacking – an act of isolated, technical expertise – and turned it into something much bigger: a public statement backed by steadfast political and moral beliefs. Its cyberattacks, in many ways, are a microcosm of the larger cybersecurity picture. The attacks are becoming more sophisticated, the targets more varied, and the damage more serious.

Keeping the development of hacktivism in mind in assessing the proffered bills emerging from Washington, each of the two major political parties has made its preference for a legislative solution clear. The Obama Proposal, issued in May 2011, envisions a centralized regulatory framework, with the Department of Homeland Security at the forefront of the cybersecurity movement, establishing and enforcing cybersecurity standards for high-risk entities in the private sector. Meanwhile, the Task Force Proposal would opt for a decentralized regulatory approach where the Department of Homeland Security plays no role and private entities improve cybersecurity standards in order to realize market incentives established by the new law.

The Obama Proposal (and other bills drafted in its vein) has properly accounted for the nature of the threat. So long as cyberattacks continue to escalate in seriousness, most Washington experts believe, inevitably to the point of cyberwarfare, the U.S. government needs to take steps now to equip itself to defend against threats in the near and distant future.

Anonymous has already demonstrated that very trend as the most public actor in cyberspace. While many of Anonymous's attacks are relatively harmless when compared to the possibility of cyberwarfare, one could envision that gap closing based on the collective's moralistic/politcal motivations and increasing sophistication in cyberattacks.

Cybersecurity is a public good that an inter-connected America depends on each and every day. Empowering DHS to lead the new regulatory regime properly accounts for the fact that cybersecurity is a public issue, not a private one. Legislators would be prudent to realize that highlighting the public nature of Anonymous's activities will only help drive this point home.

We must come to think of cybersecurity in the same way that our country has come to think of increased traditional counterterrorism: as associated with real and existing threats. Investing today in a centralized cybersecurity regulatory regime is substantially more than needless government expenditure or an arbitrary policy choice. The Obama Proposal fully comprehends this point and makes a strong case for why a centralized legislative reform model is the appropriate solution in the cybersecurity debate.