Cascades:

The Anonymous Hack of HBGary (Part A)

This case study was created as part of the Open Technology Institute's (OTI) effort to create a curriculum focused on how digital technology is transforming public policy and governance. It is intended for use in a classroom setting.

CASCADES

In January 2011, Aaron Barr thought he had discovered a goldmine. And it could not come soon enough. Since becoming the CEO of HBGary Federal (a company that sold IT security services to the federal government) in fall 2009, Barr had struggled to generate revenue, occasionally selling "social media training[s]" to private firms but failing to secure the large contracts he had predicted at the start of his tenure.[1] Now he believed that he had uncovered the key to identifying the leaders of Anonymous, a collection of hacktivists that had gained prominence for (among other things) carrying-out attacks against several financial firms that had stopped processing donations to WikiLeaks.[2] Barr planned to share his findings in February at B-Sides, a technology security conference in San Francisco, and he believed that the presentation (titled, "Who Needs the NSA When We Have Social Media") could jumpstart his career and resolve HBGary Federal's financial woes.[3] As Gabriella Coleman, a cultural anthropologist at McGill University, wrote in her recent book on Anonymous, "If HBGary was really badass enough to identify the movers and shakers behind Anonymous—before even the FBI—corporate executives would, with good reason, be falling all over themselves to employ them."[4]

The plan backfired. After HBGary leaked the story to *The Financial* Times, which reported on Barr's research and plans in early February, Anonymous unleashed an attack that overwhelmed HBGary, Inc., Barr's firm, and Barr himself.[5] More specifically, Anonymous—which as Coleman wrote, was "ready to rumble"[6] after seeing *The Financial Times* piece—defaced the company's website, released tens of thousands of the company's e-mails, bragged about deleting a terabyte of the firm's data, and took over Barr's Twitter account.[7] The hackers posted doctored images of Barr, released e-mails detailing his marital strife, and went so far as to publish Barr's home address and social security number as well as several tweets with extremely crude content.[8] Among them: "Sup mother[redacted]: I'm CEO of a shitty company and I'm a giant media-[redacted]. Lol check out my [redacted] Greg's site: rootkit.com." And "Okay my fellow Anonymous [redacted] we're working on bringing you the finest Lulz as we speak. Stay tuned!"[9, 10]

For the HBGary brand, the financial fallout (estimated to be in the millions of dollars) and broader damage was significant.[11] "They [the hackers] have committed a crime against our company, and, unfortunately, we are legally bound," said Penny Leavy, the President of HBGary, Inc. For the IT security community, the incident was frightening. "[It] makes me want to change all my PWs [passwords] and re-evaluate

my processes," tweeted Jeremiah Grossman, the founder of WhiteHat Security, a firm that specializes in web security, adding, "Do not poke the bear."[12] And for the hacktivists, it was a demonstration of power. "You've tried to bite at the Anonymous hand," the hacktivists wrote on HBGary Federal's website, "and now the Anonymous hand is bitch-slapping you in the face."[13]

As the initial shock of the attacks wore off, Barr, his colleagues, and industry experts found themselves grappling with a number of difficult questions, with important policy implications. How did a technology security firm that was supposed to be demonstrating and selling best practices get hacked so easily? How did Barr fail to realize that his research—and his public comments surrounding it—would provoke such a forceful response? And what lessons can technology experts, public policy officials, and academics glean from this crisis as they try to make the Internet more secure?

Background

Headquartered in Sacramento, CA and with a sales office in Washington, D.C., HBGary, Inc. was a mid-sized technology security company with a high-profile CEO and which in 2011 was trying to gain a foothold in the market for federal government IT security services. The firm had been founded in 2003 by Greg Hoglund, a technology-security entrepreneur and researcher who had gained recognition for launching another IT security firm, Cenzic, Inc., and for his extensive work on "rootkits," software that allows malware and viruses to penetrate a computer without detection.[14, 15] HBGary, Inc. had traditionally focused on selling software that helped organizations in the financial, healthcare, and public sectors identify and understand IT security threats. However, in 2009, Hoglund, looking to expand, decided to establish a subsidiary that would focus on selling the company's services to the U.S. federal government.[16] The new group was called HBGary Federal, and HBGary, Inc.—which at the time had 30 employees and would soon sell for $24 million—would own 10% of the organization.[17]

To lead the group, Hoglund hired Barr, a former military official who had started to build a reputation in the IT security industry and was eager to run his own company. Barr had begun his career in the Navy where over the course of 12 years and multiple international deployments (including a period in Kosovo when he came under fire), he had served as a signals intelligence officer.[18, 19] Hoglund felt this experience would help Barr market the company's products to the U.S. government; he also believed that Barr's more recent experience at Northrop Grumman, a large aerospace and defense contractor where Barr had helped to lead multi-million dollar projects, reinforced his credibility. As Hoglund wrote in an e-mail to colleagues upon Barr's hiring, "We have known Aaron and Ted [Ted Vera was another employee hired alongside Barr] for more than 5 years. These two are A+ players in the DoD contracting space and are able to 'walk the halls' in customer spaces."[20] Hoglund added in an interview in March 2011, shortly after the Anonymous hack of HBGary, "Aaron has a very high IQ. He's a very smart individual. He also has an incredibly good reputation, or he did at that time."[21]

For his part, Barr felt that the opportunity to run his own company was too good to pass up. "I'd always had an itch to try the small-business side and work

in a more fluid, less process-oriented environment that had a lot of technical innovation," he explained, "and so I decided to give it a try."[22]

IT Security

Over the last decade, the IT security field had become extremely lucrative because of both the world's increasing dependence on the Internet and the difficulty of securing it. Originating from academic and U.S. government research that began in the 1960s, the Internet was initially used to connect regional academic and military networks in the United States.[23] However, by the first decade of the 21st century, this vast computer network had become foundational to commerce, communication, and social interaction. According to a 2011 McKinsey report, the Internet had been responsible for more than one-fifth of GDP growth in mature economies over the previous five years. During the same period, Facebook had exploded to more than 800 million users.[24] "The Internet," argued Manuel Castells, a professor of communication technology and society at USC, "is the decisive technology of the information age...."[25]

Unfortunately, efforts to secure the Internet had not kept pace with the platform's increasing significance; in particular, individuals were considered vulnerable to malicious attempts to obtain sensitive information (e.g., credit card information), and organizations were susceptible to attacks that attempted to disable their services and unearth their data.[26] The frequency and financial impact of these incidents was disturbing. According to a September 2014 report from Pricewaterhouse Coopers, there had been 42.8 million information security incidents worldwide over the previous year, costing victims an average of $2.7 million;[27] and in the same year, the Center for Strategic and International Studies (CSIS) released a report estimating that cybercrime cost the world economy more than $445 billion (nearly 1% of the world's income) per year.[28] What's more, some of the individual attacks had devastating consequences. The "Love Letter" virus, for example, cost between $4 and $10 billion, which according to James Adams, a successful entrepreneur and widely published author in the cyber-security field, is "the equivalent of a complete obliteration of a major American city."[29, 30]

Even as experts called for improved cyber-security, they disagreed about how best to achieve it. This stemmed in part from a foundational disagreement about why the Internet was insecure. Some argued that the problem was technological. Seen from this point of view, developers—dating to the Internet's genesis—had prioritized ease of use, not security. "The Internet," suggested Joseph Menn, a technology industry author and *Reuters* reporter, "was basically in beta when it got out of the lab and escaped, but now the world economy depends on it."[31] Others, however, felt that people, not technology, were the linchpin of IT security. This perspective emphasized that security hinges more on the people operating at the endpoints of electronic connections making good decisions and keeping their defenses up-to-date.[32] Put differently, networks help computers connect and communicate with one another, but it is primarily up to humans to decide whether sending and accepting those messages is a good

idea.

With Internet-related security issues becoming more prominent, the IT security industry had become extremely lucrative and was trying to leverage an array of strengths and mitigate several weaknesses as it continued to expand. In 2013, the IT security sector—which designed and marketed products like authentication software, anti-malware, and firewalls—was valued at $60 billion and expected to expand tenfold over the next decade.[33] According to Richard Stiennon, the founder of IT-Harvest (an IT security analyst firm) and a widely published author and veteran analyst in the IT security field, the sector benefitted from extraordinary innovation in the face of new security threats and substantial information sharing among providers and subscribers;[34] in addition, the sector's research, Menn argued, "can be extremely helpful in understanding how malicious software spreads, who is behind it, and what to look out for." Nonetheless, the IT security sector also had weaknesses. Chief among them were, as Stiennon noted, that many security firms were vulnerable to attacks and, as Menn added, "that many companies make exaggerated claims about their detection ability."

Hacktivism

One of the forces to which IT security companies were responding was hacktivism, an increasingly prominent but difficult-to-define and highly controversial phenomenon. A combination of the words "hacking" and "activism," the term "hacktivism" was first used in 1996 by a group that used technology to promote human rights and "protect the free flow of information."[35] Within several years, the media began to apply the word "hacktivism" to the activities of groups that engaged in Distributed Denial of Service (DDoS) attacks—efforts to drive traffic to and overload a website—and other strikes against the websites of organizations involved in the Kosovo War. By 2015, there were more than 1,000 hacktivist organizations worldwide.[36, 37] Nonetheless, it was difficult to pin down precisely what made someone a hacktivist (some said a unifying element was the belief that "information on the Internet should be free"), and some feared that the difficulty of parsing the term contributed to a trend in which all hacktivists were unfairly maligned.[38]

Peter Krapp, a professor of film and media studies at the University of California-Irvine, and a widely published writer on hacktivism, elaborated on this problem in an e-mail exchange. He wrote:

> Hacktivism is a controversial term. Some argue it was coined strictly to describe how electronic direct action might work toward social change by combining programming skills with critical thinking. Others use it as practically synonymous with malicious, destructive acts that undermine the security of the Internet as a technical, economic, and political platform. Yet others associate it specifically with expressive politics, free speech, human rights, or information ethics. ... If we start using the term too loosely, it stops being a meaningful term and starts to be a catch-all to scare people.[39]

Melissa Hathaway, formerly the acting senior director for cyberspace at the National Security Council and a cybsersecurity advisor to Presidents George W. Bush and Barack Obama, echoed this point. In particular, she emphasized that it is important to distinguish between hacktivists who are legally and peacefully expressing a political viewpoint and hackers engaging in activity that is disruptive to civil society or criminal. To separate these behaviors, Hathaway, who now runs a consulting firm focused on cybersecurity, suggests identifying an analog between hackers' behavior in the digital world and more familiar activity in the physical world. For example, when hackers use Twitter to organize peaceful protests on the streets, they are neither engaging in illegal activity nor disrupting civil society. By contrast, a distributed denial of service attack (DDoS) that brings down a business or government agency's website can prevent that organization from operating. That is disruptive. Going one step further, hackers who obtain and release a group's documents and e-mails are engaging in illegal activity, not dissimilar to criminals breaking and entering into and removing property from a home. Separating these behaviors is critical, Hathaway emphasizes, because, on the one hand, the United States prides itself on protecting freedom of speech; at the same time, it is imperative to prevent criminal activity. Policymakers therefore must ask themselves whether hacktivism is "disrupting civil society" and "What is this [analogous to] in my physical world?"[40]

Anonymous

One of the most prominent hacktivist organizations in the world in 2011—and one of the groups that inspired the debate over the meaning of hacktivism—was Anonymous. Established as an offshoot of 4chan.org, a popular website with anonymous, time-limited discussion forums,[41] Anonymous began to gain substantial media attention in 2008 when it launched Project Chanology, a series of actions—including a DDoS attack—targeting the Church of Scientology.[42] By early 2011, Anonymous had developed even more notoriety for its actions directed at (among others) the Westboro Baptist Church; governments; and major financial firms like PayPal, MasterCard, and Visa.[43]

Anonymous's operations generated substantial controversy. To critics, the group's activities were often criminal and extremely dangerous. "This really is cyberwar, and I don't use that term in a sensational way," said Richard Power, the author of a book on cybercrime in the 1990s. "You're looking at not just one particular cause. You're attacking the whole power structure. It involves some core critique."[44] But others lauded the hacktivists (whose missions, such as launching DDoS attacks against Tunisian government websites during the Arab Spring, often had a social justice bent) as "a digital version of Robin Hood."[45] Regardless of whether one supported Anonymous, there was no denying the collective's growing clout. In 2012, *Time* identified Anonymous as one of the 100-most influential people in the world.[46]

The Role of Government

The combination of the Internet's increasing prominence, the difficulty of securing it, and hacktivists' growing sophistication had created enormous challenges for U.S. government

officials. To some extent, the impediment to securing the Internet lies in its scope: widely used across the globe, the Internet cannot be policed by a single country. Unfortunately, achieving transnational coordination is difficult because of a dearth of mutual assistance agreements on cybercrime as well as the fact that some cyber-attacks are sponsored by nations with which the United States has tense relations (e.g., North Korea and Iran).[47] Meanwhile, the domestic regulatory landscape is fractured. According to a 2009 White House report, responsibilities for cybersecurity are scattered across multiple agencies and departments, including the Department of Homeland Security (which has an Office of Cybersecurity and Communications), the FBI, and the CIA (which announced a plan in March 2015 to create a special division devoted to cyber espionage).[48] Yet another coordination difficulty involves the private sector, from which many new technologies emerge and which plays a key role in protecting the Internet but with which the government can bolster its partnership.[49]

Establishing effective coordination and security will prove difficult (particularly because it will need to be balanced against the imperatives of ensuring privacy and civil liberties), but it is also crucial to ensure the well-being of U.S. citizens. The White House report concluded, "Cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights."[50]

Or as President Obama put it more colorfully in a February 2015 address, "The cyberworld is the Wild Wild West – to some degree, we're asked to be the sheriff."[51]

November 2009 - December 2010: The Struggles of HBGary Federal

Early in Barr's tenure as CEO, HBGary Federal, tried to secure a foothold in "incident response," a market that sells forensic services and products to organizations attempting to thwart cyber-attackers. But Barr's efforts were unsuccessful, and the company—which had just three employees—was barely surviving by selling $25,000 "social media training[s]."[52] As a result, in early October 2010, Hoglund, HBGary, Inc.'s CEO, wrote an e-mail to Barr saying, "We should have a pow-wow about the future of HBGary Federal. [HBGary President] Penny [Leavy] and I both agree that it hasn't really been a success... You guys are basically out of money and none of the work you had planned has come in." Barr concurred, replying, "This has not worked out as any of us have planned to date and we are nearly out of money."[53, 54]

Looking back, Hoglund and Barr, some believe, should have begun a dialogue about the company's woes earlier or even anticipated the likelihood of such a negative outcome when they launched the venture. According to Stiennon, most IT security firms enter a new market with a tested product, venture capital funding, and a distribution strategy. Most firms also wait a long time to enter the market for federal government services because the process of securing those contracts is extremely long and tedious. HBGary Federal, however, immediately plunged into that market and seemed to lack a clear product

(or solution to a problem) and strategy. As a result, the firm's success was largely dependent on Barr's whims.

Stiennon explained:

> In HBGary's case, they hired a figure who gave them a piece of the action. That was different than the way most organizations do it. It was almost like they were just an opportune, 'Hey, I like your product. I can sell it for you. Let me set up a separate company and I'll be a reseller of your product.' Of course, that allowed this personality, Aaron Barr, to be in a position to fly off on tangents just going after opportunistic things that he discovered, which in this case [was], 'Make a name for ourselves by blabbering about Anonymous on Twitter.'

January 1, 2011 – February 4, 2011: The Search and The Press

As the New Year got underway, Barr began his research into Anonymous. Up until that point, the FBI and other law enforcement agencies had struggled to stop Anonymous because according to some, the group did not have any leaders but instead was "a shape-shifting subculture."[55, 56]

As he began his research, Barr, however, started to think the group had distinct leaders. To discern this, he started to spend time in Anonymous' Internet chat rooms and then attempted to match the comments made in the chat rooms with simultaneous social media posts, especially via Twitter; he then gleaned additional information about possible members from other sites, like LinkedIn and Facebook.[57]

After employing these techniques for several weeks, Barr was convinced that he had honed in on three of Anonymous's key operatives (two in California and one in New York). As Barr—who had also compiled a 20-page document with information on potential members—wrote in an e-mail to a coworker, "They think I have nothing but a heirarchy [sic] based on IRC [Internet Relay Chat] aliases! As 1337 [elite] as these guys are supposd [sic] to be, they don't get it, I have pwned [owned] them! :)"[58] Yet Barr's colleagues lacked confidence in his analysis and were wary of the impact that it could have on them and the firm. One programmer questioned Barr, writing: "Step 1: Gather all the Data Step 2: ??? Step 3: Profit."[59] The coder later shared his concerns with a company official, writing in an e-mail, "I feel his arrogance is catching up to him again and that has never ended well ... for any of us."[60]

Nonetheless, Barr began to make plans to disseminate his research. This included scheduling a presentation at BSides, the technology security conference in San Francisco in February. He also developed plans—which would involve HBGary, Inc.'s communications staff—to start reaching out to the press. "This will generate a big discussion in Anonymous channels, which are attended by the press," Barr wrote in an e-mail to senior company officials in late January.[61]

Looking back, analysts offered conflicting perspectives on the wisdom of HBGary, Inc.'s decision to allow Barr to initiate and publicize his research. Stiennon suggested that HBGary, Inc. should have been far more cautious. "Most organizations," he argued, "would not put up with a federal salesperson who made that much

noise in public. The chief marketing officer would shut them down immediately. 'You're going off message, you haven't cleared it with us.'"

Menn, who wrote about Barr's research as a reporter for *The Financial Times* in 2011, was more sympathetic. He acknowledged that "Barr was honestly wrong and overconfident, and that there was insufficient review of his work by others before he went public;" however, he also emphasized that some of his findings may have been accurate and that, unlike the hacktivists, he did nothing illegal. "Yes, Barr thumbed his nose at the wrong people," Menn added. "But he did nothing criminal, and they did, and the world would be a worse place if we all avoided doing legal things because we were afraid of criminals."

The morals of his plan notwithstanding, Barr's strategy was extremely risky. As comedian Stephen Colbert later quipped, "To put this in hacker terms, Anonymous is a hornet's nest, and Barr said, 'I'm going to stick my [private parts] in that thing.'"[62]

The Story Breaks

Nonetheless, the company went forward with Barr's proposed strategy. Specifically, the public relations staff reached out to Menn, then a reporter at *The Financial Times*, who agreed to do an interview with Barr. As Menn later explained, he commonly interviewed technology security experts in advance of their presentations at security conferences, and he thought that it was worth speaking to Barr. This was in part because he thought Barr's analytical approach of using social media to identify Anonymous's leaders was an "interesting idea. "I was also swayed by the fact," Menn added, "that while I had never heard of Aaron Barr, I had known the head of HBGary proper, a guy named Greg Hoglund, for years. And Greg is a very, very smart guy and extremely capable. And HBGary proper had a good reputation with a lot of people I've known who are experts in security."

Menn later characterized the interview with Barr as a "mixed bag." On the one hand, Barr provided a "plausible overview" of his strategy for and success in tracking down Anonymous's leaders. On the other, Barr did not disclose the names of the leaders he believed he had identified.

Consequently, Menn wrote what he later described as "a middle of the road piece" about Barr's research. Titled "Cyberactivists Warned of Arrest," the story—which was published in *The Financial Times* on Friday, February 4, 2011—described how through using social media techniques, Barr believed he had tracked down Anonymous's leaders, including a man in New York who used the alias "Owen" and multiple senior members in California. It also mentioned Barr's upcoming talk at the B-Sides conference. The lone quotation from Barr in the piece was embedded in a broader statement about Anonymous's leadership. Menn wrote: "Of a few hundred participants in operations, only about 30 are steadily active, with 10 people who 'are the most senior and coordinate and manage most of the decisions,' Mr. Barr told the Financial Times." The story also emphasized that Barr was not planning to "give specifics [about Anonymous's leadership] to police" and that his conclusions about the identities of leaders were simply "educated guesses."[63]

At the time, Menn thought the story "was not a major piece by any stretch." ("Little did I know," he later said, in an allusion to the article's far-reaching consequences.) Barr, however, immediately embraced the article—and the buzz it began to generate—as the break that he and his firm had been seeking. In an e-mail to Hoglund and Leavy, HBGary, Inc.'s senior leaders, he wrote, "Story is really taking shape." Hoglund replied, "We should post this on the front page, throw out some tweets, 'HBGary Federal sets a new bar as private intelligence agency.' The pun on bar is intended lol." Upon seeing the article, the FBI contacted Barr, and they planned to meet on Monday morning.[64]

Heading into the weekend, Barr believed that he had unlocked the key to his company's salvation. Little did he know that the company's demise was imminent.

Index

1. Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*, Little Brown and Company: New York, 2012, pp. 5-6.

2. Robert Mackey, "'Operation Payback' Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks," *The New York Times*, December 8, 2010, available at http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks/ (accessed on December 5, 2015).

3. "Security B-Sides Announces 2011 Speaker Line-Up & Participants at B-Sides San Francisco," *Market Wired*, February 8, 2011, available at http://www.marketwired.com/press-release/security-b-sides-announces-2011-speaker-line-up-participants-b-sides-san-francisco-1392222.htm (accessed on September 22, 2015); and Olson, *We Are Anonymous*, pp. 5-6.

4. Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, Verso: London, 2014, Amazon Kindle Edition, Chapter 7.

5. Joseph Menn, "Cyberactivists Warned of Arrest," *The Financial* Times, February 5, 2011, available at http://www.ft.com/intl/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html#axzz3ksQm5IRg (accessed on September 5, 2015).

6. Coleman, *Hacker, Hoaxer...*, Chapter 7.

7. Jerome Taylor, "Hacktivists Take Control of Internet Security Firms," *The Independent (London)*, October 22, 2011, available at http://www.independent.co.uk/news/media/online/hacktivists-take-control-of-internet-security-firms-2207440.html (accessed on September 22, 2015); and Nate Anderson, "How One Man Tracked Down Anonymous—and Paid A Heavy Price," *ArsTechnica*, February 9, 2011, available at http://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/ (accessed on December 5, 2015).

8. Coleman, *Hacker, Hoaxer...*, Chapter 7.

9. For full quotations, see Olson, *We Are Anonymous*, pp. 19-20.

10. Lulz is "a corruption of the phrase 'laugh out loud' and a reference to hackers' penchant for tomfoolery." Ty McCormick, "Hacktivism: A Short History," *Foreign Policy*, April 29, 2013, available at http://foreignpolicy.com/2013/04/29/hacktivism-a-short-history/ (accessed on September 23, 2015).

11. Brian Krebs, "HBGary Federal Hacked by Anonymous," *Krebs on Security*, February 11, 2011, available at http://krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/ (accessed on September 22, 2015).

12. Joseph Menn, "'Hacktivists' Retaliate Against Security Expert," *The Financial Times*, February 7, 2011, available at http://www.ft.com/intl/cms/s/0/0c9ff214-32e3-11e0-9a61-00144feabdc0.html#axzz3ksQm5IRg (accessed on September 5, 2015); and "WhiteHat History," WhiteHat Security, available at https://www.whitehatsec.com/company.html (accessed on September 22, 2015).

13. Kim Zetter, "Anonymous Hacks Security Firm Investigating It; Releases E-Mail," *Wired*, February 7, 2011, available at http://www.wired.com/2011/02/anonymous-hacks-hbgary/ (accessed on September 5, 2015).

14. "HBGary Unveils Digital DNA Technology," *Forensic Focus*, March 12, 2009, available at http://www.forensicfocus.com/index.php?name=News&file=article&sid=1103 (accessed on September 6, 2015); "Greg Hoglund," RSA Conference, available at http://www.rsaconference.com/speakers/greg-hoglund (accessed on September 6, 2015); and "What is a Rooktkit Virus?" pctools by Symantec, available at http://www.pctools.com/security-news/what-is-a-rootkit-virus/ (accessed on November 30, 2015).

15. Hoglund co-authored the book, *Rootkits: Subverting the Windows Kernel*; he also created a well trafficked website, www.rootkit.com, devoted to researching this tool. "Greg Hoglund," RSA Conference; Greg Hoglund and James Butler, *Rootkits: Subverting The Windows Kernel*, Addison Wesley: Upper Saddle River, 2006, p. xxi; and Lucian Constantin, "Rootkit.com Compromise Poses Risks To Other Sites," *InfoSec News*, posted on website of Department of Information and Technology, City of Seattle, February 15, 2011, available at http://techtalk.seattle.gov/2011/02/15/rootkit-com-compromise-poses-risks-to-other-sites/ (accessed on September 23, 2015).

16. Peter Bright, "With Arrests, HBGary Hack Saga Finally Ends," *ArsTechnica*, March 10, 2012, available at http://arstechnica.com/tech-policy/2012/03/the-hbgary-saga-nears-its-end/ (accessed on November 30, 2015); and "HBGary Launches HBGary Federal," *Forensic Focus*, December 9, 2009, available at http://www.forensicfocus.com/index.php?name=News&file=article&sid=1314 (accessed on November 30, 2015).

17. Mark Anderson, Brad Stone and Michael Riley, "Hacker vs. Hacker," *Bloomberg Business*, March 10, 2011, available at http://www.bloomberg.com/bw/magazine/content/11_12/b4220066790741.htm (accessed on December 5, 2015); "ManTech Announces Financial Results for First Quarter of 2012," ManTech International Corporation, May 3, 2012, available at http://investor.mantech.com/releasedetail.cfm?ReleaseID=670241 (accessed on September 23, 2015); and Olson, *We Are Anonymous*, p. 5.

18. Olson, *We Are Anonymous*, p. 5.

19. According to the Department of Defense, signals intelligence refers to "intelligence derived from communications, electronic, and foreign instrumentation signals." "Department of Defense Dictionary of Military and Associated Terms," Department of Defense, November 8, 2010 (as amended through November 15, 2015), pp. 221-222, available at http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed on November 30, 2015).

20. Olson, *We Are Anonymous*, p. 5; Ally Schmidt, "Northrop Grumman: A Top 10 U.S. Defense Contractor," *Market Realist*, February 24, 2015, available at http://marketrealist.com/2015/02/northrop-grumman-top-10-us-defense-contractor/ (accessed on December 5, 2015); and Coleman, *Hacker, Hoaxer...*, Chapter 7.

21. Stone and Riley, "Hacker vs. Hacker."

22. Aaron Barr: "Computer Security Is A 'Hunt, An Investigation, It's A Challenge,'" *Executive Biz*, June 2, 2010, available at http://blog.executivebiz.com/2010/06/aaron-barr-computer-security-is-a-hunt-an-investigation-its-a-challenge/ (accessed on September 5, 2015).

23. For additional details on the role of the U.S. government and American universities in the genesis of the Internet, see "NSF and The Birth of the Internet – 1960s," National Science Foundation, available at http://www.nsf.gov/news/special_reports/nsf-net/textonly/60s.jsp (accessed on September 23, 2015); and "History of the Internet," New Media Institute, 2014, available at http://www.newmedia.org/history-of-the-internet.html (accessed on September 23, 2015).

24. James Manyika and Charles Roxburgh, "The Great Transformer: The Impact of The Internet On Economic Growth and Prosperity," McKinsey Global Institute, October 2011, available at http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_transformer (accessed on September 23, 2015).

25. Castells lamented that even though the Internet is ubiquitous, there are "great levels of inequality in bandwidth, efficiency, and price." Manuel Castells, "The Impact of the Internet on Society: A Global Perspective," *MIT Technology Review*, September 8, 2014, available at http://www.technologyreview.com/view/530566/the-impact-of-the-internet-on-society-a-global-perspective/ (accessed on September 23, 2015).

26. Kenneth Rapoza, "The Top 10 Security Issues That Will Destroy Your Computer In 2013," *Forbes*, December 5, 2012, available at http://www.forbes.com/sites/kenrapoza/2012/12/05/top-10-security-issues-that-will-destroy-your-computer-in-2013/ (accessed on September 23, 2015).

27. "Security Incidents Continue to Rise in Cost and Frequency While Budgets Decrease, according to PwC, CIO and CSO's The Global State of Information Security Survey 2015," PWC, September 30, 2014, available at http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html (accessed on November 30, 2015).

28. Ellen Nakashima and Andrea Peterson, "Report: Cybercrime and Espionage Costs $445 Billion Annually," *The Washington Post*, June 9, 2014, available at https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html (accessed on September 25, 2015).

29. Richard Power, "The Financial Costs of Computer Crime," PBS Frontline, 2001, available at http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/cost.html (accessed on September 28, 2015); and "About," Adams Strategy Group, available at http://adamsstrategygroup.com/about/ (accessed on January 28, 2016).

30. For more information on the "ILOVEYOU virus," see Larry Seltzer, "'I Love You,' Virus Turns Ten: What Have We Learned?", *PC Magazine*, April 28, 2010, available at http://www.pcmag.com/article2/0,2817,2363172,00.asp (accessed on September 28, 2015); Mark Ward, "A Decade On From The ILOVEYOU Bug," *BBC News*, May 4, 2010, available at http://www.bbc.com/news/10095957 (accessed on December 5, 2015); and Mark Landler, "A Filipino Linked To 'Love Bug' Talks About His License To Hack," *The New York Times*, October 21, 2000, available at http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html (accessed on September 28, 2015).

31. Interview with Joseph Menn, by telephone, September 3, 2015. Hereafter cited as Menn interview. Unless noted, subsequent quotations from and attributions to Menn come from this interview and a follow-up interview conducted via e-mail on September 25, 2015.

32. The FBI for example advises Americans to (among other things) use caution with what they download and keep their operating systems and anti-virus software up-to-date. "How to Protect Your Computer," FBI, available at https://www.fbi.gov/scams-safety/computer_protect (accessed on January 1, 2016).

33. Richard Stiennon, "IT Security Industry To Expand Tenfold," *Forbes*, August 14, 2013, available at http://www.forbes.com/sites/richardstiennon/2013/08/14/it-security-industry-to-expand-tenfold/ (accessed on September 5, 2015).

34. Interview with Richard Stiennon, by telephone, September 23, 2015. Hereafter cited as Stiennon interview. Unless noted, subsequent quotations from and attributions to Stiennon come from this interview and a follow-up interview conducted via e-mail on September 24, 2015.

35. McCormick, "Hacktivism: A Short History."

36. Dorothy Denning, "The Rise of Hacktivism," *Georgetown Journal of International Affairs*, September 8, 2015, available at http://journal.georgetown.edu/the-rise-of-hacktivism/ (accessed on September 28, 2015).

37. According to the U.S. Department of Justice, "DDoS attacks are attempts to render a computer unavailable to users through a variety of means, including by saturating the target computers or networks with external communication requests, thereby denying service to legitimate users." Melinda Hagg, "Major Achievements in the Courtroom: United States v. 'Anonymous,'" Offices of the United States Attorneys, United States Department of Justice, available at http://www.justice.gov/usao/priority-areas/cyber-crime/major-achievements-courtroom-united-states-v-anonymous (accessed on September 23, 2015).

38. McCormick, "Hacktivism: A Short History."

39. Interview with Peter Krapp, Professor, Department of Film & Media Studies, University of California-Irvine, by e-mail, September 24, 2015. Hereafter cited as "Krapp interview." Unless noted, subsequent quotations from and attributions to Krapp come from this e-mail.

40. Interview with Melissa Hathaway, President, Hathaway Global Strategies, LLC, by telephone, October 25, 2015.

41. For more information on 4Chan, see Caitlin Dewey, "Absolutely Everything You Need To Know To Understand 4Chan, The Internet's Own Bogeyman," *The Washington Post*, September 25, 2014, available at https://www.washingtonpost.com/news/the-intersect/wp/2014/09/25/absolutely-everything-you-need-to-know-to-understand-4chan-the-internets-own-bogeyman/ (accessed on September 23, 2015); "4Chan," available at http://www.4chan.org (accessed on September 24, 2015); and McCormick, "Hacktivism: A Short History."

42. For more details on Project Chanology, see David Kushner, "The Masked Avengers," *The New Yorker*, September 8, 2014, available at http://www.newyorker.com/magazine/2014/09/08/masked-avengers (accessed on September 28, 2015); and Patrick Barkham, "Hackers Declare War on Scientologists Amid Claims of Heavy-Handed Cruise Control," *The Guardian (London)*, February 4, 2008, available at

http://www.theguardian.com/technology/2008/feb/04/news (accessed on November 30, 2015).

43. Bill Gardner and Valerie Thomas, *Building An Information Security Awareness Program*, Elsevier: Waltham, 2014, p. 11, accessed via Google Books on September 30, 2015.

44. Somini Sengupta, "The Soul of the New Hacktivist," *The New York Times*, March 17, 2012, available at http://www.nytimes.com/2012/03/18/sunday-review/the-soul-of-the-new-hacktivist.html (accessed on December 6, 2015).

45. Yasmine Ryan, "Anonymous and the Arab Uprisings," *Al Jazeera*, May 19, 2011, available at http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html (accessed on September 24, 2015); and Adam Carter, "From Anonymous To Shuttered Websites, The Evolution of Online Protest," *CBC News Canada*, March 15, 2012, available at http://www.cbc.ca/news/canada/from-anonymous-to-shuttered-websites-the-evolution-of-online-protest-1.1134948 (accessed on September 5, 2015).

46. Barton Gellman, "Anonymous," *Time*, April 18, 2012, available at http://content.time.com/time/specials/packages/article/0,28804,2111975_2111976_2112122,00.html (accessed on September 29, 2015).

47. Denning, "The Rise of Hacktivism"; and Joseph Menn, *Fatal System Error: The Hunt for The New Crime Lords Who Are Bringing Down The Internet*, Public Affairs: New York, 2010, pp. 231-236.

48. "Cyberspace Policy Review: Assuring A Trusted and Resilient Information and Communications Infrastructure," The White House, May 8, 2009, p. i available at https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed on September 24, 2015); "Office of Cybersecurity and Communications," Department of Homeland Security, October 27, 2015, available at http://www.dhs.gov/office-cybersecurity-and-communications (accessed on January 28, 2016); Richard Quinn, National Security Assistant Special Agent in Charge, Philadelphia Field Office, FBI, Statement Before the House Homeland Security Committee, Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies, April 16, 2014, available at https://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security (accessed on September 23, 2015); and Brian Bennett, "CIA To Create A Digital Spy Division," *Los Angeles Times*, March 6, 2015, available at http://www.latimes.com/nation/nationnow/la-na-nn-cia-cyber-espionage-20150305-story.html (accessed on September 24, 2015).

49. "Cyberspace Policy Review...," pp. iv-v and 17-19; and Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing Securing America's Cyber Future: Simplify, Organize and Act, Before the House Committee on Homeland Security Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology, March 10, 2009, pp. 4-5, available at https://www.whitehouse.gov/files/documents/cyber/Congress%20-%20Charney-microsoft-SFR_10Mar09.pdf (accessed on September 23, 2015).

50. "Cyberspace Policy Review...," p. i.

51. Nicole Perlroth and David Sanger, "Obama Calls for New Cooperation To Wrangle The 'Wild West' Internet," *The New York Times*, February 13, 2015, available at http://www.nytimes.com/2015/02/14/business/obama-urges-tech-companies-to-cooperate-on-internet-security.html (accessed on September 25, 2015).

52. Stone and Riley, "Hacker vs. Hacker;" and Olson, *We Are Anonymous*, pp. 5-6.

53. Nate Anderson, "Spy Games: Inside The Convoluted Plot To Bring Down WikiLeaks," *ArsTechnica*, February 14, 2011, available at http://arstechnica.com/tech-policy/2011/02/the-ridiculous-plan-to-attack-wikileaks/ (accessed on September 5, 2015).

54. In fall 2010, Barr began talks with Hunton & Williams, a law firm that had several clients—including Bank of America—that reportedly might be interested in HBGary Federal's services. Barr therefore formed Team Themis (the title alludes to the Greek Titaness of divine order and justice), a partnership between HBGary Federal and two other security firms that marketed its services to Hunton & Williams. The plan that that Team Themis developed, details of which were released publicly following the hack proved extremely controversial and, according to some observers, proposed illegal activities. The parties never signed a contract.

Olson, *We Are Anonymous*, pp. 5-6; and Coleman, *Hacker, Hoaxer...*, Chapter 7.

55. Jeb Boone, "Anonymous: Sorry, FBI, You Don't Scare Us," *Salon* (via *The Global Post*), August 22, 2013, available at http://salon.com (accessed on September 6, 2015); and Kushner, "The Masked Avengers."

56. As if to reinforce Anonymous's nebulous and mysterious quality, group members in public protests sometimes sported a stylized mask of Guy Fawkes, a 17th-century Roman Catholic terrorist. The group's attachment to the mask originated in 2008 when, while planning protests as part of Project Chanology, Anonymous said to participants, "Cover your face. This will prevent your identification from videos taken by hostiles." "How Guy Fawkes Became The Face of Post-Modern Protest," *The Economist*, November 4, 2014, available at http://www.economist.com/blogs/economist-explains/2014/11/economist-explains-3 (accessed on September 24, 2015).

57. Coleman, *Hacker, Hoaxer...*, Chapter 7; and Stone and Riley, "Hacker vs. Hacker."

58. Anderson, "How One Man...."; and Olson, *We Are Anonymous*, p. 8.

59. Anderson, "How One Man...."

60. Coleman, *Hacker, Hoaxer...*, Chapter 7.

61. In the same exchange, Barr anticipated the possibility that his activities would provoke an attack from the hacktivists. He wrote, "But it will also make us a target. Thoughts?" Hoglund replied, "Well, I don't really want to get DDOS'd, so assuming we do get DDOS'd then what? How do we make lemonade from that?" Peter Bright, "HBGary's Open Letter: Full of Denials That Don't Hold Water," *ArsTechnica*, April 19, 2011, available at http://arstechnica.com/tech-policy/2011/04/hbgary-issues-denials-snipes-at-the-blog-o-sphere-in-open-letter/ (accessed on January 8, 2015).

62. Eric Bangeman, "*Colbert Report* Features Ars Anonymous/HBGary Coverage," *ArsTechnica*, February 25, 2011, available at http://arstechnica.com/staff/2011/02/our-anonymous-hbgary-coverage-on-colbert-report/ (accessed on September 7, 2015).

63. Menn, "Cyberactivists...."

64. Olson, *We Are Anonymous*, p. 9; and Coleman, *Hacker, Hoaxer...*, Chapter 7