Vanderbilt Journal of Entertainment & Technology Law

Volume 15
Issue 1 *Issue 1 - Fall 2012*

Article 6

2012

Hacking for Lulzi: Employing Expert Hackers to Combat Cyber Terrorism

Swathi Padmanabhan

Hacking for Lulz[1]: Employing Expert Hackers to Combat Cyber Terrorism

ABSTRACT

Because hacking collectives Anonymous and LulzSec have routinely breached supposedly secure computer networks—including Visa, MasterCard, and the Central Intelligence Agency—the threat of cyber terrorism has become more prominent. Many US industries and companies depend on online communication and information storage. If terrorists compromise these capabilities, they could cripple the US economy and perhaps even cause widespread fatalities. Members of Anonymous and LulzSec lack the necessary intent to be prosecuted as cyber terrorists because they hack not to cause fear, but rather to create laughter. Their method of posting all necessary instructions and information regarding intended targets on online message boards could, however, serve as a model for terrorists seeking to cause harm. Indeed, the Anonymous and LulzSec model permits an unknown number of hackers to anonymously participate in attacks. Without the ability to trace these individuals, the Computer Fraud and Abuse Act and all subsequent legislative attempts to improve cyber security and combat cyber terrorism, which require that the identity of perpetrators be known, are ineffective.

This Note therefore proposes a new bill that seeks to preempt attacks before they occur. It suggests more extensive public- and private-sector collaboration to anticipate novel hacking techniques and to uncover weaknesses in network security. Most importantly, it concludes that hiring Anonymous and LulzSec members, rather than prosecuting them, will more effectively aid the United States in protecting itself against cyber terrorism.

1. Lulz is derived from the neologism "LOLs," or "laughing out loud," which suggests laughter directed at the victim of a prank. Andrew Morse & Ian Sherr, *For Some Hackers, Goal Is Pranks*, WALL ST. J., June 6, 2011, http://online.wsj.com/article/SB10001424052702304906004576367870123614038.html.

TABLE OF CONTENTS

I. CYBERCRIME: WHAT IT IS AND HOW IT IS CONDUCTED 195
A. Hacking and Distributed Denials of Service: Two Visible Forms of Cybercrime 196
B. Development of Hacker Groups Anonymous and LulzSec 198
1. Anonymous Hacking Group 198
2. Lulz Security Hacking Collective 201
II. THE PROPOSED CYBER-SECURITY LAW TO CRIMINALIZE CYBERCRIMES: AN INSUFFICIENT EFFORT 205
A. An Overview of Existing Legislative Proposals Targeting Cybercrime 207
1. The White House's Proposal 207
2. Senate Bill 413: Cyber Security and Internet Freedom Act of 2011 209
3. House Resolution 2096: Cybersecurity Enhancement Act of 2011 210
4. House Resolution 3523: Cyber Intelligence Sharing and Protection Act of 2011 210
5. House Resolution 3674: Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act 211
B. The Government Should Not Regulate Anonymous and LulzSec's Activities under Any of These Proposals 212
1. The Government Should Not View Anonymous and LulzSec's Activities as a New Form of Terrorism 212
2. If Enacted, the Proposals Will Not Effectively Deter Anonymous and LulzSec's Hacking Activities 214
3. Despite Statements to the Contrary, Lawmakers May Not Actually Intend to Use These Proposals to Target Members of Anonymous and LulzSec 214
C. The Deficiencies in Each of These Proposed Solutions With Respect to Cyber Terrorism 217
1. The White House Proposal, the Lieberman Bill, and the Information Sharing Bill: All Inadequate Proposals 217
2. Both Congress and President Obama's Proposals Provide a Necessary Foundation, but Congress Must Expand upon Them to Ensure Their Effectiveness 219

III. HOW TO SOLVE AN UNSOLVABLE PROBLEM? 220
A. Keep Friends Close, Keep Enemies Closer: Allying Anonymous and LulzSec in the Struggle to Contain Cyber Terrorism 221
B. Greater Public- and Private-Sector Interaction Is Necessary 224
IV. CONCLUSION 225

With its enormous capacity to make information accessible, the Internet has changed the way Americans interact.[2] Consumers now routinely shop, pay bills, and bank—activities which once required face-to-face human contact—online.[3] Consumers, increasingly aware of their dependence on the Internet to transact and communicate with others, have raised concerns regarding the safety of their private information.[4] Breaches of supposedly secure computer networks have repeatedly compromised consumer data, thus evidencing the inadequacy of current cyber-security systems, which strive to safeguard confidential information.[5] Additionally, because of the federal government's dependence on the Internet, these security breaches could threaten national security.[6] However, the government's failure to prevent unauthorized access to government computer networks could leave the United States vulnerable to cyber terrorism.[7]

US government websites must be secure to protect the highly classified documents they house. But hackers who self-identify as

---

2. *See* Vint Cerf, *Vint Cerf On How The Internet Changed Communication,* FORBES (Oct. 24, 2005, 9:00 AM), http://www.forbes.com/2005/10/19/cerf-vint-networking-internet-comm05-cx_de_1024cerfnet.html.

3. *See* Hadley Malcolm, *Shoppers Ring Up Online Sales Surge,* USA TODAY, Dec. 6, 2011, http://www.usatoday.com/money/industries/retail/story/2011-12-06/online-retail-sales-surge/51682896/1; Tina Brandon, *Online Bill Pay Increase WEB ACH Payments,* NATIONALACH (Feb. 2, 2010), http://www.nationalach.com/ach/online-bill-pay-increase-web-ach-payments; Catherine New, *As Angry Customers Flee Financial Giants, Online Banks Are Booming,* DAILY FIN. (Oct. 6, 2011, 3:30 PM), http://www.dailyfinance.com/2011/10/06/as-angry-customers-flee-financial-giants-online-banks-are-boomi.

4. *See Privacy Concerns Stress Consumers,* IDENTITY THEFT RES. CENTER (Aug. 13, 2010, 12:24 PM), http://www.idtheftcenter.org/artman2/publish/m_press/2010_Consumer_Survey.shtml.

5. *See* Dan Goodin, *US Credit Card Payment House Breached By Sniffing Malware,* REGISTER (Jan. 20, 2009, 6:57 PM), http://www.theregister.co.uk/2009/01/20/heartland_payment_breach; Ina Steiner, *Security Breach at eBay's PayPal Service Raises Many Questions But Few Answers,* ECOMMERCE BYTES (Mar. 27, 2006), http://www.auctionbytes.com/cab/abn/y06/m03/i27/s04.

6. *See* Michael Schmidt, *New Interest in Hacking as Threat to Security,* N.Y. TIMES, Mar. 13, 2012, http://www.nytimes.com/2012/03/14/us/new-interest-in-hacking-as-threat-to-us-security.html.

7. *See id.*

members of Anonymous or LulzSec, two notorious hacking collectives, have demonstrated that these websites are not always secure. Indeed, Anonymous and LulzSec have gained notoriety for hacking websites previously thought to be among the most impenetrable in the world, including the websites that the US Senate, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), state governments, and various multinational US corporations maintain.[8] The threat of cyber terrorism is thus realistic. Consequently, lawmakers must enact legislation that better reflects the consequences of hacking. Specifically, Congress must determine whether the use of hacking to take websites offline should be classified as cyber terrorism.

Members of both hacking collectives have thus far violated privacy rights by releasing email addresses and phone numbers of government officials and private citizens.[9] In addition to leaking contact information, they have also taken websites offline for several hours, in part as a response to perceived Internet censorship.[10] But these attacks have not resulted in the publication or distribution of classified information that could compromise national security.[11] Rather, they have highlighted holes in companies' online security mechanisms.[12] Therefore, an argument can be made that Anonymous and LulzSec do not harm society. Instead, they provide government and private-sector targets a service akin to that of the CIA Red Cell, which identifies security threats that the United States faces from unconventional sources.[13]

---

8. *See* Ellen Nakashima, *CIA Web Site Hacked; Group LulzSec Takes Credit*, WASH. POST, June 15, 2011, http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html; Sandra Laville, *Anonymous Hacks Into Phone Call Between FBI And Scotland Yard*, GUARDIAN (Feb 3, 2012, 11:54 AM), http://www.guardian.co.uk/technology/2012/feb/03/anonymous-hacks-call-fbi-scotland-yard; Daniel Tencer, *Hackers Take Down Website of Bank That Froze Wikileaks Funds*, RAW STORY (Dec. 6, 2010, 8:32 PM), http://www.rawstory.com/rs/2010/12/06/hackers-website-bank-froze-wikileaks-funds.

9. *See* Daniel Bischoff, *LulzSec Says Goodbye With a Torrent Full of Your Personal Information*, GAME REVOLUTION (June 26, 2011, 2:38 PM), http://www.gamerevolution.com/news/lulzsec-says-goodbye-with-a-torrent-full-of-your-personal-information-6427; *NDAA Mass Dox*, PASTEBIN (Dec. 15, 2011), http://pastebin.com/nSvjR2Ev.

10. *See infra* Part I.A.

11. The closest they have gotten is LulzSec's release of classified documents from the State of Arizona in protest of its arguably discriminatory immigration law. *See* Suzanne Choney, *LulzSec Claims Hack of Arizona Law Enforcement Info*, NBCNEWS.COM TECH (June 23, 2011, 7:48 PM), http://technolog.msnbc.msn.com/_news/2011/06/23/6928929-lulzsec-claims-hack-of-arizona-law-enforcement-info.

12. *See* Rowan Puttergill, *LulzSec and Anonymous: Showing Us That Internet Security Is a Joke*, MEMEBURN (July 25, 2011), http://memeburn.com/2011/07/how-lulzsec-and-anonymous-are-showing-us-that-internet-security-is-a-joke.

13. *See* Jordan Yerman, *What Is the CIA's Red Cell?*, NOW PUBLIC (Aug. 25, 2010, 10:41 AM), http://www.nowpublic.com/world/what-cias-red-cell-2654851.html; *see also History*, CENT.

But the possibility still remains that terrorists seeking to harm the United States and its allies could adopt Anonymous's or LulzSec's tactics and organizational methods. Therefore, while this Note concludes that Anonymous' and LulzSec's humor-seeking activities are not acts of cyber terrorism, it recognizes that both groups have set a precedent for leaking information to media outlets. Terrorist organizations seeking to upset the US way of life and promote anti-US sentiments could replicate these actions by hacking into government databases (just as Anonymous and LulzSec have), acquiring inflammatory information, and leaking it to websites like Wikileaks.org. Because Wikileaks verifies only the veracity of the information, and not the means by which it was acquired,[14] the organization could inadvertently publish information that promotes terrorists' agendas at the expense of national and international security. To prevent such acts of cyber terrorism, this Note suggests that the US government should harness Anonymous's and LulzSec's skills by hiring its members to identify hackers that pose a threat to national security, strengthening weaknesses in cyber-security networks, and otherwise preempting attacks on national security.

In Part I, this Note provides a definition for the term "cybercrime" that takes into account recent use of the Internet to carry out cyber attacks. Furthermore, it explores how cybercrime is conducted. Part II demonstrates the inadequacy of the Computer Fraud and Abuse Act (the controlling legislation that criminalizes cyber attacks), President Obama's cyber-terrorism proposal, and bills recently introduced in Congress that punish and thereby seek to prevent the perpetration of cybercrime. Finally, in Part III, this Note proposes new legislation that seeks to employ members of Anonymous and LulzSec in the fight against cyber terrorism, rather than prosecute them.

I. CYBERCRIME: WHAT IT IS AND HOW IT IS CONDUCTED

Given the increasingly widespread use of the Internet for academic purposes and business and government operations, it has become common for law enforcement officials, among others, to term

---

INTELLIGENCE AGENCY (July 19, 2011, 9:21 AM), https://www.cia.gov/offices-of-cia/intelligence-analysis/history.html.

14. Yerman, *supra* note 13. In an effort to minimize harm, Wikileaks claims to "remove or significantly delay the publication of some identifying details from original documents to protect life and limb of innocent people." Mehmood Ahmed, *About Wikileaks*, WIKILEAKS (Dec. 16, 2010, 8:19 AM), http://wikileaks420.blogspot.com/2010/12/about-wikileaks.html. When and how often it engages in such censorship is unclear.

criminal activity conducted online as "cybercrime."[15] The label refers to "the use of a computer to facilitate or carry out a criminal offense."[16] But the Department of Justice (DOJ) has defined it more broadly to include "any violations of criminal law that involve a knowledge of computer technology for the perpetration, investigation, or prosecution" of criminal activity conducted via the Internet.[17] Thus, in addition to capturing within the term's scope traditional crimes that computers facilitate, the DOJ has also included novel, technology-based crimes, such as distributed denials of service (DDoS),[18] which lack a corresponding analog in existing criminal law.[19]

A. Hacking and Distributed Denials of Service: Two Visible Forms of Cybercrime

Cybercrime is not a new or even recent phenomenon.[20] Nearly twenty-four years ago, a Cornell University student released the "Morris Worm," allegedly to gauge the size of the Internet.[21] The worm was a virus that crippled the Internet, ultimately causing as much as $10 million in total damage, with some individual computers requiring $53,000 each in repairs.[22] The release of the worm resulted in the first conviction in the United States under the 1986 Computer Fraud and Abuse Act (CFAA).[23] But because so few people used the Internet at that time, the effect of the cyber attack was limited.[24] Indeed, the country remained largely unaware of the worm's devastating impact.[25] Now, with over 2 billion people using the Internet worldwide for both personal and professional purposes,

15. Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 241 (2000) (quoting NAT'L INST. OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989) (internal quotation marks omitted)).

16. *Id.*

17. *Id.* For an articulation of the definition of "cybercrime," see NAT'L INST. OF JUSTICE, *supra* note 15, at 2.

18. *See infra* Part I.A.

19. *See infra* Parts I.A, II.A.

20. *See* O'Neill, *supra* note 15, at 238.

21. *See* Tony Long, *July 26, 1989: First Indictment Under Computer Fraud Act*, WIRED (July 26, 2011, 7:00 AM), http://www.wired.com/thisdayintech/tag/morris-worm.

22. Miranda Marquit, *The 12 Costliest Computer Viruses Ever*, INSURE (Aug. 3, 2010), http://blog.insure.com/2010/08/03/the-12-costliest-computer-viruses-ever.

23. *See* O'Neill, *supra* note 15, at 238-39; *Computer Crime Laws*, FRONTLINE, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html (last visited Sept. 19, 2012).

24. *See* O'Neill, *supra* note 15, at 239.

25. *See id.*

cybercrime has the potential to halt global activities and devastate economies worldwide.[26]

Hacking and DDoS are two of the most visible forms of cybercrime.[27] Hacking, which is the "unauthorized trespass of a system by an intruder," enables individuals to remotely take control of others' property via the Internet and use it or distribute it to the general public.[28] Given that effective attack scripts—codes for malicious computer programs that facilitate the breach of computers and networks—and protocols for hacking are readily accessible on the Internet, those seeking to conduct basic hacking no longer require extensive programming knowledge.[29] But government and corporate networks have sophisticated firewalls and security measures in place.[30] Therefore, it is likely that only technically competent, experienced hackers can infiltrate these more advanced networks without assistance.

A DDoS attack shuts down websites by overwhelming their servers with millions of requests to connect, thereby denying legitimate users access. Hacking a website or network is typically the first step in launching a DDoS attack.[31] Indeed, only after a hacker gains access to a computer system can he run the programming code that will turn that system into a "master" system.[32] The hacker then infiltrates other networks and runs codes that render those systems "slaves" of the master network.[33] The master then commands the slaves to flood the target (typically a website) with requests to connect.[34] The target system's ultimate inability to sustain the flood of traffic will cause it to shut down.[35] Consequently, legitimate customers or users of the target website are unable to connect, thereby disrupting routine business or governance operations.[36] DDoS hackers are difficult for law enforcement officials to trace because hackers (1) log in to computers remotely, and (2) use fictitious Internet protocol

26. *The Internet Big Picture: World Internet Users and Population Stats*, INTERNET WORLD STATS (July 29, 2012), http://www.internetworldstats.com/stats.htm.

27. *See* O'Neill, *supra* note 15, at 244-46.

28. *Id.* at 246.

29. *See id.*

30. *See, e.g.*, *Solutions Overview*, PALO ALTO NETWORKS, http://www.paloaltonetworks.com/solutions/overview (last visited Sept. 23, 2012).

31. *See* O'Neill, *supra* note 15, at 244-45.

32. *See id.* at 245.

33. *See id.*

34. *See id.*

35. *See id.*

36. *See id.*

(IP) addresses to conceal their identities.[37] Thus, DDoS attacks via hacking make it difficult, often impossible, to identify the perpetrator.

B. Development of Hacker Groups Anonymous and LulzSec

Hacking has become increasingly popular in recent years for a myriad of reasons.[38] Hackers seek, *inter alia*, to make political statements,[39] cause laughter,[40] and expose holes in the security protocols of both governments and businesses.[41] Two groups have emerged as the prominent faces of this pursuit: Anonymous and Lulz Security.

1. Anonymous Hacking Group

Anonymous, established in 2003, is a radical, chaotic group that seeks to incite civil disobedience while maintaining its members' anonymity.[42] According to self-identified members, membership in Anonymous is based entirely on users' ability to conceal their identities while using the Internet.[43] Members whose identities are revealed to the public are automatically removed from the group.[44] Deemed a "loose coalition of Internet denizens,"[45] Anonymous, whose

---

37. *See id.* IP addresses are binary numbers that have two purposes: (1) identify and (2) trace the location of users attempting to connect with websites on the Internet. *How to Trace an IP Address*, WIKIHOW, http://www.wikihow.com/Trace-an-IP-Address (last updated Sept. 12, 2012).

38. *See Rise in Hacking Attacks Demand Better Website Security*, VOIP & TECH WORLD NOW (May 11, 2012, 6:19 AM), http://www.techworldnow.org/2012/05/rise-in-hacking-attacks-demand-better.html.

39. *See* Kevin Poulson, *LulzSec Releases Arizona Police Documents*, WIRED (June 24, 2011, 12:19 AM) http://www.wired.com/threatlevel/2011/06/lulzsec-arizona; Alastair Stevenson, *Operation Anti-Security: Anonymous Yet to Act While LulzSec Rampage*, INT'L BUS. TIMES (June 22, 2011, 3:37 PM), http://www.ibtimes.co.uk/articles/167639/20110622/lulzsec-lulz-security-anonymous-operation-anti-security-anti-sec-hacked-cleary-ryan-arrest-attack.htm.

40. *See* Nate Anderson, *LulzSec Manifesto: "We Screw Each Other Over For a Jolt of Satisfaction"*, ARS TECHNICA (June 17, 2011, 12:25 PM), http://arstechnica.com/tech-policy/news/2011/06/lulzsec-heres-why-we-hack-you-bitches.ars.

41. *See id.*

42. *See* Die Redaktion, *Anonymous: Who They Are—What They Want*, INT'L CLUB OF POL. (Dec. 13, 2010), http://clubofpolitics.de/wissenschaft-bildung/anonymous-who-they-are-what-they-want; Carissa Wyant, *Anonymous: A New Civil Disobedience Movement For The Twenty-First Century*, MINT PRESS NEWS (Feb. 21, 2012), http://www.mintpress.net/anonymous-a-new-civil-disobedience-movement-for-the-twenty-first-century.

43. *See The Face of Anonymous*, CBC RADIO (Feb. 7, 2008), http://web.archive.org/web/20110608152146/http://podcast.cbc.ca/mp3/searchengine_20080207_4645.mp3.

44. *See id.*

45. COMMONWEALTH OF VA. DEP'T OF STATE POLICE, 2009 VIRGINIA TERRORISM THREAT ASSESSMENT 45 (2009), *available at* http://www.infowars.com/media/vafusioncenterterror assessment.pdf (internal quotation marks omitted).

members comprise users of Internet sites including 4chan,[46] 711chan,[47] 420chan,[48] Something Awful,[49] Fark,[50] Encyclopedia Dramatica,[51] Slashdot,[52] IRC Channels,[53] and YouTube,[54] lacks a designated leader.[55] Rather, its success depends on its individual members performing the same hack at the same time, such that the net effect benefits the goals of the collective.[56] As a member of Anonymous explained: "We have this agenda that we all agree on and we all coordinate and act, but all act independently toward it, without any want for recognition. We just want to get something that we all feel is important done . . . ."[57] On January 8, 2012, a member of Anonymous uploaded to the group's Facebook page the following statement regarding the group's identity and purpose:

> Anonymous has NO leader. We are one. We are many. One does not speak for many. Many do not speak for all. No one speaks for all. . . . We are not terrorists. We are freedom fighters, helping to give voices to the voiceless.
>
> . . . We do it because we can. We do it for the future, of our children and all life on this planet. We do it because we see lies and deceit. We do it because every digital account is fuelled with the strength of human emotion, but mostly we do it for the lulz.58

In its infancy, Anonymous primarily targeted websites as a form of entertainment.[59] But in 2008, it shifted its focus to issues pertaining to Internet freedom and freedom of speech in a manner

---

46. *See id*; *see also* David George-Cosh, *Online Group Declares War on Scientology*, NAT'L POST (Jan. 26, 2008), http://web.archive.org/web/20080129063500/http://www.nationalpost.com/most_popular/story.html?id=261308.

47. *See* COMMONWEALTH OF VA. DEP'T OF STATE POLICE, *supra* note 45.

48. *Id.*

49. *Id.*

50. *Id.*

51. Shaun Davies, *Critics Point Finger at Satirical Website*, NINEMSN (May 8, 2008, 1:00 PM), http://news.ninemsn.com.au/article.aspx?id=459249; *see also* COMMONWEALTH OF VA. DEP'T OF STATE POLICE, *supra* note 45.

52. *See* COMMONWEALTH OF VA. DEP'T OF STATE POLICE, *supra* note 45.

53. *Id.*

54. *Id.*

55. James Harrison, *Scientology Protestors Take Action Around World*, STATE NEWS (Feb. 12, 2008, 3:28 PM), http://www.statenews.com/index.php/blog/entertainment/2008/02/internet_group_; *see also* COMMONWEALTH OF VA. DEP'T OF STATE POLICE, *supra* note 45.

56. Harrison, *supra* note 55; *see also* COMMONWEALTH OF VA. DEP'T OF STATE POLICE, *supra* note 45.

57. Chris Landers, *Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything)*, CITY PAPER (Apr. 2, 2008), http://www2.citypaper.com/columns/story.asp?id=15543.

58. Anonymous, *Anonymous Manifesto*, FACEBOOK (Jan. 8, 2012, 9:49 AM), https://www.facebook.com/wedonotforgive.wedonotforget.expectus/posts/359200827429894.

59. *See* Quinn Norton, *Anonymous 101: Introduction to the Lulz*, WIRED (Nov. 8, 2011, 5:30 AM), http://www.wired.com/threatlevel/2011/11/anonymous-101/all/1.

known as "hacktivism."[60] Anonymous gained prominence worldwide as a hacktivist group for Project Chanology, an initiative that targeted the Church of Scientology for conduct it believed constituted Internet censorship.[61] As part of the initiative, Anonymous members coordinated a series of DDoS attacks targeting Scientology websites.[62] They also initiated prank calls and sent black faxes to Scientology centers that were designed to use as much of the recipient's fax ink, toner, thermal paper, or disc space as possible. [63]

In December 2010, Anonymous made headlines for targeting groups that opposed Wikileaks.[64] Code named "Operation Avenge Assange," Anonymous's DDoS attacks targeted Amazon, PayPal, MasterCard, Visa, and the Swiss bank PostFinance for freezing Wikileaks-affiliated bank accounts.[65] Because of the attack, the MasterCard website remained inaccessible for much of the day.[66] Just as MasterCard restored its website, hackers shut down Visa's website.[67] Anonymous thus successfully crippled some of the largest and most sophisticated websites in the world.

More recently, Anonymous has embraced political issues for its "humorous" attacks. Indeed, its members have conducted DDoS attacks against the websites of the Irish political party Fine Gael

---

60. *See id.*

61. *See* 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. Following the leak to YouTube of a video filmed by the Church featuring Tom Cruise, the Church alleged violation of its copyright and requested that YouTube remove the video. John Cook, *Cult Friction*, RADAR (Mar. 17, 2008), http://web.archive.org/web/20080323063402/http://www.radaronline.com/from-the-magazine/2008/03/scientology_anonymous_protests_tom_cruise_01.php.

62. *See* Singel, *supra* note 61.

63. Matthew A. Schroettnig, *Anonymous Versus Scientology: Cyber Criminals or Vigilante Justice?*, LEGALITY (Feb. 6, 2008), http://www.thelegality.com/2008/02/06/anonymous-versus-scientology-cyber-criminals-or-vigilante-justice.

64. Cassell Bryan-Low & Sven Grundberg, *Hackers Rise for Wikileaks: Cyber Attackers Seek Revenge against Organizations That Have Tangled with Document-Leaking Site*, WALL ST. J., Dec. 8, 2010, http://online.wsj.com/article/SB10001424052748703493504576007182352309942.html; Sean-Paul Correll, *Operation: Payback Broadens to "Operation to Avenge Assange"*, PANDALABS BLOG (Dec. 6, 2010), http://pandalabs.pandasecurity.com/operationpayback-broadens-to-operation-avenge-assange; Fahmida Y. Rashid, *PayPal, PostFinance Hit By DoS Attacks, Counter-Attack in Progress*, EWEEK (Dec. 6, 2010), http://www.eweek.com/c/a/Security/ PayPal-PostFinance-Hit-by-DoS-Attacks-CounterAttack-in-Progress-860335; Daniel Tencer, *Hackers Take Down Website of Bank That Froze Wikileaks Funds*, RAW STORY (Dec. 6, 2010, 8:32 PM), http://www.rawstory.com/rs/2010/12/06/hackers-website-bank-froze-wikileaks-funds.

65. *Supra* note 64.

66. Corky Siemaszko, *Wikileaks Supporters Cripple Visa, MasterCard Websites, Hack Sarah Palin in 'Operation Payback'*, N.Y. DAILY NEWS, Dec. 8, 2010, http://articles.nydailynews.com/2010-12-08/news/27083817_1_wikileaks-megrahi-lockerbie-bomber.

67. *Id.*

during Ireland's 2011 General Election,[68] the government of Tunisia during the Tunisian Revolution for its anti-Wikileaks behavior,[69] and the Egyptian government[70] and Syrian Defense Ministry[71] during the Arab Spring of 2012. On January 19, 2012, Anonymous also targeted the FBI's website in a DDoS attack, taking it—in addition to the websites of the DOJ, Universal Music Group, Recording Industry Association of America, and the Motion Picture Association of America—offline in retaliation for the federal raid on the file-sharing service Megaupload.[72]

But while Anonymous's activities have assumed a political bent, the fact that its members' primary motivation is a desire to garner "lulz"[73] on a widely visible stage is perhaps the strongest argument against deeming their activities terroristic in nature.[74]

2. Lulz Security Hacking Collective

Lulz Security, more commonly referred to as LulzSec, was founded in May 2011 with a dual purpose: (1) to expose holes in organizations' Internet security systems, and (2) to laugh at the victims of its pranks (hence the "Lulz" in the group's name[75]).[76]

---

68. Anonymous replaced the site with a page depicting the group's logo and the following statement: "Nothing is safe, you put your faith in this political party and they take no measures to protect you. They offer you free speech yet censor your voice. WAKE UP!" Gavan Reilly, *Fine Gael Website Defaced by Anonymous 'Hacktivists'*, JOURNAL (Jan. 10, 2011), http://www.thejournal.ie/fine-gael-website-defaced-by-anonymous-hacktivists-2011-01 (internal quotation marks omitted).

69. *Anonymous Activists Target Tunisian Government Sites*, BBC NEWS (Jan. 4, 2011, 3:24 PM), http://www.bbc.co.uk/news/technology-12110892.

70. *See* Ravi Somaiya, *Hackers Shut Down Government Sites*, N.Y. TIMES, Feb. 2, 2011, http://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html. The attack against the Egyptian government website sought to help protestors defy the government's shut-down of the Internet. *See id.*

71. *See* Bill Chappell, *Syria Is Hacked by Anonymous, and Pressed by Gulf Allies*, NPR (Aug. 8, 2011, 12:23 PM), http://www.npr.org/blogs/thetwo-way/2011/08/08/139094501/syria-is-hacked-by-anonymous-and-pressed-by-gulf-allies. Anonymous members replaced the Ministry's typical content with an image of the pre-Ba'athist Flag—a symbol of the country's pro-democracy movement—and a message supporting the pro-democracy uprising and encouraging Syrian soldiers to defect and protect protesters from harm. *See id.*

72. *Anonymous Downs Government, Music Industry Sites in Largest Attack Ever*, RT (Jan. 20, 2012, 1:48 AM), http://rt.com/usa/news/anonymous-doj-universal-sopa-235.

73. *See supra* note 1.

74. *See* Anonymous, *supra* note 58.

75. *See supra* note 1.

76. *See id.* It should be noted that some have indicated that LulzSec has used stolen credentials (i.e. login information) to execute its attacks. *Id.* But Ian Paul, an author at PCWorld, wrote, "As its name suggests, LulzSec claims to be interested in mocking and embarrassing companies by exposing security flaws rather than stealing data for criminal purposes." *Lulz Boat Hacks Sony's Harbor: FAQ*, PCWORLD (June 3, 2011, 3:03 AM), http://www.pcworld.com/article/229316/lulz_boat_hacks_sonys_harbor_faq.html.

During its five-week official existence,[77] the group increasingly focused on politics.[78] It cited anti-Wikileaks behavior, a lack of freedom of expression on the Internet, corruption, and privacy breaches as the impetus for several of its attacks.[79]

The group, which was allegedly a spinoff of Anonymous, maintained close connections with Anonymous.[80] Indeed, Topiary, one of LulzSec's leaders who ran LulzSec's Twitter account, was reportedly a media-relations manager for the website Anonymous AnonOps, which provided server support for Anonymous-led attacks.[81] LulzSec's organizational structure, however, distinguished it from its counterpart Anonymous. Unlike Anonymous, LulzSec maintained both a "home base" website that served as a launching pad for many of the group's attacks, and a Twitter page to publicize its activities.[82] In addition, its membership structure differed substantially from that of Anonymous's. LulzSec had six core members who controlled the group's actions. The Internet usernames of these members were Sabu, Topiary, Kayla, T-flow, Avunit, and Pwnsauce.[83] Sabu occupied a

77. *See* Zack Whittaker, *LulzSec Disbands: Final Cache Includes AT&T Internal Data and 750,000 User Accounts*, ZDNET (June 25, 2011, 6:47 PM), http://www.zdnet.com/blog/igeneration/lulzsec-disbands-final-cache-includes-at-and-t-internal-data-and-750000-user-accounts/11134. LulzSec did carry out one more attack in July against Rupert Murdoch after its official disbandment. John E. Dunn, *LulzSec Attacks Sun Newspaper with Rupert Murdoch Death Hoax*, TECHWORLD (July 19, 2011, 11:03 AM), http://news.techworld.com/security/3292174/lulzsec-attacks-sun-newspaper-with-rupert-murdoch-death-hoax.

78. *See, e.g.*, Ellen Nakashima, *CIA Web Site Hacked; Group LulzSec Takes Credit*, WASH. POST, June 15, 2011, http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html (stating that LulzSec claimed credit for hacking the public website of the CIA); David Meyer, *LulzSec Claims Soca Site Takedown*, ZDNET (June 20, 2011, 4:00 PM), http://www.zdnet.com/lulzsec-claims-soca-site-takedown-4010022772 (reporting that LulzSec, in conjunction with Anonymous, carried out an attack against the United Kingdom's Serious Organised Crime Agency after attacks on the US Senate and the CIA); Max Read, *LulzSec Hackers Go After FBI Affiliates*, GAWKER (June 4, 2011, 9:56 AM), http://gawker.com/5808517/lulzsec-hackers-go-after-fbi-affiliates (reporting that LulzSec hacked InfraGuard, a nonprofit organization associated with the FBI, to protest the Obama administration's classification of hacking as an act of war); Reuters, *LulzSec Hackers Claim Break-In of Senate Computers*, HUFFINGTON POST (June 13, 2011, 6:41 PM), http://www.huffingtonpost.com/2011/06/13/lulzsec-hackers-senate-computers_n_876304.html (reporting that LulzSec hacked the US Senate's network).

79. *See* Nick Ross, *LulzSec Teams Up with Anonymous*, AUSTL. BROAD. CORP. (June 20, 2011), http://www.abc.net.au/technology/articles/2011/06/20/3248520.htm.

80. *See* Damon Poeter, *Who Is LulzSec?*, PCMAG.COM (June 30, 2011), http://www.pcmag.com/slideshow/story/266414/Who-Is-LulzSec.

81. *See id.*; Ryan Gallagher & Charles Arthur, *Inside LulzSec: Chatroom Logs Shine a Light on the Secretive Hackers*, GUARDIAN (June 24, 2011, 9:03 AM), http://www.guardian.co.uk/technology/2011/jun/24/inside-lulzsec-chatroom-logs-hackers.

82. The website is no longer active, but at the time of the collective's official existence, its domain name was http://lulzsecurity.com. LULZSEC, http://lulzsecurity.com (last visited July 14, 2011) (available at http://web.archive.org/web/20110714002349/http://lulzsecurity.com).

83. Poeter, *supra* note 80.

particularly strong leadership position in the group, often deciding which targets to attack and which members could participate.[84]

While Anonymous and LulzSec differ in organizational structure, the two groups have similar methods of operation. Like Anonymous, LulzSec commonly used DDoS attacks to temporarily shut down its victims' websites.[85] In its short lifespan, LulzSec also gained recognition for brazenly attacking websites of high-profile corporations and other organizations.[86] Its first attack targeted Fox.com in response to the network's labeling of Common, the rapper and entertainer, as "vile" on the Fox News Channel.[87] The group also leaked 62,000 usernames and passwords to a series of unlisted websites thought to include the game *World of Warcraft* and Gmail.[88] It then hacked the American Public Broadcasting System (PBS) website to defend Bradley Manning, the US soldier accused of passing 250,000 US diplomatic cables to Wikileaks;[89] it believed the network portrayed Manning negatively on the PBS program "Wikisecrets."[90]

LulzSec infiltrated the website of the US Senate, releasing a number of users' email addresses and passwords and the directory structure of files stored on the Senate website.[91] All other confidential

---

84. *See* Gallagher & Arthur, *supra* note 81.

85. *See* Peter Bright, *Titanic Takeover Tuesday: LulzSec's Busy Day of Hacking Escapades*, ARS TECHNICA (June 14, 2011, 4:22 PM), http://arstechnica.com/tech-policy/news/2011/06/titanic-takeover-tuesday-lulzsecs-busy-day-of-hacking-escapades.ars; Matthew Lynley, *LulzSec Hits U.S. Senate Website, Throws a "DDoS Party"*, VENTUREBEAT (June 14, 2011, 1:14 PM), http://venturebeat.com/2011/06/14/lulzsec-ddos-party-attacks; *Soca Website Taken Down After LulzSec 'DDoS Attack'*, BBC NEWS (June 20, 2011, 8:32 PM), http://www.bbc.co.uk/news/technology-13848510.

86. *See, e.g.*, Chris Gayomali, *LulzSec Hacks 'News of the World' and 'The Sun,' Plants Fake Murdoch Death Story*, TIME.COM (July 18, 2011), http://techland.time.com/2011/07/18/lulzsec-hacks-news-of-the-world-and-the-sun-plants-fake-murdoch-death-story; Andy Greenberg, *LulzSec Says Goodbye, Dumping NATO, AT&T, Gamer Data*, FORBES (June 25, 2011, 10:46 PM), http://www.forbes.com/sites/andygreenberg/2011/06/25/lulzsec-says-goodbye-dumping-nato-att-gamer-data; Whittaker, *supra* note 77.

87. *A Brief History of the LulzSec Hackers*, FOX NEWS (June 21, 2011), http://www.foxnews.com/scitech/2011/06/21/brief-history-lulzsec-hackers.

88. Kit Eaton, *LulzSec Leaks 62,000 Passwords, Usernames for Unknown Sites*, FAST CO. (June 16, 2011), http://www.fastcompany.com/1760500/lulzsec-gets-anarchic-62000-passwords-usernames-for-unknown-sites-leaked.

89. Ian Paul, *Hackers Deface PBS Site, Promise More Lulz*, PCWORLD (May 30, 2011, 10:48 AM), http://www.pcworld.com/article/228983/hackers_deface_pbs_site_promise_more_lulz.html.

90. Parmy Olson, *Interview With PBS Hackers: We Did It For 'Lulz and Justice'*, FORBES (May 31, 2011, 10:33 AM), http://www.forbes.com/sites/parmyolson/2011/05/31/interview-with-pbs-hackers-we-did-it-for-lulz-and-justice; Paul, *supra* note 89.

91. Ed Oswald, *LulzSec Hacks US Senate Website, Although No Data Taken*, BETANEWS, http://betanews.com/2011/06/14/lulzsec-hacks-us-senate-website-although-no-data-taken (last visited Oct. 3, 2012).

information the hackers gained access to remained confidential.[92] Therefore, given that Senate officials did not deem the published information sensitive, the intended effect of the attack was arguably not to compromise national security.[93] Rather, as the group stated in its press release, "This [was] a small, just-for-kicks release of some internal data from Senate.gov—is this an act of war, gentlemen?"[94] LulzSec also attacked the CIA's website,[95] taking it offline for more than two hours, much like Anonymous did to the FBI and the DOJ websites.[96]

On June 23, 2011, the State of Arizona classified LulzSec as a cyber-terrorist organization in response to the hacking and release of sensitive documents from the Arizona Department of Public Safety.[97] Lulzsec engaged in a data dump entitled "Chinga la migra," which translates to "Fuck the border patrol."[98] The documents included email addresses, passwords, and numerous files listed as "sensitive" or "for official use only."[99] LulzSec leaked the information to protest Arizona's law requiring some aliens to carry registration documents at all times.[100] This attack was part of an overarching collaboration with Anonymous called "Operation Antisec," which encouraged participants to hack into, steal, and leak classified government documents.[101]

LulzSec officially disbanded on June 26, 2011, in a statement titled "50 Days of Lulz," in which the six core members confirmed that they would take down their website.[102] LulzSec claimed that the

92. *See id.*

93. *See id.*; *see also* Reuters, *supra* note 78.

94. Parmy Olson, *LulzSec Hackers Hit Senate Website 'Just For Kicks'*, FORBES (June 14, 2011, 5:07 AM), http://www.forbes.com/sites/parmyolson/2011/06/14/lulzsec-hackers-hit-senate-website-just-for-kicks (internal quotation marks omitted).

95. *LulzSec Hackers Claim CIA Website Shutdown*, BBC NEWS (June 16, 2011, 7:20 AM), http://www.bbc.co.uk/news/technology-13787229.

96. *Id.*; *see* Andy Greenberg, *Anonymous Hackers Hit DOJ, FBI, Universal Music, MPAA and RIAA After MegaUpload Takedown*, FORBES (Jan. 19, 2012, 5:45 PM), http://www.forbes.com/sites/andygreenberg/2012/01/19/anonymous-hackers-claims-attack-on-doj-universal-music-and-riaa-after-megaupload-takedown.

97. Press Release, Ariz. Dep't of Pub. Safety, DPS Victim of Cyber Attack (June 27, 2011), *available at* http://www.azdps.gov/Media/News/View/?p=316.

98. Alexia Tsotsis, *LulzSec Releases Arizona Law Enforcement Data, Claims Retaliation for Immigration Law*, TECHCRUNCH (June 23, 2011), http://techcrunch.com/2011/06/23/lulzsec-releases-arizona-law-enforcement-data-in-retaliation-for-immigration-law.

99. Doug Aamoth, *LulzSec Claims Breach Against Arizona Law Enforcement*, TIME.COM (June 23, 2011), http://techland.time.com/2011/06/23/lulzsec-claims-breach-against-arizona-law-enforcement.

100. Tsotsis, *supra* note 98.

101. Ross, *supra* note 79.

102. Leena Rao, *After 50 Days of Attacks, Hacker Group LulzSec Calls It Quits*, TECHCRUNCH (June 25, 2011), http://techcrunch.com/2011/06/25/after-50-days-of-attacks-hacker-group-lulzsec-says-its-done.

group had intended to be active for only fifty days.[103] As a member related to the Associated Press, "We're not quitting because we're afraid of law enforcement. The press are getting bored with us, and we're getting bored with us"; this suggests that despite its highly political targets, LulzSec existed largely to garner "lulz."[104] Some of LulzSec's members have reportedly joined forces with members of Anonymous to continue Operation Antisec.[105] But law enforcement officials may have arrested several of the group's inner core.[106] Indeed, London's Metropolitan Police arrested a sixteen-year-old using the Internet moniker T-flow on July 19, 2011.[107] Police also arrested teenager Jake Davis, who is thought to be Topiary, in Shetland, United Kingdom on July 27, 2011.[108] Davis was later charged with unauthorized access of a computer and conspiracy, among other offenses.[109] Members of Anonymous have since confirmed that Davis is indeed Topiary, launching a "Free Topiary" campaign in part to assist him as he faces multiple hacking charges in the United Kingdom.[110]

II. THE PROPOSED CYBER-SECURITY LAW TO CRIMINALIZE CYBERCRIMES: AN INSUFFICIENT EFFORT

In their recent escapades, both Anonymous and LulzSec have managed to exploit a gaping hole in the 1986 CFAA, the controlling

---

103. Edward Moyer, *Hacking Group LulzSec Says It's Calling It Quits*, CNET (June 25, 2011, 5:44 PM), http://news.cnet.com/8301-1009_3-20074416-83/hacking-group-lulzsec-says-its-calling-it-quits.

104. Peter Svensson, *Hacker Group LulzSec Says It's Disbanding*, USA TODAY, June 26, 2011, http://www.usatoday.com/tech/news/2011-06-26-lulzsec-disbands_N.htm (internal quotation marks omitted).

105. Nathan Olivarez-Giles, *AntiSec 'Hackers Without Borders' Claim New Hack on Arizona State Police*, L.A. TIMES, June 29, 2011, http://latimesblogs.latimes.com/technology/2011/06/antisec-hackers-leak-files-said-to-be-from-arizona-state-police.html.

106. Jeremy A. Kaplan, *Leading Member of LulzSec Hacker Squad Arrested in London*, FOX NEWS (July 19, 2011), http://www.foxnews.com/scitech/2011/07/19/leading-member-lulzsec-hacker-squad-arrested-in-london; *Man Arrested Over Computer Hacking Claims*, BBC NEWS (July 27, 2011, 2:25 PM), http://www.bbc.co.uk/news/uk-14315442; *Teenager Arrested on Suspicion of Hacking*, BBC NEWS (June 21, 2011, 3:32 PM), http://www.bbc.com/news/technology-13859868.

107. Kaplan, *supra* note 106.

108. *LulzSec: Shetland Teen Charged Over Computer Hacking Claims*, BBC NEWS (July 31, 2011, 3:23 PM), http://www.bbc.co.uk/news/uk-14359933; *Man Arrested Over Computer Hacking Claims*, *supra* note 106.

109. *LulzSec: Shetland Teen Charged Over Computer Hacking Claims*, *supra* note 108.

110. *See* Trent Nouveau, *Anonymous Kicks Off "Free Topiary" Campaign*, TG DAILY (Aug. 2, 2011, 4:15 PM), http://www.tgdaily.com/security-features/57647-anonymous-kicks-off-free-topiary-campaign.

piece of legislation that criminalizes cyber attacks.[111] Absent the existence of at least one known perpetrator, law enforcement cannot enforce the CFAA, which criminalizes the intentional accessing of computers to obtain (1) national security data, (2) financial records from financial institutions, or (3) information involved in interstate or foreign commerce without authorization.[112] Given that both Anonymous and LulzSec conduct their attacks in complete anonymity, prosecutors are unable to charge perpetrators under the CFAA. Even if law enforcement could identify several perpetrators, there will likely always be an unknown number of participants originating in an unknown number of countries. Thus, even if prosecutors can charge several individuals, there are likely countless others willing to plan new attacks. Consequently, while the CFAA's primary intent is to reduce malicious interferences with computer systems and to address computer offenses,[113] the Act is difficult to enforce against Anonymous-style hacktivism, where the perpetrators of the attack are unidentifiable and their deeds indistinguishable.

The executive and legislative branches of the federal government have rapidly sought to push new cyber-security legislation through Congress to protect against Anonymous-style cybercrime, which the Pentagon has deemed a form of cyber terrorism.[114] Within the last year, the White House has issued a detailed proposal to both amend existing laws and create new ones to mandate prison time for hacking and DDoS attacks.[115] Additionally, Senator Joseph Lieberman (I-CT) and Representatives Daniel Lundgren (R-CA), Peter King (R-NY), Mike Rogers (R-MI), C.A. "Dutch" Ruppersberger (D-MD), and Michael McCaul (R-TX) have

---

111. 18 U.S.C. § 1030 (2006).

112. *Id.*

113. H.R. Rep. No. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689.

114. Oswald, *supra* note 91. Interestingly, Anonymous-style cybercrime would not constitute cyber terrorism under the DHS's definition. The National Infrastructure Protection Center—housed within the DHS—defines "cyber terrorism" as "a criminal act through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies." Nazura Abdul Manap & Pardis Moslemzadeh Tehrani, *Cyber Terrorism: Issues in Its Interpretation and Enforcement*, 2 INT'L J. INFO. & ELECTRONICS ENGINEERING 409, 410 (2012), *available at* http://www.ijiee.org/papers/126-I149.pdf (internal quotation marks omitted). Neither Anonymous nor LulzSec's activities have resulted in violence, death, destruction, or terror. This dichotomy between the DOD and the DHS will be a central player in this Note in subsequent sections.

115. *See* OFFICE OF MGMT. & BUDGET, LEGISLATIVE LANGUAGE: LAW ENFORCEMENT PROVISIONS RELATED TO COMPUTER SECURITY (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security.pdf; Fahmida Y. Rashid, *U.S. Congress Wants to Make Hacking Government Networks a Felony*, EWEEK (June 21, 2011), http://www.eweek.com/ c/a/Security/US-Congress-Wants-to-Make-Hacking-Government-Networks-a-Felony-455390 (discussing that this new law is intended to prevent cyber terrorism in the future).

each proposed bills promoting information sharing as a means to preempt and combat future cyber-terrorist attacks.[116] But as of October 2012, despite calls from members of both parties to make progress in the cyber-security realm, none of these bills have gained traction in Congress.[117] Indeed, no senator or congressman has incorporated the White House's proposal in its entirety into any of the proposed pieces of legislation.[118] Furthermore, none of the congressional bills have made it to a floor vote, despite months of debate in some cases.[119] Therefore, while Congress continues to debate how legislation can combat cyber-security and cyber-terrorism threats, the threats still remain.

A. An Overview of Existing Legislative Proposals Targeting Cybercrime

Both President Obama and numerous congressmen have proposed legislation to combat the growing threat of cyber terrorism. This section will discuss the merits of the relevant portions of each proposal.

1. The White House's Proposal

In May 2011, the White House proposed an extensive overhaul of US cyber-security laws.[120] The plan centers on protecting US citizens, critical infrastructure, the federal government's computer systems, and civil liberties.[121]

First, the plan proposes two major amendments to the CFAA: (1) establishing a mandatory minimum penalty of three years in prison for all criminal offenses outlined in the Act,[122] and (2) appending the crimes listed in the CFAA to the Racketeering Influenced and Corrupt Organizations Act (RICO) to increase certain

116. Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011); Cybersecurity Enhancement Act of 2011, H.R. 2096, 112th Cong. (2011); Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (2011); PRECISE Act of 2011, H.R. 3674, 112th Cong. (2011).

117. *See infra* Part II.A.

118. *See, e.g.*, S. 413.

119. One bill did, however, make it to a floor vote in the House in 2010, but it failed to make it through the Senate. Cybersecurity Enhancement Act of 2010, H.R. 4061, 111th Cong. (2010).

120. *See* OFFICE OF MGMT. & BUDGET, *supra* note 115.

121. Chloe Albanesius, *White House Unveils Cyber-Security Plan*, PCMAG (May 12, 2011, 2:31 PM), http://www.pcmag.com/article2/0,2817,2385293,00.asp.

122. OFFICE OF MGMT. & BUDGET, *supra* note 115.

penalties and to better facilitate the prosecution of organized-crime groups that carry out cyber attacks.[123]

Second, the plan emphasizes the need for greater information sharing between the public and private sectors.[124] It therefore proposes to grant businesses and local governments immunity from prosecution for cybercrimes when they, in good faith, share with the federal government any threats or vulnerabilities discovered while exercising their own preemptive measures against cyber attacks.[125] Third, the plan grants the Department of Homeland Security (DHS) leave to provide immediate assistance, upon request, to companies that have been hacked.[126] Finally, the plan calls on the Secretary of the DHS to consult with civil-liberties experts when developing and reviewing cyber-security policies to ensure that the acquisition, interception, retention, use, and disclosure of communications in the fight against cyber attacks do not impede upon privacy rights and civil liberties.[127]

Unfortunately, the White House's proposal does not close the loophole in the CFAA. It continues to underestimate the difficulty in enforcing cybercrime laws. For example, the proposal's mandatory minimum penalty does not deter violators of the law if hackers know the government cannot identify or catch them. Furthermore, treating DDoS attackers as members of organized-crime groups is shortsighted given that prosecution under RICO also depends on the presence of a known perpetrator.[128] Without the ability to ascertain the identities of anonymous cyber criminals, enhanced penalties under RICO will likely not be any more successful in deterring or punishing cybercrime than the CFAA. This proposal's failure to account for the anonymity now common in cybercrime renders it largely useless.

Ideally, computer scientists will develop a method to uncover perpetrators' hidden identities. But given that technologies are constantly evolving, solutions that focus on specific technologies will undoubtedly be obsolete in the future. It is more useful to craft solutions that can withstand unanticipated changes in Internet technologies. Moving forward, lawmakers seeking to amend

123. *Id.* Currently, RICO does not apply to cyber crimes. Therefore, despite the fact that RICO is often seen as the key tool for combating organized crime, it is useless in the fight against organized crime's increased use of cyber attacks. *Id.*

124. Albanesius, *supra* note 121.

125. *Id.*

126. OFFICE OF MGMT. & BUDGET, DEP'T OF HOMELAND SECURITY CYBERSECURITY AUTHORITY AND INFORMATION SHARING (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/dhs-cybersecurity-authority-section-by-section-analysis.pdf.

127. *See id.*

128. *See* 18 U.S.C. § 1962 (2006).

cyber-security law should focus on the proposal's call for increased dialogue between the DHS and civil-liberties experts specifically. Maintaining the critical balance between privacy and cyber security is difficult, and as new technologies emerge—like the ability to mask IP addresses, a technique that Anonymous and LulzSec employ—both sides will have to reevaluate where that balance should fall.

2. Senate Bill 413: Cyber Security and Internet Freedom Act of 2011

Sponsored by Senator Lieberman, the Cybersecurity and Internet Freedom Act of 2011 (the Lieberman Bill) has the backing of the White House and incorporates several prominent positions embraced in the White House's proposed cyber-security legislation.[129] The bill adopts a regulatory approach, establishing the National Center for Cybersecurity and Communications within the DHS, and also relies upon the private sector to "secure, protect, and ensure the resiliency of the federal information infrastructure."[130] While the federal government lacks the authority to shut down the Internet, the bill permits the President to declare a national cyber emergency, requiring the owners and operators of critical infrastructure to implement emergency-response plans.[131]

Under this bill, the President's power to declare a national cyber emergency is the equivalent of declaring war on the Internet. Given that the President could exercise this *carte blanche* authority for many (perhaps nefarious) purposes, the bill should require congressional approval prior to the President's declaration of a cyber emergency. But as currently written, it does not; rather, it requires the President only to inform Congress of a declaration of a national cyber emergency.[132] Congress may interfere only if the President seeks to extend the declaration of emergency beyond its maximum thirty-day period.[133] Therefore, the bill as currently written lacks the checks necessary to ensure the legitimate exercise of presidential authority. Furthermore, it fails to create a practicable solution to Anonymous- and LulzSec-style cyber attacks. It should not proceed to a floor vote in its current form.

---

129. Jeff Neuburger, *Who Do You Trust? Proposed Cybersecurity Bill Would Encourage Public-Private Cyber Threat Information Exchange by Providing Legal Immunity*, PROSKAUER PRIVACY LAW BLOG (Dec. 22, 2011), http://privacylaw.proskauer.com/2011/12/articles/data-breaches/who-do-you-trust-proposed-cybersecurity-bill-would-encourage-publicprivate-cyber-threat-information-exchange-by-providing-legal-immunity.

130. Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011).

131. *Id.*

132. *Id.* § 249(d)(1).

133. *Id.* § 249(f)(1).

3. House Resolution 2096: Cybersecurity Enhancement Act of 2011

Representative McCaul's Cybersecurity Enhancement Act of 2012 (the R&D Bill) exclusively targets cyber-security research and development.[134] If enacted, the Act will (1) require federal agencies to develop a strategic plan for federal cyber-security research and development, (2) reauthorize cyber-security research at the National Science Foundation, (3) grant scholarships to students studying cyber security in return for their service in the federal government, (4) require the National Institute for Standards and Technology to develop a cyber-security awareness and education program, and (5) mandate the formation of a joint university-industry taskforce to promote and improve collaboration between public and private research efforts.[135]

The extensive research and development programs this bill proposes are necessary to anticipate and correct vulnerabilities in cyber security.[136] But this kind of research creates a dual-use problem that could simultaneously create susceptibilities while also correcting them. Indeed, by identifying weaknesses in security systems and new methods of conducting cyber attacks, the government will effectively enable those working on the projects to become cyber attackers themselves. Therefore, should the President sign this bill into law, lawmakers will have to determine how to minimize this risk while still promoting the research and development efforts that will help thwart future attacks.

4. House Resolution 3523: Cyber Intelligence Sharing and Protection Act of 2011

Because of ambiguities in current cyber security and privacy law, many private actors refrain from sharing cyber threats with their private-sector counterparts for fear of inviting legal liability.[137] Recognizing that the private sector already has substantial anti-cybercrime infrastructures in place, Representative Rogers's Cyber Intelligence Sharing and Protection Act of 2011 (the Cyber Vigilante Bill) simply seeks to grant private actors clearer authority to

---

134. Cybersecurity Enhancement Act of 2012, H.R. 2096, 112th Cong. (2012).

135. Press Release, House Comm. on Sci., Space & Tech., Comm. Approves Bipartisan Cybersecurity Legislation (July 21, 2011), *available at* http://democrats.science.house.gov/press-release/committee-approves-bipartisan-cybersecurity-legislation.

136. *See* H.R. 2096.

137. *See, e.g.*, PRECISE Act of 2011, H.R. 3674, 112th Cong. (2011); Paul Rosenzweig, *Promoting Cybersecurity Through the PRECISE Act*, HERITAGE FOUND. (Feb. 6, 2012), http://www.heritage.org/research/reports/2012/02/promoting-cybersecurity-through-the-precise-act.

detect threats of cyber attacks and to participate in greater information sharing.[138] If adopted, this approach will authorize private-sector entities to (1) defend their own networks and computer systems and (2) share information of cyber-security threats with others in the private sector and the federal government.[139] The federal government will treat any information that private-sector entities share with it as proprietary information that is exempt from disclosure under the Freedom of Information Act.[140]

Furthermore, the bill proposes to expand the Department of Defense's (DOD) Defense Industrial Base Cyber Pilot project, which promotes the federal intelligence community's sharing of cyber-security threats, and the know-how to protect against them, with participating defense companies or their Internet service providers.[141] The bill intends to encourage the federal intelligence community to share classified cyber-threat intelligence with both the private sector and other individuals with the proper security clearances.[142]

5. House Resolution 3674: Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act

Representative Lungren (R-CA) introduced House Resolution 3674 (the Information Sharing Bill) in the House in December 2011.[143] This bill is one of the most recent attempts to ensure cyber security in the United States. Like Senator Lieberman's bill, it proposes the creation of the National Cybersecurity Authority to facilitate information sharing between federal agencies and state and local governments, the private sector, academia, and international entities.[144] This bill will task the Secretary of the DHS with sharing information regarding cyber-security threats and any mitigation efforts with federal agencies, state and local governments, and a class of specifically defined members of the private sector.[145] The bill also proposes to improve the flow of information from the private sector to

138. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (2011).

139. *Id.*

140. *Id.*

141. Press Release, U.S. Dep't of Def., Lynn Outlines New Cyber Security Effort (June 16, 2011), *available at* http://www.defense.gov/news/newsarticle.aspx?id=64349.

142. *Id.*

143. PRECISE Act of 2011, H.R. 3674, 112th Cong. (2011).

144. Neuburger, *supra* note 129.

145. *Id.*

the federal government through the creation of the National Information Sharing Organization.[146]

B. The Government Should Not Regulate Anonymous and LulzSec's Activities under Any of These Proposals

Of the proposals outlined above, all but the R&D Bill have some relevance to Anonymous and LulzSec's activities.[147] Because the R&D Bill focuses only on researching and developing techniques to anticipate and prevent cyber attacks, this section will not discuss it. The R&D Bill will, however, be relevant in the subsequent discussion on preventing cyber terrorism generally.

1. The Government Should Not View Anonymous and LulzSec's Activities as a New Form of Terrorism

The clear purpose of the existing cyber-security proposals is to prevent cyber-terrorist attacks that could cripple the United States' domestic and international business and governmental operations.[148] But neither Anonymous nor LulzSec's activities constitute terrorist attacks;[149] they are merely crimes under the CFAA.[150]

While conduct must necessarily be criminal for the government to deem it terrorist in nature, not all criminal activity constitutes terrorism. Criminal activity by itself is insufficient to give rise to this more extreme label.[151] "Crime" is defined as "an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law, that makes the offender liable to punishment by that law."[152] In contrast, the United States defines "terrorism" as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[153] Similarly, the United Nations General Assembly (UN) defines "terrorism" as "criminal acts *intended or calculated* to provoke a state of terror in the general public, a group of

146. *Id.*

147. *See supra* Part II.A.1-5.

148. *See supra* Part II.A; *see also* Schmidt, *supra* note 6.

149. *See infra* notes 151-156 and accompanying text.

150. Prosecuting this activity as a crime under the CFAA is useless. *See supra* Part II.

151. *See* BILL NELSON ET AL., CYBERTERROR: PROSPECTS AND IMPLICATIONS 12, (1999), *available at* http://www.au.af.mil/au/ awc/awcgate/nps/cyberterror_prospects.pdf ("In general, espionage and criminal activity do not constitute terrorism, and should not be considered part of cyberterrorism.").

152. *Crime Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/crime (last visited Sept. 21, 2012).

153. 22 U.S.C. § 2656(f)(d)(2) (2006).

persons, or particular persons for political purpose . . . ."[154] The key distinction between the US and UN definitions of "terrorism" and the definition of "crime" is the specific intent that policymakers ascribe to terrorists but not to criminals: terrorism requires intent to cause harm and/or fear on political grounds.[155] The definition of "crime," in contrast, does not depend on any specific intent.[156]

Though Anonymous and LulzSec's tendency to leak information and take websites offline for several hours has undoubtedly been disruptive, their doing so has not caused violence or fear to the degree necessary to constitute terrorism.[157] While critics fairly argue that hacktivism is political in nature and that attacks against Visa and MasterCard, among others, sparked fear amongst the general public given the potential for widespread credit-card theft and fraud, members of both groups continue to lack the necessary intent for the government to regard them as terrorists; they have made clear that the sole motive for their activity is to garner "lulz."[158]

One could certainly argue that the definition of lulz is "the joy of disrupting another's emotional equilibrium,"[159] and that fear falls within this wide umbrella, thereby potentially equating an intent to cause lulz with an intent to engage in terrorism. However, the fear typically associated with terrorism is different than fear generally. Indeed, *The Merriam-Webster Dictionary* defines "fear" as "an unpleasant, often strong emotion caused by anticipation or awareness of danger."[160] "Terror," according to *The Merriam-Webster Dictionary*, is a stronger emotion, defined as "a state of *intense* fear."[161] Therefore, the fact that society did not stop the use of credit cards for weeks in the way that it halted air travel in the aftermath of the September 11 terrorist attacks suggests that any fear resulting from the Visa and

154. G.A. Res. 49/60 (I), ¶ 3, U.N. Doc. A/RES/49/60 (Dec. 9, 1994) (emphasis added). The DOD defines "terrorism" similarly: "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological." Jeff Pierce, *Terrorism—A Simplified Explanation*, CIVIL DEF. NET (Nov. 18, 2009), http://www.civildefensenet.org/Open/Terrorism-A%20Simplified%20Explanation.pdf (internal quotation marks omitted).

155. *See supra* notes 152-154 and accompanying text.

156. *See supra* note 152 and accompanying text.

157. *See LulzSec*, WIKIPEDIA, http://en.wikipedia.org/wiki/LulzSec (last updated Sept. 19, 2012); *Anonymous (group)*, WIKIPEDIA, http://en.wikipedia.org/wiki/Anonymous_(group) (last updated Sept. 20, 2012).

158. *See supra* note 1; Anonymous, *supra* note 58.

159. Mattathias Schwartz, *The Trolls Among Us*, N.Y. TIMES, Aug. 3, 2008, http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html?pagewanted=all.

160. *Fear definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/fear (last visited Oct. 19, 2012).

161. *Terror definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/terror (last visited Oct. 19, 2012) (emphasis added).

MasterCard attacks was not intense enough to constitute a "state of terror" as the UN requires.[162] Thus, unless and until Anonymous and LulzSec's intent changes, the government can deem their activity criminal, but not terroristic.

However, the potential for Anonymous to adopt a more nefarious purpose in subsequent attacks still remains.[163] But for the government to deem a threat credible, such that it can exercise anti-terrorism measures to preemptively thwart it, intent to commit a terrorist act should already exist.[164] Given the absence of intent in this case, to label the groups' activities as a form of warfare (as the Pentagon did with respect to LulzSec) and to regulate against them is misguided.

2. If Enacted, the Proposals Will Not Effectively Deter Anonymous and LulzSec's Hacking Activities

Even if Congress enacts either the White House proposal criminalizing hacking, the Lieberman Bill, the Cyber Vigilante Bill, or the Information Sharing Bill, these bills will likely prove ineffective in curbing Anonymous and LulzSec's activities. The primary motivation for many of Anonymous and LulzSec's members skews toward a desire to show off and garner praise from peers.[165] Assuming prosecutors can identify the perpetrators of cyber attacks, which in all likelihood they cannot, the threat of penalties will probably not be an effective deterrence.[166] Enhanced defensive mechanisms may serve as an additional incentive; the greater the difficulty of the hack, the greater the lulz.[167] Consequently, the effectiveness of the proposals is limited.

3. Despite Statements to the Contrary, Lawmakers May Not Actually Intend to Use These Proposals to Target Members of Anonymous and LulzSec

Despite the Pentagon's characterization of hacks for lulz as acts of war, these existing proposals are not designed to combat Anonymous' and LulzSec's activities. Rather, Congress and the White House may be using the media frenzy surrounding both groups'

---

162. *See supra* note 155.

163. *See, e.g.*, Byron Acohido, *Hacktivist Attacks Grow, Get Political*, USA TODAY, July 24, 2012, http://www.usatoday.com/MONEY/usaedition/2012-07-25-Hacktivism-Surges_CV_U.htm.

164. *See supra* notes 151-158 and accompanying text.

165. Rashid, *supra* note 115.

166. *Id.*

167. *See generally id.*

activities to push an alternate agenda. Indeed, both entities may be seeking to bring the federal government's authority to engage in domestic anti-cyber terrorism operations in line with its already extensive international authority.

Since the September 11 terrorist attacks, the US government has emphasized combating the threat of cyber terrorism.[168] In June 2009, the Secretary of Defense instructed the Director of US Strategic Command to create as a sub-entity the US Cyber Command.[169] This Command is responsible for:

> [P]lanning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations . . . in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.170

Peter Wood, operations chief with First Base Technologies and an expert in cyber-warfare, stated:

> [T]he only way to counteract both criminal and espionage activity online is to be proactive. If the US is taking a formal approach to this, then that has to be a good thing. The Chinese are viewed as the source of a great many attacks on western infrastructure and, just recently, the US national grid. If that is determined to be an organised attack, I would want to go and take down the source of those attacks.171

This statement, coupled with others, suggests that this arm of the DOD has the authority to combat threats from abroad.[172]

But under the Posse Comitatus Act, state and local governments and law enforcement agencies cannot use federal

---

168. *See The Comprehensive National Cybersecurity Initiative*, WHITE HOUSE, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (last visited Sept. 21, 2012).

169. The US Strategic Command is one of nine Unified Combatant Commands of the DOD that the government has established to provide effective command and control of US military forces in both times of peace and war. *U.S. Cyber Command*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command (last updated Dec. 2011). ANDREW FEICKERT, CONG. RESEARCH SERV., R42077, THE UNIFIED COMMAND PLAN AND COMBATANT COMMANDS: BACKGROUND AND ISSUES FOR CONGRESS 19 (2012), *available at* http://www.fas.org/sgp/crs/natsec/R42077.pdf (regarding the instruction to create the US Cyber Command).

170. *Id.*

171. *US Needs 'Digital Warfare Force'*, BBC NEWS (May 5, 2009, 2:47 PM), http://news.bbc.co.uk/2/hi/technology/8033440.stm (internal quotation marks omitted).

172. For example, Lt. Gen. Keith Alexander, Commander of the new Cyber Command, promoted a US military cyberattack that dismantled an online forum operated for intelligence-gathering by Saudi Arabia and the CIA in 2008 because of evidence suggesting that extremists were using the forum to plan attacks. *See* Ellen Nakashima, *Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies*, WASH. POST, Mar. 19, 2010, www. washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html; *see also Military Asserts Right to Return Cyber Attacks*, CBS NEWS (Apr. 14, 2010, 11:07 AM), www. cbsnews.com/2100-205_162-6394031.html ("The U.S. must fire back against cyber attacks swiftly and strongly and should act to counter or disable a threat even when the identity of the attacker is unknown, [Lt. Gen. Alexander] told Congress.").

military personnel to enforce the laws of the land without explicit authorization either in the US Constitution or from Congress.[173] The relevant text of the Act states:

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.174

Currently, only the FBI possesses the necessary authority to engage in cyber-security operations to protect national security domestically.[175] The federal government may be attempting to create an analog to the US Cyber Command within the DHS to permit the US government to act within the United States, independently of the FBI.[176]

Notably, the White House Proposal, the Lieberman Bill, and the Information Sharing Bill all explicitly mention an enhancement of the DHS's authority in the cyber-security sphere.[177] Furthermore, both the Senate and House bills, of which the former has received White House backing, propose the creation of an organization within the DHS's umbrella specifically charged with protecting against cyber-security attacks.[178] Thus, while the federal government appears to be targeting Anonymous- and LulzSec-style activities, it may actually be using the buzz surrounding the group to fill a hole in US domestic policy.[179] Whether the federal government will prosecute attacks for lulz once the legislation passes is uncertain given that prosecution of these crimes may not be the intended goal. However, if the government does prosecute, it will probably target only hacking that poses an actual threat to homeland security.[180]

---

173. 18 U.S.C. § 1385 (2006).

174. *Id.*

175. *Addressing Threats to the Nation's Cybersecurity*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1 (last visited Oct. 4, 2012).

176. *See infra* notes 177-82 and accompanying text.

177. PRECISE Act of 2011, H.R. 3674, 112th Cong. § 2 (2011); Cybersecurity and Internet Freedom Act of 2011, S. 413 § 101(a)(3), 112th Cong. (2011); OFFICE OF MGMT. & BUDGET, *supra* note 115.

178. H.R. 3674; S. 413.

179. *See supra* Part II.B.

180. *See* Rashid, *supra* note 115 ("No matter how disruptive a denial of service attack can be on a site, it is not necessarily on the same level of seriousness as someone 'intent on threatening national security by stealing highly sensitive information.'").

C. The Deficiencies in Each of These Proposed Solutions With Respect to Cyber Terrorism

While Anonymous and LulzSec may not be the targets of these proposals, the organizational structure and the methods of attack they use is relevant to the broader discussion of preventing cyber terrorism. The remainder of this Note will consider the efficacy of these proposed amendments should terrorist organizations model their attacks on those that Anonymous and LulzSec have executed.

1. The White House Proposal, the Lieberman Bill, and the Information Sharing Bill: All Inadequate Proposals

Though well intentioned, the White House Proposal, the Lieberman Bill, and the Information Sharing Bill are inadequate attempts to combat cyber-terrorist groups using Anonymous's structure.[181] The more amorphous the hacking group's makeup, the more difficult it is to identify the culprits. Therein lies the structural distinction between Anonymous and LulzSec: because LulzSec used a formal website to launch its attacks, hackers were able to breach its network and uncover the members' identities, thus leading to the arrest of several key leaders.[182] LulzSec has since disbanded, and law enforcement officials worldwide have arrested many of its alleged top members, suggesting that groups that depend on a home-base website to coordinate attacks are vulnerable when law enforcement officials arrest those individuals.[183] Because of the built-in anonymity and the resulting protection from prosecution that Anonymous's structure provides, it is logical that terrorist organizations seeking to engage in cyber terrorism will adopt the model Anonymous uses.

Because leaders of cyber attacks often post the procedure for attacks on message boards like 4chan, which only tracks users' IP addresses, it is nearly impossible to identify every individual involved in the attack.[184] Indeed, only IP addresses for users who post details

---

181. *See supra* Part II.B.1-2.

182. Two Americans have been charged with being members of LulzSec. *See* Rebecca Camber et al., *British Teenager Charged Over Cyber Attack on CIA as Pirate Group Takes Revenge On 'Snitches Who Framed Him'*, MAIL ONLINE (June 22, 2011, 2:34 PM), www.dailymail.co.uk/sciencetech/article-2006118/Ryan-Cleary-charged-cyber-attack-CIA-LulzSec-takes-revenge.html; *see also supra* Part I.B.1-2; Graham Cluley, *LulzSec Hacking Suspect 'Topiary' Arrested in the Shetland Islands*, NAKED SEC. (July 27, 2011), nakedsecurity.sophos.com/2011/07/27/suspected-hacker-arrested-in-shetland-islands; Jana Winter, *FBI Arrests Suspected LulzSec and Anonymous Hackers*, FOX NEWS (Sept. 22, 2011), www.foxnews.com/scitech/2011/09/22/fbi-arrests-suspected-lulzsec-and-anonymous-hackers.

183. *See* Rao, *supra* note 102 (indicating that LulzSec has been disbanded).

184. 4CHAN, http://www.4chan.org/faq (last visited Feb. 24, 2011).

of the attack or in response to a call to attack are traceable. The hundreds of individuals who participate in an attack without posting about it can never be traced. Furthermore, because hackers can falsify their IP addresses,[185] individuals who post on message boards will likely be untraceable.[186] Finally, even if law enforcement officials can properly ascertain the identities of those who posted, they cannot easily determine who hacked the master computer to carry out the attack.[187] Terrorist organizations can thus tap into the broad pockets of anti-American sentiment worldwide and enlist the assistance of hackers whom law enforcement officials can never catch. Therefore, the Obama administration's proposal to impose a mandatory-minimum three-year penalty[188] appears to miss the mark because its more stringent standard is difficult, if not impossible, to enforce.

Increased information sharing will be difficult to realize in practice given that terrorist organizations communicate in many languages using creative codes.[189] The number of analysts required to monitor all terrorist hotbeds and disseminate relevant information to the appropriate private-sector entities will require substantial federal resources and cooperation among multiple federal agencies and departments (including, *inter alia*, the CIA, the DOD, and the DHS). Thus, the Information Sharing Bill's effectiveness will be dependent on the federal government's commitment of funds to cyber security in the annual budget.[190] Given lawmakers' current efforts to trim the budget (and the defense budget in particular[191]) and the 2012 presidential candidates prominently discussing fiscal responsibility,[192]

---

185. Jack Cola, *How to Make a Fake IP Address & Mask Yourself Online*, MAKE USE OF (Nov. 27, 2009), http://www.makeuseof.com/tag/how-to-mask-yourself-online-use-a-fake-ip-address.

186. Between 2009 and 2010, Anonymous members increasingly began to use the Low Orbit Ion Canon (LOIC), which attackers can program to carry out their DDoS attacks automatically. 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/3. But the LOIC does not hide attackers' IP address. *Id.* Consequently, if the owners of the attacked site turn server logs over to the authorities, some attackers who fail to mask their IP addresses could be identified and thus face legal liability. *Id.* However, the sheer magnitude of the attacking cohorts renders the majority of attackers safe from identification and prosecution. *Id.*

187. *See* notes 32-35 and accompanying text.

188. OFFICE OF MGMT. & BUDGET, *supra* note 115, at 1.

189. Gabriel Weimann, *How Modern Terrorism Uses the Internet*, J. OF INT'L SECURITY AFF. (Spring 2005), http://www.securityaffairs.org/issues/2005/08/weimann.php.

190. *See* PRECISE Act of 2011, H.R. 3674, 112th Cong. (2011).

191. Binyamin Applebaum, *A Shrinking Military Budget May Take Neighbors With It*, N.Y. TIMES, Jan. 6, 2012, http://www.nytimes.com/2012/01/07/us/a-hidden-cost-of-military-cuts-could-be-invention-and-its-industries.html.

192. *See Fiscal Responsibility*, MITT ROMNEY FOR PRESIDENT, http://www.mittromney.com/issues/fiscal-responsibility (last accessed Sept. 21, 2012); Matt Friedman, *N.J. Sen. Kyrillos*

this program may not be a priority. Additionally, because the Information Sharing Bill is dependent on an annual federal government budget allocation, future administrations may revoke funding should they choose not to value the bill as highly as the Obama and Bush administrations have in the last decade.[193] The Information Sharing Bill therefore lacks the reliability necessary to be effective.

Finally, the Lieberman Bill is too reactionary to be effective in preventing cyber-terrorist attacks.[194] Hacking techniques are increasingly sophisticated, and successfully counteracting a completed hack can be difficult.[195] Rather than focusing solely on the scope of the President's authority in the event of a cyber attack, the federal government should place equal, if not more, emphasis on what it can do to preempt cyber attacks.

2. Both Congress and President Obama's Proposals Provide a Necessary Foundation, but Congress Must Expand upon Them to Ensure Their Effectiveness

Of the proposals outlined thus far, the most promising is the Cyber Vigilante Bill. It recognizes that criminalizing cybercrime and further regulating how the private sector anticipates and responds to cyber threats will not effectively thwart cyber-terrorist activity.[196] Rather, with their existing cyber-security infrastructures, private entities are best equipped to protect themselves from cybercrime.[197] The sponsors of the Cyber Vigilante Bill recognized this and have attempted to clearly delineate and enhance private-sector entities' authority to do so.[198] The bill, however, cannot be successful on its own, because it does not mandate that the federal government's intelligence community share newly discovered cyber threats with the private sector.[199] Because the sharing of information is voluntary

---

Talks Fiscal Responsibility in Launch of U.S. Senate Campaign, NJ.COM (Feb. 1, 2012, 1:55 PM), http://www.nj.com/news/index.ssf/2012/02/nj_sen_kyrillos_preaches_fisca.html; *Santorum Comments on Obama Budget Proposal*, RICK SANTORUM FOR PRESIDENT, http://www.ricksantorum.com/pressrelease/santorum-comments-obama-budget-proposal (last visited Feb. 24, 2012).

193. *See The Comprehensive National Cybersecurity Initiative*, *supra* note 168 (outlining both President Obama and former President Bush's commitment to cyber security).

194. *See* Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011).

195. William J. Lynn III, *Defending a New Domain*, FOREIGN AFFAIRS (Sept./Oct. 2010), http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

196. *See* Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523 § 2, 112th Cong. (2011).

197. H.R. REP. NO. 112-445, at 5-6 (2011).

198. *Id.* at 5.

199. *See* H.R. 3523.

under this bill, if Congress and the President enact it, private-sector entities that cannot afford to employ their own analysts to discover and assess the danger of possible threats will face difficulties with respect to threat assessment.[200] Indeed, the breadth of the Internet and the number of languages and codes available to terrorists render such efforts cost prohibitive for these companies. Additionally, continuous technical research testing the impenetrability of computer networks would add to companies' cost of protecting their systems from new hacking techniques.

Representative McCaul (R-TX) anticipated this need for technical research, proposing in the R&D Bill that the federal government develop a strategic plan for coordinating cyber-security research and development across agencies.[201] But because this bill focuses solely on research and development and neglects to empower private-sector entities to protect themselves, it, too, fails to effectively combat the threat of cyber terrorism.[202]

III. HOW TO SOLVE AN UNSOLVABLE PROBLEM?

Hacking techniques are constantly evolving, rendering previously impenetrable networks penetrable.[203] The innovative nature of the field coupled with the use of sophisticated communication methods suggests that the legislative proposals discussed above, without more, cannot anticipate vulnerabilities quickly enough to be preventive.[204] They all possess crucial elements of a more effective cyber-security policy, including mandatory sharing of cyber threats and a focus on research and development to continuously secure computer networks against new hacking techniques.[205] But no single bill contains all of these elements. By combining several elements from these existing bills and building upon them, however, Congress could formulate new legislation that emphasizes cybercrime prevention, rather than troubleshooting.

The Cyber Vigilante Bill, which authorizes private-sector entities to defend themselves against cyber attacks, provides the best foundation upon which to build a new proposal.[206] Because

200. *See id.*

201. Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 103 (2011).

202. *See id.*

203. *Different Types of Hacking Techniques*, HACKING TECHNIQUES (Nov. 12, 2011, 5:32 AM), http://hackingtechniques.org/different-types-of-hacking-techniques.

204. *See supra* Part II.A.

205. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. § 2 (2011); Cybersecurity Enhancement Act of 2011, H.R. 2096, 112th Cong. (2011).

206. H.R. 3523.

perpetrators of Anonymous-style attacks are virtually undetectable, both public- and private-sector entities must attempt to anticipate and thwart cybercrime before it occurs.[207] Given that software developers construct each server, computer, and device differently, the group of individuals that can most effectively protect against hacking is probably the group of developers who initially constructed the server, computer, or network. Therefore, Congress can establish the best protection scheme by permitting entities to defend themselves, as the Cyber Vigilante Bill does.[208] Janet Napolitano, Secretary of the DHS, seems supportive of this endeavor, indicating that she might be willing to permit private companies to engage in "proactive" cyber vigilantism against international hackers.[209]

Although the bill establishes important cyber-security protections, lawmakers should nonetheless modify the Cyber Vigilante Bill extensively. Foremost among these amendments, Congress should propose the creation of a cyber-security arm within the DHS, as proposed in the Lieberman Bill and the Information Sharing Bill and endorsed by the White House, to serve as a domestic analog to the DOD's Cyber Command. Homegrown cyber threats may be as prevalent as those emanating abroad.[210] The DHS should therefore maintain a dedicated group to monitor and defend against domestic threats.

A. Keep Friends Close, Keep Enemies Closer: Allying Anonymous and LulzSec in the Struggle to Contain Cyber Terrorism.

Once established, Congress should charge the DHS's cyber-security arm with overseeing extensive cyber-security research and development efforts per the R&D Bill. To be effective, both public- and private-sector entities must anticipate novel hacking techniques and update their security systems accordingly. As part of

---

207. *But see* Jana Winter, *FBI Arrests Suspected LulzSec and Anonymous Hackers*, FOX NEWS (Sept. 22, 2011), www.foxnews.com/scitech/2011/09/22/fbi-arrests-suspected-lulzsec-and-anonymous-hackers (noting that a suspected member of Anonymous was arrested, that these arrests are rare, and that they largely depend on insider knowledge).

208. *See* H.R. 3523 § 2.

209. Steve Johnson, *Homeland Security Chief Contemplating Proactive Cyber Attacks*, MORNINGSTAR (Apr. 17, 2012 9:40 AM), http://news.morningstar.com/all/acquire-news/ff80808 1369ada980136c08a488d6937/homeland-security-chief-contemplating-proactive-cyber-attacks-san-jose-mercury-news-calif.aspx; Tim Maurer, *Breaking Bad*, FOREIGN POL'Y (Sept. 10, 2012), http://www.foreignpolicy.com/articles/2012/09/10/breaking_bad.

210. Indeed, several alleged members of LulzSec and Anonymous are Americans. Matt Liebowitz, *LulzSec Leader 'Sabu' Speaks About Life on the Run*, TECH NEWS DAILY (Oct. 10, 2011, 5:53 PM), http://www.securitynewsdaily.com/1127-lulzsec-leader-sabu-speaks-about-life-on-the-run-.html.

this effort, Congress should set aside its desire to bring Anonymous and LulzSec members to justice for their previous crimes and instead enlist their efforts to expose flaws both in the federal government and in
private-sector companies' security systems. Hacking requires creative instincts and a complete understanding of computer programming that government employees cannot learn in a training program. Therefore, while the DHS can train analysts to combat hacks in a manner similar to that of the DOD,[211] hackers-turned-government-consultants are a better choice. They bring with them the same mindset that hackers working against the government will employ and are thus best equipped to anticipate their opponents' next moves.

The use of the general public to solve difficult problems is not new. Scientists at the University of Washington have used Foldit—a collaborative online game designed to enlist the help of the public to solve problems deemed too great for researchers and advanced computers to tackle alone—to discern the protein structure of a retrovirus similar to HIV.[212] This protein structure, an understanding of which will help the treatment of AIDS, confounded researchers for over ten years.[213] Foldit gamers solved the structure in less than ten days.[214] Other researchers have garnered assistance from the general public in identifying planets, classifying galaxies, deciphering ancient texts, and building climate models.[215] Capitalizing on the skill sets of hundreds of expert hackers can only assist the government in its effort to prevent crippling cyber-terrorist attacks.

Despite the secrecy that hackers rely upon to be successful, there is a slowly growing movement amongst hackers to turn against Anonymous—and LulzSec, when it existed—to reveal information about other hackers.[216] It may therefore become increasingly difficult

---

211. Mark Thompson, *To Battle Computer Hackers, the Pentagon Trains Its Own*, TIME (Mar. 18, 2010), http://www.time.com/time/nation/article/0,8599,1972896,00.html.

212. Zoran, *Recent Exciting Discoveries by Foldit*, FOLDIT (Apr. 19, 2011 5:15 PM), http://fold.it/portal/node/989576; *see also* Collins Kilgore, *Gaming for the Greater Good*, VAND. J. ENT. & TECH. L. BLOG (Sept. 27, 2011) http://www.jetlaw.org/?p=8381.

213. Zoran, *supra* note 212.

214. Alan Boyle, *Gamers Solve Molecular Puzzle That Baffled Scientists*, COSMIC LOG (Sept. 18, 2011, 1:00 PM), http://cosmiclog.msnbc.msn.com/_news/2011/09/16/7802623-gamers-solve-molecular-puzzle-that-baffled-scientists.

215. *Ancient Lives Research*, ANCIENT LIVES, http://ancientlives.org/research (last visited Feb. 24, 2012); *Humans vs. Machines*, PLANETHUNTERS, http://www.planethunters.org/science# human (last visited Feb. 24, 2012); *The Story So Far*, GALAXY ZOO, http://www.galaxyzoo.org/ #/story (last visited Feb. 24, 2012); *Why Scientists Need You*, OLD WEATHER, http://www.old weather.org/why_scientists_need_you (last visited Feb. 24, 2012).

216. Josh Halliday, *LulzSec Site Take Down by Lone-Wolf Hacker*, GUARDIAN (June 24, 2011, 5:13 PM), http://www.guardian.co.uk/technology/blog/2011/jun/24/lulzsec-site-down-hacker-

for hackers to remain anonymous. Indeed, in the last year, four independent entities have taken credit for uncovering and circulating the identities of Anonymous and LulzSec members.[217] These groups have released to the authorities LulzSec's private Internet Relay Chat logs and the names and identities of alleged members of the two groups, largely in an effort to give Anonymous and LulzSec a taste of their own lulz.[218] Furthermore, Sabu, a former high-ranking member of LulzSec who stated that "the ironic twist will be that my own friends will take me down" has aided government investigations against both groups following his arrest.[219] Experts predict that mistrust will grow within Anonymous.[220]

Government collaboration with Anonymous and LulzSec members may be feasible, despite criticisms that doing so is impractical and unjust. First, members of the groups may prefer to avoid prosecution by accepting a job with the US government.[221] Second, many of the participating members of Anonymous and LulzSec probably fall within the 18–30 age bracket, which faces one of the highest unemployment rates in the United States.[222] Along with the threat of prosecution, the prospect of a well-paying job could provide the incentive necessary to draw these hackers to the ranks of government employees.

---

jester; Alexander Higgins, *A-Team Hacker Group Leaks Alleged Identities of 10 LulzSec and Anonymous Members*, ALEXANDER HIGGINS BLOG (June 26, 2011, 11:43 AM), http://blog.alexanderhiggins.com/2011/06/26/ateam-hacker-group-leaks-alleged-identities-lulzsec-anonymous-hacker-group-members-31251; Jeff Hughes, *Hacker Vigilantes Web Ninjas Lashing Out At LulzSec*, DIGITAL TRENDS (June 21, 2011), http://www.digitaltrends.com/computing/web-ninjas-hacker-vigilantes-lashing-out-at-lulzsec; Colin Tan, *Hacker Group LulzSec Becomes Victim of Hack*, GAMINGUNION.NET (June 24, 2011, 6:20 PM), http://www.gamingunion.net/news/hacker-group-lulzsec-becomes-victim-of-hack--5565.html.

217. *Supra* note 216 and accompanying text.

218. Charles Arthur & Ryan Gallagher, *LulzSec IRC Leak: The Full Record*, GUARDIAN (June 24, 2011, 9:17 AM), http://www.guardian.co.uk/ technology/2011/jun/24/lulzsec-irc-leak-the-full-record; Gallagher & Arthur, *supra* note 81.

219. Liebowitz, *supra* note 210 (internal quotation marks omitted); *see* Somini Sengupta, *Arrests Sow Mistrust Inside a Clan of Hackers*, N.Y. TIMES, Mar. 6, 2012, http://www.nytimes.com/2012/03/07/technology/lulzsec-hacking-suspects-are-arrested.html.

220. Sengupta, *supra* note 219.

221. Sabu, for example, was willing to cooperate with the FBI in at least tracking down his co-conspirators, and he may have been content to continue his activities under FBI direction. *Id.*

222. Press Release, Bureau of Labor Statistics, The Employment Situation—August 2012 (Sept. 7, 2012), *available at* http://www.bls.gov/news.release/pdf/empsit.pdf (using Table A-10 to show the unemployment rates for workers 16–19 years old (24.6 percent), 20–24 (13.9 percent), 25–54 (7.1 percent), and 55 and over (5.9 percent)). *See, e.g.*, Quinn Norton, *How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down*, WIRED (July 3, 2012, 6:30 AM), http://www.wired.com/ threatlevel/2012/07/ff_anonymous (suggesting that those arrested in connection to Anonymous activities were generally between their late teens and mid-thirties).

While it may be difficult to identify every hacker who participates in a DDoS attack, the leaders of attacks will likely have to communicate with each other. Because Anonymous and LulzSec members are able to infiltrate their fellow hackers' preferred methods of communication, they are better able to bring perpetrators of cyber terrorism to justice. The currently growing cyber-vigilante movement in which hackers are identifying other hackers is undoubtedly small in comparison to the number of Anonymous members worldwide.[223] But the government has relied on criminals-turned-friends before, with much success, and the government generally accepts the idea of doing so.[224] Indeed, four-star General Keith Alexander, head of the National Security Administration, recently told thousands of hackers, professional defenders, and software researchers at the annual Def Con conference, "You're going to have to come in and help us . . . ."[225] These groups therefore represent the way forward as the United States seeks to protect itself from cyber terrorists.

B. Greater Public- and Private-Sector Interaction Is Necessary.

A successful plan to curb cyber-terrorism threats will require greater public- and private-sector interaction. Per section 244(a) of the White House proposal, Congress should grant the DHS's cyber-security program the authority to extend programmatic support when needed to assist, upon request, with breaches of security networks. Furthermore, Congress should permit the cyber-security program to provide updates on methods to combat innovations in hacking techniques. Because the cyber-security program will only exercise this authority upon request, it will better manage the balance between ensuring security and violating an individual's right to privacy than if the DHS could become involved at will.

By combining and expanding upon elements from Congress and the White House's already-existing proposals, Congress can create a law that may not die in committee as its predecessors have. Furthermore, this new proposal corrects many of the limitations and ambiguities in the CFAA, thereby making more effective

---

223. Indeed, as far as authorities can tell, Jester (one of the more famous anti-Anonymous and -LulzSec vigilantes) was just one person. TJ O'Connor, *The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare*, SANS INST. (Dec. 30, 2011), http://www.giac.org/paper/gcpm/298/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare/121884.

224. Joseph Menn & Jim Finkle, *Spy Chief Asks Hackers to Help Government to Secure Internet*, REUTERS (July 27, 2012, 1:15 AM), http://www.reuters.com/article/2012/07/27/net-us-usa-security-hackers-idUSBRE86Q1KM20120727.

225. *Id.*

anti-cyber-terrorism measures possible. But the proposal is not complete because it does not require the federal government to disclose to other public or private entities specific threats against them. Rather, while the government has deemed sharing information appropriate, doing so is ultimately only voluntary. Omitting this provision from a new bill is the compromise necessary to achieve the greater goal: protecting against cyber terrorism.

Private-sector stakeholders will therefore need to collaborate with the federal government to reach an agreement regarding when disclosure will be mandatory, if at all. While information sharing could strengthen the effort to preempt cyber terrorism, requiring it could create a free-rider problem. Companies may lazily defer all cyber-threat analysis activities to the government. Such reliance would impose upon the federal government a heightened risk of liability. Indeed, should it fail to disclose a threat in time, the recipients of the information could attempt to hold the government responsible for the consequences of the attack.[226] But if the government does not require information sharing in at least some situations, smaller organizations that lack the resources necessary to effectively monitor both domestic and international threats will be more vulnerable to attacks. Consequently, the government and private companies will have to jointly formulate legislation to effectively and fairly regulate this middle ground.

IV. CONCLUSION

Though neither Anonymous nor LulzSec likely poses a threat to US security, Anonymous's organizational structure creates novel challenges for anti-terrorism professionals seeking to prevent cyber-terrorist attacks. With no viable way to ascertain the identities of the perpetrators, law enforcement agencies must explore alternative deterrence mechanisms to minimize the threat of attack. Legislating against an untraceable enemy, however, is difficult, as evidenced by the failure of five previous proposals to make it to a floor vote in Congress.[227]

The proposed bill advocated in this Note, which combines and expands upon the best features of previous governmental efforts, balances the need for individual autonomy and privacy with the need to ensure cyber security better than previous proposals. Specifically,

---

226. The United States can be held liable as a defendant for tort claims caused by the negligence of federal employees acting within the scope of their employment. 28 U.S.C. § 1346(b). The contours of this law, and whether governmental failure to disclose a terrorist threat could lead to governmental tort liability in practice, are beyond the scope of this Note.

227. *See supra* Part II.A.

the bill permits private companies and organizations to work independently to prevent cyber-security breaches. Furthermore, Congress should create a cyber-security team within the DHS to monitor and defend against domestic cyber-security threats. Most importantly, however, this Note recommends that the government enlist Anonymous and LulzSec members as consultants who will work to preempt cyber-security attacks. The cyber-vigilante movement has shown that accomplished hackers can effectively and efficiently discover the identities of attack leaders. Therefore, while permitting hackers to become federal employees may be a radical solution, it may be the only viable option unless and until computer scientists develop technology to track and identify cyber terrorists.

Swathi Padmanabhan[*]

* J.D. Candidate, Vanderbilt University Law School, 2013; A.B., Public Policy Studies, Duke University, 2010. The Author expresses her heartfelt gratitude to her parents and brother for their unconditional love and support. Without them, this Note would not be possible. In addition, the author wishes to thank Jeremy Block for his feedback during the writing process, as well as Jeremy Gove, Francie Kammeraad, Mike Dearington, and Shane Valenzi of the VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW for their invaluable edits.