YOUNG FELLA, IF YOU'RE LOOKING FOR TROUBLE I'LL ACCOMMODATE YOU[1]: DEPUTIZING PRIVATE COMPANIES FOR THE USE OF HACKBACK

Zach West[†]

CONTENTS

INTRODUCTION 119
I. WE STAND AT A CROSSROADS 122
A. "They're Stealing Everything Not Bolted Down" 123
B. It's Going to Get Worse Before It Gets Better 124
II. WHO SHOULD RESPOND, AND HOW? 124
A. The U.S. Government 125
B. Law Enforcement 127
C. The Private Sector 128
D. Taking Responsibility 130
III. WELCOME TO THE WILD WEST: SELF DEFENSE IN CYBERSPACE 130
A. "Yes, It's Illegal, but So Was Rosa Parks Sitting in Front of the Bus" 131
B. The Benefits of Hackback 133
C. The Problem with Hackback 135
IV. TAMING THE WILD WEST 138
A. The CFAA: There's a New Sheriff in Town 138
B. Meet My New Deputy 139
C. Making the Case 142
CONCLUSION 145

INTRODUCTION

A computer operator sits in front of a computer screen, monitoring a tank of toxic chemicals.[2] A series of computers control the tank's physical hardware. All of a sudden, the lights in the control room fail, the computers go offline, and the computer operator yells, "[t]hey're

1. TRUE GRIT (Paramount Pictures 1969).

† Juris Doctor Candidate 2013, Syracuse University College of Law.

2. Ellen Nakashima, *Homeland Security Tries To Shore Up Nation's Cyber Defenses*, WASH. POST, Oct. 1, 2011, http://www.washingtonpost.com/world/national-security/homeland-security-tries-to-shore-up-nations-cyber-defenses/2011/09/27/gIQAtQ6bDL_story.html.

hitting one of our servers!"[3] Hundreds of miles away, a team of hackers hired by Barney Advanced Domestic Chemical Co. ("BAD Company") stare as lines of code scroll by on their laptops.[4] BAD Company has just infiltrated and taken command of their business rival's servers.[5] With the click of a mouse, hackers from BAD Company order the toxic chemical tanks to overflow.[6] Toxic chemicals seep out of the tanks and contaminate the surrounding countryside.[7] The computer operators immediately call for a hazmat team.[8] The exercise ends.[9]

This episode was just a Department of Homeland Security ("DHS") cybersecurity exercise, but it highlights a massive national security threat: the ability for malicious computer code to infiltrate computer systems, cripple critical infrastructure, and steal massive quantities of intellectual property.[10] The United States National Counterintelligence Executive ("ONCIX") noted that "[s]ensitive [U.S.] economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries."[11] The loss of this technology has already cost the United States ("U.S.") anywhere from $2 billion to $400 billion.[12] Furthermore, the pace of U.S. data loss is increasing.[13] Foreign intelligence services, private individuals, and foreign corporations have increased their efforts directed at stealing intellectual property, costing U.S. companies millions of dollars in development costs and tens or hundreds of millions of dollars in potential profits.[14]

There is no doubt that these cyber threats pose a huge problem for both the U.S. government and U.S. companies. How, then, can we effectively prevent these threats? Should we pour more money into network defenses? Should we focus on attack response and recovery

3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. Nakashima, *supra* note 2.
8. *Id.*
9. *Id.*
10. *Id.*
11. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECON. SECRETS IN CYBERSPACE, Report to Cong. on Foreign Econ. Collection and Industr. Espionage, 2009-2011, i (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [hereinafter "FOREIGN SPIES"].
12. *Id.* at 4.
13. *Id.* at 1.
14. *Id.*

from the inevitable network penetration?[15] Should we pursue an offensive doctrine that establishes a deterrent policy? Perhaps the best approach is a combination of all three?

Furthermore, who should prevent these intrusions? Should the U.S. government protect private networks, and does it have the legal ability to do so? Should U.S. companies shoulder the burden of protecting themselves? Do we want to empower companies to defend themselves outside their own perimeters?[16] If so, how far does a company's ability to defend itself extend?

These questions highlight a disturbing reality: many of the networks that control our electricity, water, financial systems, and other critical industries operate in a largely unregulated and unprotected cyberspace.[17] In fact, cyberspace has drawn comparisons to the American Wild West; in both areas, black hat criminals have taken advantage of the lawlessness of their respective domains.[18] To bring order to this chaos and tame the Wild West, private companies must have the ability to protect themselves in cyberspace. As such, this note advocates for a form of cyber self-defense called active defense. Active defense, colloquially known as "hackback," is when a targeted entity uses a counter-cyberattack against an attacker's system, thereby stopping the cyberattack in progress and discouraging future attacks.[19]

Part I of this note will analyze the cyber threat that both the U.S. government and U.S. companies currently face. Part II will consider who is best suited to respond to these cyber threats—whether it is the private or the public sector—and what options each entity can pursue. Part III assesses how the law of self-defense applies in cyberspace, paying particular attention to both the benefits and drawbacks of hackback. Part IV transitions to a discussion of the Computer Fraud and Abuse Act ("CFAA"), the basic federal anti-hacking statute, and

15. Gen. Michael V. Hayden, *The Future of Things "Cyber"*, 5 STRATEGIC STUD. Q. 3, 5 (2011), www.au.af.mil/au/ssq/2011/spring/spring11.pdf.

16. *Id.*

17. *See* Greg Y. Sato, *Should Congress Regulate Cyberspace?*, 20 HASTINGS COMM. & ENT L.J. 699, 709 (1998) ("the Internet is highly unregulated; cyberspace is not subject to any central control and operates without any supervision . . . Since there is no supervising or police-like authority which overlooks activity on the Internet, 'anything goes' in cyberspace"); *see also In Praise of Chaos: Governments' Attempts to Control the Internet Should be Resisted*, ECONOMIST, Oct 1, 2011, *available at* http://www.economist.com/node/21531011 ("For something so central to the modern world, the internet is shambolically governed . . . It is in short a bit chaotic.").

18. Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 60 (2005).

19. Alexander Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses*, 20 CARDOZO J. INT'L & COMP. L. 537, 538-40 (2012).

explains how the Department of Justice ("DOJ") might view hackback.[20] In doing so, I will propose a legal framework that allows companies to hackback under a deputy arrangement with the U.S. government, providing the benefits of hackback with the oversight of government regulation.

I. WE STAND AT A CROSSROADS

A 2009 report from the American Bar Association concluded that the U.S. stands at a crossroads: "the decisions we make [on cyberspace] today will help determine the defining images of [cyberspace] tomorrow."[21] Indeed, the U.S. must decide how to defend its cyberspace today in order to ensure the security of its cyberspace tomorrow. However, before choosing that method of defense, we must understand the extent of the threat from both cyberattacks and cyberexploitation.

What exactly is a cyberattack? "Cyberattack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[22] The Department of Defense ("DOD") views such computer sabotage as an act of war, and reserves the right to respond using traditional military force.[23] Cyberexploitation, on the other hand, refers to the collection of confidential information[24] to monitor foreign governments and/or engage in intellectual property theft by "penetrating the computer systems of a competing nation's major industrial firms."[25] Both companies and government agencies face cyberexploitation.[26] This note will focus on how U.S. companies deal with cyberexploitation, and more specifically, on the intellectual property theft dimension of cyberexploitation.

20. *See generally* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

21. PAUL ROSENZWEIG, NATIONAL SECURITY THREATS IN CYBERSPACE 30 (2009), *available at* http://nationalstrategy.com/portals/0/documents/national%20security%20threats%20in%20cyberspace.pdf.

22. NAT'L RES. COUNCIL OF THE NAT'L ACAD., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009).

23. Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force*, WALL ST. J., May 31, 2011, at A1.

24. Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L. SECURITY L. & POL'Y. 63, 63 (2010).

25. Owens et al., *supra* note 22, at 3.

26. *Id.*

A. "They're Stealing Everything Not Bolted Down"

There have been an increasing number of cyberexploitations of both U.S. government and U.S. private networks.[27] In 2005, there were 4,095 known cyber intrusions into U.S. computer systems.[28] In 2008, that number rose to 37,258 intrusions, and an estimated one trillion dollars were lost in the U.S. alone.[29] In 2010, the DHS recorded 5.4 million intrusions overall and 15,000 intrusions a day.[30] At any given time, more than one hundred foreign intelligence organizations are trying to break into U.S. computer systems.[31] In one of the largest attacks to date, hackers broke into more than 75,000 computers at nearly 2,500 companies around the world.[32]

General Keith Alexander, head of U.S. Cyber Command and the National Security Agency ("NSA"), described cyberexploitation against U.S. companies as "the 'greatest raid on intellectual property'" in history.[33] Due to cyberexploitation, one unnamed company lost over one billion dollars in technology that took more than twenty years to develop.[34] Cyber-expert Richard Clarke explained the extent of the damage:

> What has been happening over the course of the last five years is that China—let's call it for what it is—has been hacking its way into every corporation it can find listed in Dun & Bradstreet . . . Every corporation in the U.S., every corporation in Asia, every corporation in Germany. And using a vacuum cleaner to suck data out in terabytes and petabytes. I don't think you can overstate the damage to this country that has already been done.[35]

One U.S. lawmaker claimed that Chinese cyberexploitation accounted for one trillion dollars in intellectual property theft and ten

27. FOREIGN SPIES, *supra* note 11, at 1.

28. Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1539 (2010).

29. *Id.* at 1537, 1539.

30. *Federal Networks Attacked 15,000 Per Day in 2010, Says DHS Official*, INFOSECURITY, May 27, 2011, http://www.infosecurity-magazine.com/view/18274/federal-networks-attacked-15000-per-day-in-2010-says-dhs-official/.

31. Jensen, *supra* note 28, at 1539.

32. *Id.* at 1536.

33. Stew Magnuson, Editorial, *Defense Department Partners With Industry To Stem Staggering Cybertheft Losses*, NAT'L. DEF., Dec. 2011, at 22.

34. *Id.*

35. Michael Riley & John Walcott, *China-Based Hacking Of 760 Companies Reflects Global Cyber War*, BLOOMBERG BUSINESSWEEK, Dec. 22, 2011, http://www.businessweek.com/news/2011-12-22/china-based-hacking-of-760-companies-shows-cyber-cold-war.html.

thousand American jobs lost.[36] The same U.S. lawmaker noted, "'[the Chinese] are stealing everything that isn't bolted down, and it's getting exponentially worse.'"[37] Disturbingly, these losses could be drastically understated. Many companies are unaware of the pervasive cyberexploitation they face, and those that are aware are reluctant to report their loss, fearing damage to investor relations.[38]

B. It's Going to Get Worse Before It Gets Better

The reports of cyberexploitation against U.S. networks are legion, and highlight the vulnerability of U.S. networks even after companies have put increased security protections in place. What's more, the "pace of . . . industrial espionage activities against major [U.S.] corporations . . . is accelerating."[39] The U.S. is "fully dependent upon information technology and [] information infrastructure,"[40] thereby making it "particularly vulnerable to cyber threats."[41] As methods of cyber intrusion advance and technology becomes increasingly prevalent, both the severity and frequency of cyberexploitation will continue to increase. The U.S. cannot afford to watch as billions of dollars of intellectual property flows to foreign countries. There must be some response.

II. WHO SHOULD RESPOND, AND HOW?

Is the private sector, the U.S. government, or law enforcement best suited to stopping cyberexploitation? A company has several options when facing cyberexploitation. The company could: (1) turn to the U.S. government and hope for a state response utilizing the military and other government cyber resources;[42] (2) decide to litigate and prosecute the hacker by filing a complaint with the DOJ or by pursuing a private

36. *China's Cyber Threat A High-Stakes Spy Game*, NAT'L. PUB. RADIO, Nov. 27, 2011, http://www.npr.org/2011/11/27/142828055/chinas-cyber-threat-a-high-stakes-spy-game?sc=tw.

37. Riley & Walcott, *supra* note 35.

38. FOREIGN SPIES, *supra* note 11, at i.

39. *Id.* at 1.

40. U.S. DEP'T OF HOMELAND SEC., NAT'L STRATEGY TO SECURE CYBERSPACE 6 (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

41. Melnitzky, *supra* note 19, at 538.

42. Though unlikely, the government could be made responsible for conducting active defenses on behalf of private companies. *See* Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Defense in Cyberspace*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 333-34 (Committee on Deterring Cyberattacks: Informing Strategies and Developing Options & National Research Council ed., 2010).

suit; (3) upgrade their cyberdefenses by investing in an improved intrusion detection system with enhanced firewalls to prevent future attacks; (4) do nothing, recover their computer system, and assess the damage; or (5) they can exercise their right to self-defense.[43]

A. The U.S. Government

A U.S. company could turn to the U.S. government when suffering cyberexploitation. In this sense, the company could ask the U.S. government to target the cyberexploitation's source or use its legal authority to shut down the incoming attacks. The U.S. government probably has the greatest expertise in the area of cyberattack.[44] Through the U.S. Cyber Command, the U.S. military, the DHS, the Central Intelligence Agency ("CIA"), and the NSA, the U.S. government has vast cyber-resources at its disposal. Furthermore, someof the targeted intellectual property has military applications, so the U.S. government might naturally be involved due to the national security threat.[45]

However, the U.S. government may not have the legal authority to respond to hackers targeting U.S. companies. U.S. companies mostly face cyberexploitation, not cyberattack. The U.S. government has yet to formulate cyber rules of engagement,[46] so it is uncertain whether cyberexploitation would merit a government response. Nevertheless, most legal commentators agree that cyberexploitation is not an act of war; cyberexploitation is not illegal under international law[47] and does not constitute an armed attack under the United Nations ("U.N.") Charter.[48] At some point, the U.S. government may—and should—view the theft of vast quantities of intellectual property to be a national security threat. Indeed, considering its destructive effect on the U.S. economy, cyberexploitation may be a form of economic warfare that amounts to an armed attack.[49] However, as things currently stand,

43. *See* Jay P. Kesan & Ruperto Majuca, *Optimal Hackback*, 84 CHI.-KENT L. REV. 831, 835 (2010).

44. Melnitzky, *supra* note 19, at 549 ("It is generally accepted that America's offensive cyber warfare capabilities are the best in the world").

45. *Id.* at 545 ("In some instances, IP theft presents a direct threat to national security, such as when Chinese hackers stole terabytes worth of data on the F-35 fighter plane being developed by Lockheed Martin.").

46. Donna Miles, *Doctrine To Establish Rules of Engagement Against Cyber Attacks*, AM. FORCES PRESS SERVICE, Oct. 20, 2011, http://www.defense.gov/news/newsarticle.aspx?id=65739.

47. Commander Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 217 (1999).

48. Melnitzky, *supra* note 19, at 563-64.

49. *Id.* at 564.

cyberexploitation is just a crime,[50] and the U.S. government will probably be unwilling to bring its cyber-arsenal to bear against countries engaged in cyberexploitation.[51] Thus, a U.S. company probably cannot turn to the U.S. government and ask it to attack the source of the offending cyberexploitation.

Moreover, the U.S. government might not have the legal authority to stop further incoming cyberexploitation. Agencies like the CIA, NSA, U.S. State Department, DOJ, and the DHS all have competing claims to U.S. cybersecurity responsibility.[52] This complicates which agency would respond in the event of a cyberattack. General Keith Alexander, head of U.S. Cyber Command and the NSA, explained: "I do not have the authority to look at what's going on in other government sectors, nor what would happen in critical infrastructure. That right now falls to DHS. It also means that I can't stop it, or at network speed . . . see what's happening to it."[53] Under certain circumstances, U.S. Strategic Command has the authority to respond to cyberattacks against DOD networks, but it cannot respond to cyberexploitation against private systems.[54]

The DHS may also lack the authority to protect U.S. companies. The DHS has cybersecurity responsibility for the defense industrial base and critical infrastructure providers.[55] However, "neither DHS nor any other part of [the U.S.] government has been given the authority to conduct active threat neutralization on behalf of any part of the private sector (including the companies of the defense industrial base and the providers of critical infrastructure)."[56] Thus, with an inability to use military resources on the one hand, and a confused regulatory framework for stopping incoming cyberexploitation on the other, the U.S. government may be unable to effectively help a company suffering

50. *See* Economic Espionage Act, 18 U.S.C. §§ 1831-1839 (1996) (criminalizing economic and industrial espionage).

51. *See* Jack Goldsmith, *The Pervasive Cyberthreat that Goes Unchallenged*, WASH. POST, Nov. 25, 2011, http://www.washingtonpost.com/opinions/the-insidious-cyberthreat-that-goes-unreported/2011/11/25/gIQAKXdIxN_story.html ("[B]ecause cyber exploitations do not violate international law . . . [they] would not justify a large-scale military response, kinetic or cyber.").

52. *See* Ellen Nakashima, *Cyber-intruder Sparks Massive Federal Response—and Debate Over Dealing with Threats*, WASH. POST, Dec. 8, 2011, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

53. *Id.*

54. Owens et al., *supra* note 22, at 203.

55. *Id.* at 203.

56. *Id.*

cyberexploitation.

B. Law Enforcement

If cyberexploitation is a crime rather than an act of war, U.S. companies could turn to law enforcement.[57] In essence, this approach asks that companies victimized by cyberexploitation file a complaint with the DOJ.[58] However, traditional law enforcement schemes do not work well in cyberspace.[59] First, the anonymity of the internet protects those who engage in cyberexploitation, making attribution very difficult.[60] Most hackers can successfully mask the source of an intrusion by spoofing IP addresses,[61] making it appear that a cyberattack originating in China is actually coming from Virginia. If you cannot track the source of the intrusion, you cannot find the guilty party.

Furthermore, jurisdictional issues slow any proper response from law enforcement. Even if you could successfully track the source of cyberexploitation, the country of origin needs to have similar computer crime laws to the investigating jurisdiction and be willing to prosecute the hacker.[62] Evidentiary concerns also complicate the effort to prosecute hackers.[63] Often times the prosecuting country needs to rely upon local authorities to gather evidence logs.[64] These evidence logs probably do not exist or may cost too much to investigate in the first place.[65] These same problems exist for private tort remedies.[66] In reality, the probability of a hacker's capture and prosecution is low, while the prevalence of hacker havens is high.[67]

Finally, even if there were no jurisdictional or evidentiary problems, law enforcement has limited resources. A U.S. company simply cannot call law enforcement and expect cyberexploitation in progress to stop. Countless websites face cyberexploitation, so law enforcement is hard-pressed to respond at all, much less to

57. Kesan & Majuca, *supra* note 43, at 835.

58. *Id.*

59. *Id.* at 834.

60. Trevor A. Thompson, *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under the CFAA*, 36 FLA. ST. U. L. REV. 537, 547 (2009).

61. *Id.* at 548.

62. *Id.* at 552.

63. *Id.* at 553.

64. *Id.*

65. Thompson, *supra* note 60, at 553.

66. *Id.* at 552.

67. *Id.* at 553.

cyberexploitation in progress.[68] With limited resources making a response unlikely, law enforcement is an ineffective choice for a company suffering cyberexploitation. Considering the limitations on both law enforcement and the U.S. government, we must look to the private sector.

C. The Private Sector

Of course, companies could just improve their own network defenses.[69] The private sector "designs, builds, owns, and operates" the majority of computer network equipment,[70] so it might make sense to put the burden on the private sector to increase cybersecurity. However, given the technology behind the internet's infrastructure, "the web [may be] so skewed toward advantage for the attacker that we are reaching the point of diminishing returns for defending a network at the perimeter. . . ."[71] At some point, a hacker will be able to find a zero-day exploit, so it is almost inevitable that a network penetration will occur.[72] Indeed, Deputy Secretary of Defense William Lynn stated that:

> Our defenses need to be dynamic. A fortress mentality will not work in the cyber. We cannot retreat behind a Maginot line of firewalls. Cyber war is much more like maneuver warfare, and these new technologies help us find and neutralize intrusions. But we must also keep maneuvering. If we stand still for a minute our adversaries will overtake us.[73]

Although companies should continually evaluate and improve network defenses, reliance on them is not sufficient, as those defenses are unlikely to be effective in the long term.[74]

Even if private network defenses were reliable, their constant upgrade and maintenance may be cost prohibitive for most companies. A survey found that in order to stop 95% of cyber intrusions, private and public critical infrastructure providers would have to "boost spending to a group total of $46.6 billion from the current $5.3

68. Owens et al., *supra* note 22, at 207.

69. Kesan & Majuca, *supra* note 43, at 835.

70. WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATION INFRASTRUCTURE iv (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; Jensen, *supra* note 28, at 1559.

71. Hayden, *supra* note 15, at 6-7.

72. *See id.* at 7.

73. Jensen, *supra* note 28, at 1560.

74. Owens et. al, *supra* note 22, at 203.

billion."[75] Thus, each company would have to increase cybersecurity spending from $22.9 million to $292.4 million in order to achieve that 95% level,[76] over a 1,000% increase in spending! The largest company in the survey (by market capital) reported $277 million in quarterly profits.[77] It is not realistic to expect a large company to devote over a quarter of its yearly profits to cybersecurity spending, much less expect smaller companies (with much less market capital) to do the same. Although this survey only considered public and private critical infrastructure providers,[78] its results are likely representative of the entire private sector. In reality, even if private network defenses were reliable, the private sector will not spend such an exorbitant amount to assure proper cybersecurity. If private companies are best suited to respond to cyberexploitation, then solely improving network defenses cannot be the answer.

Finally, companies could do nothing, recover their computer systems, and assess the damage that the cyberexploitation caused.[79] Unfortunately, it seems that this approach has been the norm for far too long. Companies do not have to disclose whether they were the victims of attack, so the true costs of cyberexploitation are either hidden or not understood by the public.[80] Even more disturbing than the severity and frequency of cyberexploitation were the low rates at which companies reported them to law enforcement.[81] One survey found that "in four out of five cases, the compromised organization declined to report" cyberexploitation to law enforcement.[82] These organizations explained that they were unwilling to report cyberexploitation because they feared that "'negative publicity would hurt their organization's stock and/or image.'"[83] This attitude can no longer endure, and, hopefully, new Securities and Exchange Commission guidelines for disclosure after

75. Eric Engleman & Chris Strohm, *Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps*, BLOOMBERG (Jan. 31, 2012, 5:00 AM), http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html.

76. *Id.*

77. Brian Wingfield, *Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months*, BLOOMBERG (Feb. 1, 2012, 12:00 AM), http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html.

78. *Id.*

79. Kesan & Majuca, *supra* note 43, at 835.

80. Hayden, *supra* note 15, at 5.

81. Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 172 (2005).

82. *Id.*

83. *Id.* at 172-73.

cyber intrusions will provide a better guide for companies.[84] At any rate, in the face of losing tremendous amounts of intellectual property data to foreign nations, companies can no longer conduct business as usual. There must be a response.

D. Taking Responsibility

We find ourselves in a complicated situation. Both the frequency and sophistication of cyberexploitation will increase. The costs are high; beyond national security concerns, the U.S. economy cannot afford to let so much intellectual property go to foreign shores. The U.S. government, however, cannot bring its formidable cyber-arsenal to bear and may lack the authority to stop incoming attacks. Law enforcement is largely ineffective.[85] As such, in answering our first question, companies are best suited to responding to cyberexploitation against their own systems.

If companies are best suited to responding to cyberexploitation, how should they respond? Improving network defenses, while needed, is not sufficient.[86] Determined hackers can overcome network defenses, and even if these defenses were reliable, companies will not spend the required amounts to assure effective cybersecurity. Thus, companies must have something more: a cheap, effective, and realistic method of stopping cyberexploitation in progress. Companies must have a right to self-defense in cyber-space. Companies must have the right to hackback.

III. WELCOME TO THE WILD WEST: SELF DEFENSE IN CYBERSPACE

One way to control cyberexploitation is to allow companies to exercise their right to self-defense in cyberspace. As a general legal principle, an entity can defend its property using reasonable force.[87] U.S. common law even admits certain rights of defense of property for corporations.[88] The exercise of this right generally involves the use of non-lethal force to neutralize an immediate threat to property.[89] Here, a U.S. company could exercise its right to defense of property (its computer networks and intellectual property).

84. Joseph Menn, *SEC Issues Guidelines on Hacking*, FIN. TIMES (Oct. 14, 2011, 1:53 AM), http://www.ft.com/intl/cms/s/0/32e2adae-f5fc-11e0-bcc2-00144feab49a.html#axzz1alNT7hc6.

85. Kesan & Majuca, *supra* note 43, at 834.

86. *See* Owens et al., *supra* note 22, at 203.

87. Kesan & Majuca, *supra* note 43, at 833.

88. Owens et al., *supra* note 22, at 204.

89. *Id.* at 205.

Consequently, there is a historical case for private companies exercising their right to self-defense in cyberspace. During the European colonization of the Western Hemisphere, large private corporations like the East India Tea Company defended themselves during expeditions.[90] The expanse of cyberspace is similar to the unregulated lands of mankind's era of discovery.[91] Essentially, if companies have historically defended themselves in unregulated domains, why should cyberspace be any different?

I, however, prefer an analogy to the American Wild West; the inherent lawlessness of the internet fits nicely with the Wild West mythology. In this sense, black hat rogues (hackers) target the townsfolk (U.S. companies) on the lawless plains of the Wild West (the internet). The white-hat sheriffs (government agencies and law enforcement) have a limited ability to defend the thinly populated Wild West: "'the men in black hats can strike anywhere, while the men in white hats have to defend everywhere.'"[92] However, the white-hats cannot, or will not, defend everywhere. The townsfolk must have some means of defending themselves.

A. "Yes, It's Illegal, but So Was Rosa Parks Sitting in Front of the Bus"

We now find ourselves at the concept of hackback. An entity engages in hackback when it uses a cyberattack to stop cyberexploitation in progress.[93] The cybersecurity firm Symbiot has identified three methods of hackback: (1) invasive techniques that obtain access to the hacker's system and then "pursu[es] a strategy of disabling, destroying, or seizing control over the attacking assets;" (2) symmetric counterstrikes which exploit "vulnerabilities on the attacker's system, in an amount proportional to their current attacks;" and, (3) asymmetric counterstrikes which constitute "'retaliation . . . far in excess of the attack that the aggressor has underway.'"[94]

Consequently, both companies and governments have demonstrated an interest in hackback. Some in the private sector have argued for a right to self-defense when passive defensive measures are insufficient.[95] For example, the White Wolf Security corporation

90. Hayden, *supra* note 15, at 5-6.
91. *Id.* at 5.
92. Katyal, *supra* note 18, at 60.
93. Melnitzky, *supra* note 19, at 538-40.
94. Smith, *supra* note 81, at 177-78.
95. Owens et al., *supra* note 22, at 204.

argued that corporate victims of cyberexploitation should have limited rights to use hackback in order to protect their resources and employees.[96]

Furthermore, there is evidence that many companies (including Fortune 500 companies) have already used hackback.[97] "Frustrated by their inability to stop sophisticated hacking attacks or use the law to punish their assailants, an increasing number of U.S. companies" have turned to contractors to conduct hackback.[98] One Fortune 500 company used counterespionage software that slowed a cyber intrusion in progress, sent the hackers to a "virtual tar pit," and then blocked the hacker's computer from the company's website completely.[99] By sending the hacker to the virtual tar pit, the software allowed for better attribution of the cyberexploitation by getting the hacker to reveal more identifying information.[100] Humorously, this hackback software displayed a map of the hacker's neighborhood, highlighted nearby lawyers, and displayed a message that said, "'You're probably going to need some legal help.'"[101]

The existence of similar technology hints that companies have used hackback for quite some time. In March of 2004, Symbiot announced its development of the first software that could both repel cyberattacks and accurately identify its source.[102] Symbiot's technology enabled users to reflect cyberattacks back on the hackers, ultimately disabling or destroying the hacker's computer.[103] Symbiot has even claimed that corporations "have been using 'tiger teams' for years in order to launch highly aggressive counterstrikes against attackers."[104] In addition, a company that provided web hosting for the World Trade Organization responded to a denial-of-service attack by reflecting the cyberattack onto the hacker's server.[105] Finally, the Japanese government is pushing Japanese contractors to develop a hackback virus that would identify the

96. *Id.* at n.7.

97. Jensen, *supra* note 28, at 1566.

98. Joseph Menn, *Hacked Companies Fight Back With Controversial Steps*, REUTERS, June 17, 2012, *available at* http://www.reuters.com/article/2012/06/17/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120617.

99. James Temple, *Hackers Getting Hacked by Security Firms*, S.F. CHRON., Nov. 30, 2011, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/11/30/BUVP1M5245.DTL&type=tech.

100. *Id.*

101. *Id.*

102. Smith, *supra* note 81, at 174.

103. *Id.*

104. *Id.* at 175.

105. *Id.* at 176.

source of a cyberattack and stop it.[106]

Therefore, whether it is legal or not, several U.S. companies and foreign entities have already pursued hackback. One cybersecurity official had this to say regarding hackback technologies: "'Yes, we are working on it, as are many others. Yes, it's illegal, but so was Rosa Parks sitting in front of the bus.'"[107] If so many companies already use or advocate for the use of hackback, it makes sense to legalize and regulate some limited right. To understand how that regulation would work, it is helpful to understand both the benefits and drawbacks of hackback.

B. The Benefits of Hackback

There are several reasons why a company should consider using hackback. First, by using hackback, a company can mitigate the damage to its systems from ongoing cyberexploitation.[108] By responding to cyberexploitation in progress, a company can disable the source, preventing further damage to the company's networks and stopping the ongoing theft of information.

Second, legalizing hackback would be an instant cybersecurity shot in the arm. For example, many companies already possess the technical expertise necessary to accomplish hackback. Companies often use penetration testing as a way to identify cybersecurity vulnerabilities.[109] These exercises generally involve company hired "red teams" probing a company's network for exploits.[110] The expertise needed for "red-teaming" is roughly the same as that needed to conduct hackback, so companies already have hackers that could engage in hackback.[111] If hackback was a legal option, companies could quickly put the technique into practice. In essence, there would be no protracted technological or educational run-up to hackback's widespread use.

Third, a company could prevent future attacks on its systems. Hackback could degrade an attacker's systems to the point that further cyberexploitation is impossible. More importantly, hackback would serve as a deterrent. If a hacker knows that a specific company will retaliate, they may be less likely to attack that company in the first

106. Hana Stewart-Smith, *Japan Develops Virus to Counter Cyber-Attacks: But Can it be Used?*, ZDNET (Jan. 4, 2012, 6:22 AM), http://www.zdnet.com/blog/asia/japan-develops-virus-to-counter-cyber-attacks-but-can-it-be-used/635.

107. Owens et al., *supra* note 22, at 207.

108. Kesan & Majuca, *supra* note 43, at 834.

109. Owens et al, *supra* note 22, at 204.

110. *Id.*

111. *Id.*

place. Some believe that the U.S. government's cyber-deterrence strategy does not work because foreign hackers know that the U.S. will not respond to cyber-espionage.[112] However, if U.S. companies openly exercise their ability to hackback, foreign hackers might think twice about attacking U.S. systems.

Fourth, hackback provides companies with a measure of revenge. While not a legal justification, revenge certainly has an emotional appeal. These companies face the theft of intellectual property that has been under development for years. Indeed, this intellectual property might represent millions of dollars, thousands of jobs, and the combined efforts of countless employees. In many cases, this intellectual property represents the future of the company; at least one British firm went bankrupt after a foreign nation stole their signature technology.[113] Accordingly, there is an emotional appeal to punishing the perpetrators of cyberexploitation. A security manager from a large financial institution visited the physical location where a series of cyberattacks had originated.[114] The security manager broke in, stole the offending computers, and left a note reading, "'See how it feels?'"[115] Hackback could provide a similar emotional catharsis for targeted companies.

Finally, hackback is attractive because so many of the other methods of cybersecurity are ineffective. As noted above, appeals to governmental authorities are unproductive. A company should improve its network's defensive capabilities, but those improvements are costly and cannot assure total cybersecurity. Every other method of cybersecurity is, in some sense, ineffective.

Hackback, on the other hand, is effective. Hackback would sidestep difficulties such as "lengthy prosecutions, thorny jurisdictional matters, technologically unsophisticated juries, and slow courts."[116] Law enforcement is orientated toward investigation, prosecution, and conviction of hackers targeting computer system;[117] these processes take time and are often constrained by the availability of resources and expertise.[118] In the meantime, the company can only hope that its

112. *See* Goldsmith, *supra* note 51.

113. Con Coughlin, *Foreign Hackers 'Putting UK Firms Out of Business'*, TELEGRAPH (Oct. 24, 2011, 1:10 AM), http://www.telegraph.co.uk/technology/news/8845100/Foreign-hackers-putting-UK-firms-out-of-business.html.

114. Smith, *supra* note 81, at 176.

115. *Id.*

116. Katyal, *supra* note 18, at 60.

117. Owens et al., *supra* note 22, at 203.

118. *Id.*

passive defense measures will mitigate the cyberexploitation.[119] With hackback, victims can stop cyberexploitation in progress without relying on the police.[120] Pursuing hackback would also save companies a good deal of money and resources.[121]

Most importantly, hackback provides an immediate answer for companies desperately in need. The legal landscape for U.S. cybersecurity is a confused place. "[T]here are no [effective] legal mechanisms or institution[s] . . . available to provide [U.S. companies] immediate relief [for cyberexploitation]."[122] While the U.S. government slowly formulates a coherent cyber-policy and plays politics over cyber-legislation, U.S. companies lose billions of dollars. Hackback is desirable because it provides an immediate, effective response. In the absence of the white hats, we cannot let the black hats run rampant throughout the Wild West; hackback would give the townsfolk a way to fight back. Regrettably, U.S. companies considering hackback currently face a tradeoff between the benefits from the defense of their property and its associated legal liabilities.[123] It is time to resolve that tradeoff and stop the hemorrhaging of intellectual property. It is time to establish a strong U.S. cybersecurity posture. It is time to legalize and regulate the use of hackback.

C. The Problem with Hackback

While hackback might be an effective means of stopping cyberexploitation, that effectiveness comes with a price. For example, a company utilizing hackback would play the role of the judge, jury, and executioner by deciding whether a hacker deserves reprisal and what form that reprisal will take. In effect, the company has found the target of a hackback guilty without receiving a fair trial.[124] Moreover, the company's own view of its self-interest would motivate the decision to hackback.[125] That self-interest would be unlikely to take into account other broader societal or national needs, and thus, a private party's threshold for action may be lower than public policy might dictate.[126] It is unlikely that the American public would be comfortable with a U.S. company exercising such unregulated power.

119. *Id.*
120. Katyal, *supra* note 18, at 60.
121. *Id.*
122. Owens et al., *supra* note 22, at 203.
123. *Id.*
124. Katyal, *supra* note 18, at 61.
125. Owens et al., *supra* note 22, at 211.
126. *Id.*

In addition, hackback may have negative implications for international relations.[127] A foreign nation will likely attribute a hackback by a U.S. company to the U.S. government.[128] Even if there is no such linkage, the foreign nation may seek to hold the U.S. government responsible.[129] A foreign nation may even see a denial by the U.S. government as "evidence of government complicity in a plausibly deniable attack."[130] If the foreign government believes that the U.S. government is responsible for the hackback, the foreign government may attack the U.S. directly.[131] Along the same lines, hackback by U.S. companies might interfere with cyberattacks launched by the U.S. government.[132]

A U.S. company exercising hackback could also face legal troubles. Specifically, the CFAA makes "knowingly caus[ing] the transmission of a program, information, code, or command, and . . . intentionally caus[ing] damage . . . to a protected computer" a crime.[133] I will address the CFAA later in this note. However, as the law currently stands, a company using hackback might face exposure to both criminal and civil liability under the CFAA.

Finally, companies would still face difficulty in attributing the source of cyberexploitation. The same anonymity[134] and spoofing methods[135] that bedevil law enforcement would also make attribution difficult for companies. These attribution problems raise the possibility that companies could hit the wrong person. Hackers often make use of bot-nets[136] of zombie computers to carry out their cyberattacks.[137] These bot-nets are composed of computers owned by innocent computer users.[138] If a hacker uses a bot-net to attack a company, the resulting hackback could end up accidentally destroying the computer of an

127. *Id.*
128. *Id.*
129. *Id.*
130. Owens et al., *supra* note 22, at 211.
131. *Id.*
132. *Id.*
133. 18 U.S.C. § 1030(a)(5)(A); Smith, *supra* note 81, at 182.
134. Thompson, *supra* note 60, at 539.
135. *Id.* at 548.
136. Tyler Moor, *Introducing the Economics of Cybersecurity: Principles and Policy Options, in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 6 (Committee on Deterring Cyberattacks: Informing Strategies and Developing Options & National Research Council ed., 2010).
137. Smith, *supra* note 81, at 180.
138. *Id.*

innocent person. Moreover, when bot-nets are composed of computers found in hospitals, internet service providers, and government offices, a successful hackback "could easily create a remedy worse than the disease" by accidentally damaging these systems.[139]

Hackback has its shortcomings. However, companies can mitigate these shortcomings. As there have already been improvements in the ability to attribute intrusions,[140] further technological advances should quiet fears that an innocent third party could become the victim of hackback. U.S. cybersecurity experts recently claimed that the U.S. government successfully attributed cyberattacks not only to specific Chinese hacker units, but also to specific hackers within those units.[141] Similarly, a technology like Symbiot's hackback program could progressively tease out an attacker's information, allowing for better attribution.[142]

In addition, a comprehensive legal regime regulating hackback would address the practice's questionable legality. That legal regime could institute liability for illegal hackback, hopefully diminishing fears that companies could hackback at will. The U.S. government would be the power behind that comprehensive legal regime. I will explore what that regime would look like later in this note. With the U.S. government in control, companies could coordinate their use of hackback with the government, thereby diminishing the chances of interfering with U.S. cyberattacks. Along the same lines, this coordination would give companies input as to when a hackback might be politically unwise. If international relations are at a tense point, the U.S. government could use this relationship to caution U.S. companies against the use of hackback.

Indeed, the fact that a company can abuse hackback does not necessarily mean that the U.S. government should outright deny it.[143] Rather, the U.S. government should closely regulate the practice.[144] The key is not to prohibit hackback, but to "create liability rules that ensure a firm uses hackback only when it is socially [and politically] optimal to do so."[145] The question, then, is under what regime could we

139. *Id.* at 181.

140. Kesan & Majuca, *supra* note 43, at 836.

141. *Most China-based Hacking Done by Select Few*, CBS NEWS, Dec. 12, 2011, http://www.cbsnews.com/8301-202_162-57341339/most-china-based-hacking-done-by-select-few/?tag=contentMain;contentBody.

142. Smith, *supra* note 81, at 177.

143. Kesan & Majuca, *supra* note 43, at 833.

144. *Id.* at 833-34.

145. *Id.* at 836.

closely regulate the use of hack-back?

IV. TAMING THE WILD WEST

If we are to design a statutory authorization for hackback, then time is of the essence. The cyberexploitation threat is immediate, so the statutory response must also be immediate. As such, it makes sense to alter a statute already in effect. That statute is the CFAA.

A. The CFAA: There's a New Sheriff in Town

Any discussion of computer hacking in the U.S. should begin with the CFAA, the basic anti-hacking statute.[146] The most obvious legal challenge to hackback is the CFAA, by which hackers can face civil and criminal liability.[147] The CFAA prohibits both "'knowingly caus[ing] the transmission of a program, information, code, or command, and . . . intentionally caus[ing] damage . . . to a protected computer'" and "'intentionally access[ing] a protected computer without authorization, and . . . recklessly caus[ing] damage.'"[148]

No court has decided whether hackback would violate the CFAA, or any other federal or state law.[149] Nevertheless, it seems safe to assume that hackback would fall within the CFAA's provisions. A company engaging in hackback would be "'knowingly caus[ing] the transmission of a program, code, or command to a computer'" because the company is intentionally using software to disable a hacker's computer.[150] That process would likely involve some transmission of a program, code, or command.

Whether that computer is protected, and whether the company intentionally causes some sort of damage is unclear. Symbiot envisioned a hackback arsenal that included the degradation of malicious servers,[151] so that would likely constitute intentional damage. Moreover, is a hacker's computer, or even a bot-net, a "protected computer?" According to the CFAA, a "protected computer" is "either a [U.S.] government computer, a financial institution computer, or a computer used in interstate or foreign commerce or communication."[152]

146. *See* 18 U.S.C. § 1030.
147. *Id.* Smith, *supra* note 81, at 182.
148. Smith, *supra* note 81, at 182. *See also* 18 U.S.C. § 1030 (a)(5)(A)-(B).
149. Smith, *supra* note 81, at 182.
150. *Id.*
151. *Id.* at 174.
152. Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 156-57 (2011).

"This final classification—used in interstate or foreign commerce—essentially makes a protected computer out of every computer connected to the Internet and, quite possibly, every computer."[153] Thus, it is possible that even a bot-net computer is a "protected computer" within the terms of the CFAA.

Between the absence of relevant case law and ambiguity in the CFAA's language, it is not clear whether hackback is legal. The CFAA's language appears to apply, but it is not a perfect fit. It is also unclear whether the law of defense of property affects the CFAA's application. A court could find that hackback undertaken in defense of property is allowable notwithstanding the CFAA.[154] Nevertheless, a company considering hackback would want to be on solid legal footing. Moreover, the DOJ "has taken a position unequivocally opposed to the employment of active defenses" in cyberspace.[155] If we want to give companies the right to hackback, it would be safer to alter the CFAA by giving companies explicit authorization.

In amending the CFAA, there are four possible legal regimes that could govern hackback: (1) subject hackback to both criminal and civil liability; (2) privilege hackback from criminal and civil liability; (3) impose criminal (but not civil) liability; or, (4) impose civil (but not criminal) liability.[156] A regime that subjects companies using hackback to criminal and civil liability would obviously be counterproductive. Similarly, a regime that imposes only criminal liability would still deter companies. The best approach would be to privilege the use of hackback completely, or at the very least, protect companies from criminal liability. What would this regime possibly look like? In addition, how would it fit within the statutory constraints of the CFAA?

B. Meet My New Deputy

One approach is to deputize U.S. companies under Section 1030(f) of the CFAA. Section 1030(f) reads as follows: "[t]his section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."[157]

In essence, section 1030(f) is an explicit exception from the CFAA

153. *Id.* at 157.

154. Owens et al., *supra* note 22, at 206.

155. Lieutenant Colonel Richard W. Aldrich, *How Do You Know You Are at War in the Information Age?*, 22 HOUS. J. INT'L L. 223, 258 (2000).

156. Smith, *supra* note 81, at 190.

157. 18 U.S.C. § 1030(f).

for law enforcement agencies.[158] The provision allows law enforcement agencies to undertake normally prohibited cyberattacks.[159] In fact, there are reports that the law enforcement community has already used this authority to conduct DDOS attacks against wireless networks and devices.[160] There is no explicit provision exempting private parties from the CFAA.[161]

The proposal, then, would be to deputize U.S. companies under section 1030(f) of the CFAA. This deputization would allow U.S. companies to conduct hackback under the watch of the DOJ. This is a novel proposal, so much of the deputy relationship needs definition. Principally, the U.S. government would institute a series of regulations governing the use of hackback. At a threshold level, companies would need DOJ approval in order to hackback. Granted, requiring government approval for every hackback might rob the technique of its effectiveness. Cyber intrusions occur in a matter of seconds, so a company needs to respond in a similar window of time.

Nevertheless, the U.S. government simply cannot give private companies carte blanche authority to hackback.[162] Unregulated hackback runs the risk of violating U.S. constitutional rights and perhaps causing an international incident, so the U.S. government has to exercise some means of control. Even so, companies are not really losing anything. Companies would be gaining legal protection under the CFAA in exchange for relinquishing legal control over the decision of when to hackback. Considering that hackback is probably illegal in the first place, relinquishing that decision is not a huge loss. Moreover, the government could install mechanisms—such as having a DOJ representative with the power to authorize hackback physically at the company—that ensure the approval process does not rob hackback of its effectiveness.

If a company must get DOJ authorization prior to hackback, when

158. *Id.* Owens et al., *supra* note 22, at 205.

159. Owens et al., *supra* note 22, at 205.

160. *Id.* at 201.

161. *Id.* at 205.

162. *See* Kesan & Hayes, *supra* note 42, at 333 ("It would be unwise to allow individual companies to make [the decision on when to hackback] on a case by case basis. Some companies would be more risk averse, while some may be more inclined to behave like cyber vigilantes. It is thus important to not place this significant discretion in the hands of private firms, because it would result in a wide array of differing results. In order to ensure that only socially optimal usage of [hackback] occurs, there needs to be some form of standardization for how [hackback] is implemented. One possible way to achieve this sort of standardization is to utilize a central government entity for the purpose of deciding when [hackback] would be appropriate.").

should the DOJ authorize it? The DOJ should reach that decision after consideration of several factors: whether the private company can properly attribute the incoming cyberexploitation; whether the hackback is necessary; whether the damage is proportional in the event that the hackback causes collateral damage; what types of computer systems the private company will hackback; what method the company intends to use; and finally, whether the hackback would implicate the Fourth amendment (and other relevant constitutional concerns). In essence, the U.S. government would fashion hackback rules of engagement for companies to follow. These rules of engagement would safeguard the constitutional rights of U.S. citizens while accounting for international law through an analysis of necessity, distinction, precision, and proportionality.[163]

These rules of engagement would also govern hackbacks on foreign computer systems. If it appears that a foreign government is the source of the cyberexploitation, then the U.S. government should exercise strict discretion as to whether to authorize hackback. Concededly, much of the abovementioned cyberexploitation came from foreign computer systems, so limiting the right to hackback in this fashion might make the technique toothless.[164] All the same, the U.S. government cannot allow companies to attack the computer systems of foreign governments at will. A U.S. company could sabotage U.S. diplomatic efforts by a poorly timed hackback, ultimately causing an international incident. By strictly regulating the hackback of foreign computer systems, the U.S. government could hold a powerful ace up its sleeve. For example, if the U.S. government is in strained negotiations with China, it could adjust its authorization of hackback in order to maximize political effect. If the Chinese refuse to cease their pervasive cyberexploitation, the U.S. government might authorize greater use of hackback as a means of persuasion.

Along the same lines, regulation of hackback could facilitate coordination between companies and the U.S. government. One concern surrounding hackback was that it could interfere with on-going U.S. government cyberattacks.[165] Through the deputy relationship, coordination between the U.S. government and U.S. companies would ensure that a company's hackback does not interfere with a U.S. government cyberattack. On the contrary, the deputy relationship might even bolster U.S. government cyberattacks.

163. *See* Kesan & Hayes, *supra* note 42, at 334-35.
164. *See supra* Part III.
165. Owens et al., *supra* note 22, at 203.

C. Making the Case

Authorizing private companies to hackback under a deputy relationship with the U.S. government might sound unlikely. However, the concept of deputizing a company under section 1030(f) is not farfetched. The DOJ already authorized a U.S. Air Force cybersecurity team to conduct hackback when two hackers infiltrated the computer networks of Rome Labs in Upstate New York.[166] The military does not necessarily fall under section 1030(f), so the DOJ had to expand section 1030(f)'s protections to a new entity.[167] Moreover, deputization of private entities by the U.S. government has become more prominent since the attacks of 9/11.[168] Notably, there is a "growing comfort with private actors handling sensitive national security tasks."[169] This is especially true in the area of cybersecurity where the private sector "designs, builds, owns, and operates" computer network equipment.[170]

In addition, there is already an increasing cybersecurity relationship between the U.S. government and private sector. For instance, the theme behind recent comprehensive cybersecurity legislation has been threat information sharing between the private sector and U.S. government.[171] The NSA has already begun sharing threat information with private industry.[172] The DHS has responsibility for cyber-protection of the defense industrial base and the providers of critical infrastructure, both private entities.[173]

Most encouragingly, the DOJ's National Security Division ("NSD") recently began training hundreds of prosecutors to combat

166. RICHARD BEJTILCH, THE TAO OF NETWORK SECURITY MONITORING: BEYOND INTRUSION DETECTION, 586-87 (2004) ("After a conference call with the FBI, the Secret Service, and the Department of Justice, the joint [Air Force] team got permission to break into civilian computer systems . . . Exigent circumstances justified [the Air Force's] need to bend several US laws by hacking backwards through the system. After the incident was over, the US Department of Justice told [the Air Force] . . . That was cool. Don't ever do that again").

167. *Id.*

168. Jon D. Michaels, *Deputizing Homeland Security*, 88 TEX. L. REV. 1435, 1435 (2010).

169. *Id.* at 1438.

170. Jensen, *supra* note 28, at 1559.

171. Siobhan Gorman, *House Passes Cybersecurity Bill*, WALL ST. J., Apr. 27, 2012, http://online.wsj.com/article/SB10001424052702304811304577369660212282978.html?mod=googlenews_wsj.

172. Jim Wolf, *8,000 Contractors Said Eligible for US Cyber Guard*, REUTERS, May 2012, *available at* http://www.reuters.com/article/2012/05/14/cyber-pentagon-companies-idUSL1E8GEI5S20120514.

173. Owens et al., *supra* note 22, at 203.

cyberexploitation.[174] The following description of the NSD's program sounds very similar to the proposed deputy relationship:

> Teams of specialized lawyers within NSD . . . will work with other agencies, the military and companies facing cyber intrusions. They will develop protocols for the intelligence community and federal agents in how to deal with private companies that are victims of cyber attacks. The issues revolve around how to build possible prosecutions within guidelines covering information sharing, privacy and civil liberties.[175]

Considering the threat-sharing relationships already in force, the prospect of greater coordination after passage of comprehensive cybersecurity legislation, the DHS' present cybersecurity responsibilities for private entities, and the NSD's new training program, the proposed deputization arrangement is not a huge leap.

If we accept the concept of the deputy relationship, we can see it has numerous benefits. First, "[d]eputies are force multipliers; as a matter of sheer numbers, a mobilized, vigilant public can reach more broadly than the government, on its own, can."[176] Authorizing companies to hackback would create a private cybersecurity army. That cybersecurity army could go where the U.S. government cannot by retaliating against foreign cyberexploitation. In the event of war, these companies could use their considerable hacking expertise to form cyber-militias under the onus of the U.S. government. The Chinese government has already considered such an arrangement.[177]

Second, the deputy relationship legitimizes the use of hackback. In this sense, the deputy relationship confers all of the benefits of hackback in a closely regulated environment. Companies would be able to use a technique that is inexpensive, effective, and immediate, without fear of criminal liability. Even in the absence of the white hats, the black hats would no longer control the Wild West.

Third, the deputy relationship regulates a dangerous practice that may already be in effect. Again, there is evidence that a number of U.S.

174. Sari Horwitz, *Justice Department Trains Prosecutors to Combat Cyber Espionage*, WASH. POST, July 25, 2012, at A02, *available at* http://www.washingtonpost.com/world/national-security/justice-department-trains-prosecutors-to-combat-cyber-espionage/2012/07/25/gJQAoP1h9W_print.html.

175. *Id.*

176. Michaels, *supra* note 168, at 1438.

177. Adam Segal, *Beware the Patriotic Geek: The Rise of Cyber Militias in Asia*, COUNCIL ON FOREIGN REL., Feb. 22, 2012, http://blogs.cfr.org/asia/2012/02/22/beware-the-patriotic-geek-the-risk-of-cyber-militias-in-asia/?cid=oth_partner_site-atlantic.

companies already practice hackback.[178] At the very least, if these companies do not practice hackback, they believe they should be able to. The unregulated practice of hackback is dangerous. Between damaging innocent computer systems, violating constitutional rights, and causing international incidents, unregulated hackback could have a chaotic effect on the U.S. The deputy relationship brings order to that chaos. Assuming that there would be some sort of rules of engagement, the deputy relationship could mitigate a number of the dangers of hackback. Indeed, the deputy relationship may be the best answer considering that "a simple prohibition on [hackback], or even raising the penalties for [hackback], are alone [not] sufficient to prevent all self-help actions in the future."[179] If a dangerous practice is going on regardless, an attempt to regulate it is certainly an improvement.

Granted, the deputy relationship also has a few drawbacks. The deputy relationship will complicate matters on an international level. Even if foreign nations clearly understand that a U.S. company is hacking back, those nations may construe the act as a cyberattack by the U.S. government. U.S. government authorization of the hackback would only increase the chances for misinterpretation. In the context of responding to Chinese cyberexploitation through increased hackback authorization, the Chinese might challenge the authorization as a de-facto government attack on its computer systems. This could lead to strained diplomatic relations or even an escalation to an all out cyberwar. Moreover, it is unclear whether government authorized hackback would implicate the Law of War, the U.N. Charter, or international humanitarian law.[180]

178. *See* Menn, *supra* note 98; *see also* Tim Maurer, *Breaking Bad: How America's Biggest Corporations Became Cyber Vigilantes*, FOREIGN POL'Y, Sept. 10, 2012, http://www.foreignpolicy.com/articles/2012/09/10/breaking_bad?page=0,0 (a poll of 181 participants at the infamous Black Hat conference "revealed that 36 percent [of respondents] had already engaged in retaliatory hacking in the past with 23 percent having hacked back once and 13 percent frequently"); David E. Sanger & John Markoff, *After Google's Stand on China, U.S. Treads Lightly*, N.Y. TIMES, Jan 14, 2010, *available at* http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?_r=2 (after suffering cyberexploitation, Google "began a secret counteroffensive" and "managed to gain access to a computer in Taiwan that it suspected of being the source of the attacks").

179. Owens et al., *supra* note 22, at 71 ("For this reason, it may be desirable to consider the establishment of a government-regulated institutional structure through which private sector entities that are the targets of sustained and ongoing cyberattack can seek immediate relief.").

180. *See* Kesan & Hayes, *supra* note 42, at 335-36 ("The initial [hackback] may violate the U.N. Charter if the attack rises to the level of 'use of force.' However, the U.N. Charter would prohibit the target of [a hackback] from responding in self-defense unless the initial [hackback] was severe enough to be considered an 'armed attack.').

The deputy relationship will also complicate matters on a domestic level. The focus of this note has been foreign cyberexploitation, but a hackback could hit a domestic computer network. If this is the case, there are substantial privacy concerns with companies snooping around and damaging the private computers of U.S. citizens. Hackback would probably raise Fourth Amendment search and seizure issues as the deputy relationship could implicate the state action doctrine.

Although there might be concerns with the deputy relationship, that does not mean the U.S. government should not pursue it. Ultimately, we need to remember that hackback already occurs, regardless of its legality. In the international context, foreign countries are just as likely to attribute a non-authorized hackback to the U.S. government as they are likely to attribute an authorized hackback.[181] If this is the case, and companies are already engaging in hackback,[182] the U.S. government is in a "damned if you do, damned if you don't" situation. If foreign governments will blame the U.S. government regardless of whether it gives its consent to the private company, then it might as well control the choice on when the company uses hackback.

The same argument applies in the domestic context; if hackback already occurs, the U.S. government should regulate it. There are constitutional problems with companies, authorized by the U.S. government, snooping around the private computers of U.S. citizens. However, if these companies are already snooping around, then the U.S. government should step in. To this end, strict regulation would mitigate some of those constitutional violations and would ensure that U.S. citizens are protected. Indeed, the presence of some regulatory regime for hackback, albeit flawed, is preferable to no regulatory regime for hackback at all.

CONCLUSION

U.S. companies face an incredible level of cyberexploitation. The loss of intellectual property and jobs represents both a devastating economic loss and a national security threat. This crisis demands action, but the current U.S. legal framework ties U.S. companies' hands. This is unacceptable; in the absence of a strong U.S. government presence in cyberspace, U.S. companies must have the ability to defend themselves.

Legalizing and regulating hackback through a deputy relationship is the best approach to the problem. Through legalization, U.S.

181. *Id.* at 203.
182. *Id.*

companies gain access to an immediate, effective, and cheap counter to foreign cyberexploitation. Through regulation, the U.S. government gains a way to control an on-going practice that could have adverse effects on international relations, public policy, and its citizens' constitutional rights.

The black hats have run rampant throughout the Wild West for far too long. It is time that we bring order to these lawless plains. As the Duke dryly observed, "a man settles his own problems" in the Wild West.[183] In cyberspace, companies should be able to settle theirs.

183. THE MAN WHO SHOT LIBERTY VALANCE (Paramount Pictures 1962).