The Rhetoric of Commoditized Vulnerabilities: Ethical Discourses in Cybersecurity

Brittany N. Hoskins

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Arts
In
English

Quinn Warnick, Chair
Carlos Evia
Sheila L. Carter-Tod

April 27, 2015
Blacksburg, VA

Keywords: Rhetoric, Cybersecurity, Hacking, Business Ethics, Gray Hat

The Rhetoric of Commoditized Vulnerabilities: Ethical Discourses in Cybersecurity

Brittany N. Hoskins

ABSTRACT

The field of cybersecurity is relatively uncharted by rhetoricians and sociologists but nevertheless laden with terminological assumptions, violent metaphors, and ethical conflicts. This study explores the discourse surrounding the morally contentious practice of hackers selling software vulnerabilities to third parties instead of disclosing them to the affected technology companies. Drawing on grounded theory, I utilize a combination of quantitative word-level analysis and qualitative coding to assess how notions of right and wrong on this topic are framed by three groups: 1) the hackers themselves, 2) technology companies, and 3) reporters. The results show that the most commonly constructed argument was based on a "greater good" ethic, in which rhetors argue for reducing risk to "us all" or to innocent computer users. Additionally, the technology companies and hackers assiduously build their ethos to increase their trustworthiness in the public mind. Ultimately, studying this unexplored area of "gray hat hacking" has important implications for policymakers creating new cybersecurity legislation, reporters attempting to accurately frame the debate, and information technology professionals whose livelihoods are affected by evolving social norms.

Acknowledgements

I would like to acknowledge first and foremost my awesome husband for his ongoing support and love; it's been great going on this adventure from careers to graduate school and back with you. There's a reason you're my favorite person in the world. I'd also like to thank my parents and my friends for encouraging me, loving me, and making me laugh.

At Virginia Tech, I'd like to thank my advisor, Dr. Quinn Warnick, for his candid advice and assistance on this project. He provided great resources and encouragement, and his door was always open to me. I'd also like to thank Dr. Katrina Powell for helping me frame the original project and my research questions, and my readers, Dr. Carlos Evia and Dr. Sheila Carter-Tod, for their helpful feedback on this project and others.

Table of Contents

List of Figures

Chapter 1: Introduction

Legal scholar Cassandra Kirsch asserts that rather than leveling off, "hacking incidents continue to increase in number and scope. The 2013 Target breach affected nearly a third of the U.S. population, and the FBI warns that attacks similar to the Target breach 'will continue to grow in the near term' despite its efforts" (384-385). The Target incident joins the ranks of other high profile attacks in the past five years, including the Sony Media breach and public hacktivist protests against major companies like PayPay by groups like Anonymous. In this context of increasing cybercrime, lawmakers and IT professionals must continually grapple with what hackers can realistically do, how to protect their systems, how to retaliate once an attack has happened, and how to regulate cyberspace. Equally as important is how we talk about the ethics of hacking and how this affects our conceptions of regulation and appropriate reactions. This study investigates the ethical arguments surrounding an area of hacking that is legal but morally debated (i.e. a gray hat hacking practice): the sale of software vulnerabilities to interested third-party buyers.

Before I delve into this highly nuanced hacking debate, it's important to first understand some of the existing terminological constructs that frame the cybersecurity field as a whole. For instance, when many of us hear the term "hacker," we think of an ethically questionable individual performing secret internet crime. Despite its connotation of wrongdoing, "hacking" can take a variety of forms—anything from reprogramming a piece of software to make it more useful, to stealing money and identities, to crashing a system. The outcome of hacking depends on the individual hacker and his or her goals, which may be nefarious or societally acceptable. Margaret Rouse of *SearchSecurity.com* explains that "hacker is a term used by some to mean 'a clever programmer' and by others, especially those in popular media, to mean 'someone who

tries to break into computer systems.'" Given that even the word hacker is imbued with a pervasive immoral meaning[1], it's evident that the ethics of computer security are complexly intertwined with the rhetoric we use to explain online concepts.

One of the most common constructs among computer scientists, hackers, and security reporters is the "white hats," "gray hats," and "black hats" classification system. Appropriating an ethical symbol from American cowboy movies, individual hackers are sorted into bad guys and good guys based on the color of their proverbial hats. The white hats find software problems and help affected technology companies (e.g., Microsoft, Apple, Google) fix them. Black hats perform online actions that are viewed as illegal or immoral, such as accessing another person's computer without permission. And "[s]omewhere in between the two extremes is the grey hat hacker, operating on the fringe of civil and criminal liability" (Kirsch 386). A gray hat participates in hacking activities that are morally controversial, e.g. infiltrating a company's network just to prove they can, hacking as a form of protest, reconfiguring an online program to give them access to free content. This terminological system is foundational to how hackers and hacker collectives self-identify or are externally labeled.

Two other terms that are rhetorically significant are "cyberwar" and "cyberattacks." "Cyberwar" was originally coined by John Arquilla and David Ronfeldt in 1992 as "a knowledge-related conflict at the military level," versus the similar term "netwar," or "societal struggles…associated with low intensity conflict by non-state actors, such as terrorists, drug cartels, or black market proliferators of weapons of mass destruction" ("Cyberwar is Coming!"). In the contemporary context, reporters and politicians use "cyberwar" indiscriminately, often as a catch-all term to describe such nonviolent practices as vandalizing a news site or performing a

[1] "Hacker" is typically not an offensive term within the security field; many security researchers self-identify as hackers. I will use the formal term "security researcher" interchangeably with "hacker" as both are common.

DDOS (distributed denial of service) "attack" that temporarily takes down a webpage. Online practices are often conflated with physical acts of war, which can result in confusion among politicians and ultimately, disproportionate reactions to cyberattacks. Therefore, in his examination of just war theory, Arquilla clarifies that "there is a big difference between cyber-disruption and physical destruction" ("Twenty Years of Cyberwar" 84). Similarly, Paul Rexton Kan points out that "[n]ational leaders warn of a cyberwar and cyberterrorism that may lead to a potential 'cyber Pearl Harbor'…However, these concepts are a retrofitting of those used in the physical domain to describe violent acts and responses to them" (111). It's important for rhetoricians to complicate pervasive metaphors like these and study the effects they might have on the audiences who internalize them.

Though the rhetoric of cyberwar has been studied in a limited capacity, discourses surrounding various day-to-day cybersecurity practices have not been analyzed. In particular, rhetoric surrounding the discovery, disclosure, and perceived ownership of software "vulnerabilities," also known as "bugs," "flaws," or "holes" in code has not been studied. The Microsoft Security Response Center defines vulnerabilities as "a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product" ("Definition of a Security Vulnerability"). Essentially, these vulnerabilities can act as back doors to hackers seeking ways to manipulate code for various purposes. Upon finding a "hole," hackers can create an "exploit" or "attack code" that takes advantage of it in order to perform some sort of action (e.g., collect information, modify the program, take control of the machine) (Rouse). In other words, a vulnerability is found while an exploit is developed.

Within the broader field of vulnerability management, I specifically explore the rhetoric surrounding buying and selling software vulnerabilities and exploits. Until approximately five

years ago, security researchers were expected—as a social norm—to privately disclose the vulnerabilities they found directly to companies like Google and Adobe. In return, they were thanked privately, acknowledged in vulnerability documentation once the code was fixed, or given small monetary rewards; however, recently security research companies like VUPEN, ReVuln, Exodus Intelligence, Endgame Systems, and Netragard have challenged the existing model and begun selling the vulnerabilities they find and the exploits they develop to their customers (usually government agencies with the financial resources to buy a vulnerability subscription package). The emergence of commoditized vulnerabilities as a business model has generated a heated debate across the security community.

In my previous career as a communications professional for Microsoft, I spent two years watching security incidents unfold, reading news coverage, and joining in the conversation by writing security blog posts and statements. During this time, I was intrigued by the growing controversy over selling vulnerabilities and how much agitation the practice caused on the part of security reporters and companies like Microsoft and Google. With each new blog post and news report that appeared on this topic, the online security community publicly wrestles with the tension between assumed codes of conduct and a new model. For instance, Dennis Fisher of *Threatpost* verbalizes a communal distaste for VUPEN's business, writing, "This is one of the things that bothers other researchers and some vendors about the way that VUPEN does business. Doesn't selling bugs to one customer leave everyone else exposed to their use?" Here we see VUPEN's actions framed as "exposing" end users to increased risk. These are the types of rhetorical markers I identify to analyze ethical arguments.

In light of this controversy, I examine the rhetoric surrounding vulnerability sales to better understand how different rhetors use language to frame ethical behavior. Instead of

accepting that certain online actions are innately good or evil, I investigate how the ongoing conversations of the broad security community (e.g., technology companies, security reporters, hackers) are framing ethical norms over time with regard to this gray hat hacking practice. As Gjalt de Graaf argues, "For business ethics researchers, it is important that a discourse analysis can show how forces in language influence moral positions.… Discourse analysis can also gain perspectives into the structure, dynamics, and directions of conflicting discourses, like narrative strategies" (593-594). As this practice is relatively new (VUPEN cites changing its business model in 2010), the broader security community is still struggling with whether these actions are morally tolerable. Thus, the discourse is ahead of any concrete policies, meaning that trends in rhetoric will incrementally influence the responses of governments, businesses, and lawmakers to this practice.

Literature Review

Existing Scholarship

As Ellen Barton argues in an examination of bioethics, rhetoricians can bring an important perspective to ongoing ethical debates outside our field through a methodical study of language. She notes that "the fundamental insight that composition/rhetoric offers to the literature on ethics and bioethics is that decision-making with ethical dimensions is most often interactional and therefore rhetorical. In other words, such decision making takes place between real people, in real time, in (semi-) ordinary language..." (599). Likewise, the security community is made up of security researchers, reporters, and company representatives who publicly discuss the sale of vulnerabilities, all the while shaping the ethics of the practice.

Rhetorical criticism is particularly important in this debate as computer scientists and political experts have produced most of the existing online security scholarship. In lieu of language, their investigations focus on the real-world implications of cyber-attacks (e.g., the tangible effects of malware, the potential for cyberwar, or how lawmakers should handle the increasing potency of hacking techniques). By and large, scholars have problematized misconceptions of malware and especially apocalyptic speculations that overstate the reality of what hackers can do. Numerous academics (Bendrath, Brito, Helmreich, Libicki, Rid) have attempted to better define the results of "in-the-wild" hacking, taking into consideration the sizeable investment of time, effort, and strategy it takes to create functional exploits that can do any degree of damage to a country's infrastructure. There is agreement across these experts that the frequent *sky-is-falling* speculation around large-scale, nation-level cyberwars is currently unrealistic. For instance, Roger Clarke attempts to quell cyberwar hype by delineating specific categories of malware based on their "attack vectors" and the "payloads" they deliver. His

intention is to help policymakers navigate the complex security conversation; nonetheless, his framework still relies subconsciously on war metaphors. Thus we encounter a dynamic in which industry computer scientists both critique inflammatory language while still utilizing it to describe how hackers operate.

Secondly, rhetorical study is needed in this area because much of the existing scholarship was produced between 2000 and 2007 in response to the growing number of global internet users, yet "offensive" and "defensive" security techniques have been changing at a rapid pace since then. It's necessary to explore trends in security discourse from the past few years. The conversation and analysis from earlier in the evolution of the computer science field is only partially relevant to today's challenges and doesn't address emergent topics like the commoditization of vulnerabilities.

Beginning to scratch the surface on these more timely issues, Alana Maurushat outlines the legal and ethical implications of different types of vulnerability disclosure. Specifically, her work centers on whether security researchers should disclose their vulnerability findings privately to affected technology companies or publicly. She systematically discusses and defines methods of disclosure, but does so from an applied legal perspective, without challenging the existing linguistic framework or discussing vulnerability sales in-depth (21-32). Similarly, Cassandra Kirsch examines the history of gray hat hacking and how the Computer Fraud and Abuse Act has been interpreted to regulate certain actions, arguing that corporations should work more closely with gray hat hackers (387-403).

Ashish Arora, Anand Nandkumar, and Rahul Telang track the trajectory of 328 vulnerabilities to determine the real-world effects of "secret" disclosure as compared to web disclosure. Their empirical study finds that public vulnerability disclosures increase the risk of

end users being exploited, but conversely, that hackers also take advantage of patched vulnerabilities before users apply the needed updates. Even though this study provides useful statistics on the risks associated with disclosures, it doesn't make the jump to the real-world effects of selling vulnerabilities rather than patching them. Alongside my research on vulnerability sales rhetoric, studies of the real-world impact of vulnerability sales on exploit attempt levels would help regulators and IT professionals have a more informed, less reactionary approach to these cybersecurity issues.

A Rhetorical Perspective

From a humanities perspective, although the field of cybersecurity rhetoric is currently in its infancy, scholars have approached the closely related topic of code studies. Rhetoricians are bringing new insights to the burgeoning field, examining the inherent power structures and assumptions built into the language of the internet. For example, Riley's exploration of the <style> tag and the latent assumption that content and design can be conceived separately (67-80) or Rickert's explication of the mind and body duality inherent in HTML's <head> and <body> tags (1-20). Though these instances represent a clear manifestation of rhetorical theory as applied to coding, an examination of actual discourse from the hackers who create and modify this code remains limited. This gap in scholarship provides an impetus for my research.

The language-level studies that do exist for online security have focused almost exclusively on state and nation-level cyber-rhetoric and have not systematically examined the everyday business decisions that hackers (of all hat colors) are making—studies like Myriam Dunn Cavelty's inquiry into the growth of cyber-terrorism discourse as a reflection of physical acts of terrorism (like the 1995 Oklahoma City bombing). Cavelty asserts that vague terminology feeds public fears regarding the potential for a crippling attack on U.S. infrastructure and

explains that positioning hackers as "dangerous other[s]" "located outside the U.S., both in geographical and moral terms" (30) compounds panic. In response, she argues that a "unilateral" government cybersecurity plan is a reaction to the discourse, not a practical fit for protecting the United States' decentralized infrastructure.

Similarly, Laurie Blank explains the possible consequences of terminological inflation, comparing trends in cybersecurity rhetoric to those following 9/11. She argues that the "war on terror" discourse afforded authority figures too much unchecked authority in the years following the September 11 attacks and worries that the same could be true of hacking rhetoric. She cautions:

> …the term "cyber attack" is regularly used in the mass media to denote an extremely wide range of cyber conduct, much of which falls well below the threshold of an 'armed attack' as understood in the *jus ad bellum* or an attack as defined in the law of armed conflict…[this rhetoric] can create situations in which a State has fewer obstacles to an aggressive response to cyber threats or cyber conduct, stretching or overstepping the relevant legal boundaries. (2)

Such scholars problematize cyber-language that stirs up fear and misunderstanding in the public and challenge the computer industry to use more accurate terminology.

A Theoretical Framework

To explain and ground my ultimate findings, I draw on both modern rhetorical scholars and on long-running ethical philosophies such as utilitarianism. As an example, Herman Tavini broaches utilitarianism in the technological context, explaining, "…if Policy Y encourages the development of a certain kind of computer software, which in turn would produce more jobs and higher incomes for those living in Community X, then Policy Y would be considered more

socially useful and thus the morally correct policy" (46). According to utilitarian thinkers, moral choices should be based on each action's capacity to increase pleasure or reduce pain for the greatest number of people. In the course of this study, rhetors frequently make *Greater Good* arguments that harken back to utilitarianism.

I also look to classical rhetoric, in particular the writings of Isocrates and Aristotle and their concepts of how *ethos* is constructed. For Isocrates, ethos was closely tied to a person's ongoing moral fortitude, whereas for Aristotle, ethos was most strongly embodied within an individual artifact or speech. In *On Rhetoric*, he explains that ethotic persuasion is created "through character whenever speech is spoken in such a way as to make the speaker worthy of credence; for we believe fair-minded people to a greater extent and more quickly on all subjects…And this should result from the speech, not from a previous opinion that the speaker is a certain kind of person" (2.4 lines 40-42).

Though various scholars have compared and contrasted the two philosophers' perspectives on ethos construction (Leff, Brinton, Benoit), for the purposes of this investigation, arguing for one side of this dichotomy (whether character resides in the person or in the artifact) is not as helpful as understanding how ethos manifests itself both within individual texts and through compounding reputations. Robert Holt's concept of ethos as a "perpetual project" in the online world seems particularly apropos in the contemporary business climate where company comments and blog posts become permanent records of their activities and positions. Though he argues for a revival of the Isocratean perspective that "allows us to consider how a rhetor's previously constructed character can—and necessarily does—affect an audience's response to current and future performances" (73), it's clear that each new speech or reporter article contributes to a corporation's ongoing reputation.

Though I primarily explore ethos-building in the context of online texts, it's notable that the subjects in this study come with significant pre-existing reputations. A blending of the Isocratean and Aristotelian conceptions of ethos helps explain the defensive position that hackers and technology companies bring to this debate and how they work to rectify image problems. Ethos is a central consideration for companies that operate daily in ethical gray areas.

Based on this ancient rhetorical foundation, I also look to modern scholars such as George Cheney and Lars Thøsger Christensen to develop the concept of ethos in a corporate context. They explain that in the modern business climate, "individuals and organizations are in hot pursuit of solid, favorable identities even as such identities become harder to capture and sustain. This is especially the case in situations when issues turn into crises" (18). In my study of this contentious topic, issues management is not an isolated occurrence but a constant process for hacker companies whose business is built on controversy. Similarly, Michael Leff explains that as opposed to ad hominem attacks, "[r]hetorical ethos functions as a resource for invention. It offers possibilities for speakers to construct favorable images of themselves, unfavorable images of opponents, and to do whatever else advances their purpose through reference to persons" (304). In this study, rhetors both build their own ethos and deconstruct the ethos of opponents; this interplay creates a web of blame and praise. Lastly, Clarence Walton explains that a "firm's stature and an executive's prestige depend on money and morality, on a capacity for production and a reputation for probity" (23). Modern corporations cannot divorce their profits from their credibility and the words of their top executives from their overall ethos. Therefore, a careful exploration of company quotes and online texts can provide important clues about the ethical strategies and discursive positioning that technology companies and hackers employ, shedding light on this emergent debate.

Methodology

Based on the current status of cybersecurity discourse and corresponding scholarly work, I began this investigation with several research questions in mind. First and foremost, I wanted to discover how different rhetors (technology companies, hackers, and reporters) frame the practice of selling software "vulnerabilities" and "exploits" to third parties (in contrast to disclosing or selling this "attack code" to the affected technology companies). I selected these three groups as the hackers represent the pro-sales perspective, the technology companies are often anti-sales or the "injured party," and reporters act as referees explaining all sides of the argument. These three groups provide a helpful left-to-right view of the discourse.

Secondly, I wanted to better understand how these three groups construct notions of "right" and "wrong" in their discourses. Finally, from a comparative perspective, I wanted to ascertain whether there were dominant ethical discourses that ran across multiple groups.

In order to understand how these rhetors position their core values, I performed both qualitative and quantitative analyses of their online communications. Whereas in the medical field, the fundamental "right action" (i.e., doing everything in one's power to improve the health of a patient) may be obvious, in the online security world, the core "rights" and "wrongs" are more convoluted. To understand the ethical frameworks of this debate, I developed a corpus that encapsulated the main players in the debate and then examined their language, looking for the words, phrases, and core arguments they use to frame the moral imperatives of the community.

Grounded Theory

To structure my methodology for both qualitative and quantitative analysis, I utilized grounded theory as originally defined by Barney Glaser and Anselm Strauss in 1967 as "the discovery of theory from data—systematically obtained and analyzed in social research" (1) and

revisited by Juliet Corbin and Strauss in 1990. My approach more closely mirrored Corbin and Strauss', given my use of structured research questions and phased coding. They emphasize, "Each investigator enters the field with some questions or areas for observation, or will soon generate them, and will collect data on these throughout the research endeavor, unless these questions prove during analysis to be irrelevant" (419). Additionally, Hilary Engward provides a good summary of three most common phases of grounded theory-based coding: defining open coding as "identifying, naming, categorizing, describing phenomena," axial coding as "the process of relating codes to each other," and selective coding as "choosing a core category and relating other categories to it" (39). I cycled through each of these phases in my coding process and let the data generate my theories throughout the process, as opposed to retrofitting existing theories to a fresh data set.

Collecting the Corpus

I collected three types of texts in order to analyze the broader conversation around this topic: discourse from (1) reporters (as third-party commentators), (2) the affected technology companies, and (3) the vulnerability sellers, i.e., hackers themselves.

To understand the reporter perspective, I collected 20 articles via "criterion-based sampling," as comprehensive sampling would be beyond a manageable scope for this research (Blythe 207). The criterion included: articles that were at least 300 words long, from 20 different independent publications (not in-house publications for technology companies), posted within the past three years, and focused exclusively on the issue of selling bugs or on research companies that do this. I identified my sample articles by using the web search terms "vulnerability sales" and "selling exploits." If choosing among several applicable articles, my preference was for articles that included more in-depth evaluation or commentary on the practice

of selling vulnerabilities, rather than straightforward mentions of the hackers or the practice. These articles were written primarily by staff reporters at security outlets (e.g., *Dark Reading, Threatpost)* and technology beat reporters at broader publications (e.g., *Forbes, The New York Times),* given that this topic is too nuanced for general business and consumer beat reporters. The resulting articles (Fig. 1) were composed of primarily opinion-pieces on the practice of selling vulnerabilities and stories that centered on a specific news event in which the hacking companies were involved (like a newly discovered vulnerability that was not released to a vendor).

Date	Headline	Publication	Author	Genre
08/2014	"French Company That Sells Exploits to the NSA Sat on an Internet Explorer Vulnerability for Three Years"	*TechDirt*	Tim Cushing	Technology article
07/2014	"Zero-Day Broker Exploits Vulnerability in I2P to De-Anonymize Tails Users"	*Computerworld*	Darlene Storm	Technology article
07/2014	"Zero-Day Flaws in Tails Aren't for Sale, Vulnerability Broker Says"	*IDG*	Jeremy Kirk	Newswire
09/2013	"NSA Purchased Zero-Day Exploits from French Security Firm VUPEN"	*ZD Net*	Charlie Osborne	Technology article
08/2013	"The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities"	*Washington Post*	Brian Fung	Political article
07/2013	"Nations Buying as Hackers Sell Flaws in Computer Code"	*The New York Times*	Nicole Perlroth & David Sanger	Business article
05/2013	"Exploit Sales: The New Disclosure Debate"	*Threatpost*	Dennis Fisher	Security article
05/2013	"Special Report - U.S. Cyberwar Strategy Stokes Fear of Blowback"	*Reuters*	Joseph Menn	Newswire
05/2013	"How Spies, Hackers, and the Government Bolster a Booming Software Exploit Market"	*Fast Company*	Neal Ungerleider	Business article

03/2013	"The Digital Arms Trade"	*The Economist*	Not provided	Financial article
02/2013	"In Cyberwar, Software Flaws are a Hot Commodity"	*NPR*	Tom Gjelten	General Interest article
01/2013	"Cyberwar's Gray Market"	*Slate*	Ryan Gallagher	General interest article
11/2012	"How The Sale of Vulnerabilities Will Change in 2013"	*Dark Reading*	Not provided	Security article
11/2012	"Exploit Broker Releases EXPLICIT VIDS of Holes in Industrial Control Kit"	*The Register*	John Leyden	Technology article
11/2012	"Security Firm VUPEN Claims to Have Hacked Windows 8 and IE10"	*The Next Web*	Emil Protalinski	Technology article
10/2012	"The Shadowy World of Selling Software Bugs - and How it Makes Us All Less Safe"	*ReadWrite*	Antone Gonsalves	Technology article
10/2012	"Sell Out Hackers: The Zero-Day Exploit Market"	*TechWeek Europe*	Not provided	Technology article
06/2012	"Guess Who's Buying Zero-Day Vulnerabilities?"	*Tech Republic*	Michael Kassner	Technology article
03/2012	"Hackers Can Make $250,000 Selling iOS Exploits To The Government"	*Cult of Mac*	Alex Heath	Technology article
03/2012	"Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)"	*Forbes*	Andy Greenberg	Business article

Figure 1. Articles collected in October 2014 representing the reporter perspective on commoditized vulnerabilities.

Secondly, I examined security blog posts, disclosure policy statements, and other germane commentary written by technology companies that are affected by vulnerability sales. Though these companies are often reticent to comment on vulnerability sales directly, many have well-defined disclosure policies and/or write informal blog posts that address this topic or closely related ethical issues. For instance, in 2010 Microsoft published a public policy detailing how disclosures should be handled and asking researchers for sufficient time to fix vulnerabilities

before they are publicly disclosed ("Coordinated Vulnerability Disclosure"). To determine which technology companies to study, I focused on the top 50 companies on the Fortune 500 list. I defined technology companies as computer and internet vendors and filtered out telecommunications providers, car makers, etc. Based on these parameters, I came up with Apple, Hewlitt Packard (HP), Google, International Business Machines (IBM), Microsoft, and Amazon.

I then conducted searches within each company's security blogs and corporate policy pages for relevant content. Searches within their corporate blogs included the following terms: "broker," "sale," "selling," "disclosure," "vupen," "netragard," "revuln," "vulnerability disclosure," and "exploit sale." I found applicable content for all these companies except for Apple (unsurprising as Apple is notorious for being tight-lipped on security issues). I collected a comprehensive sample of any relevant content I could find using these search terms in the primary corporate entities (without branching out into individual security researcher blogs that don't always represent the broader company's perspective). I collected documents within two primary genres: the vulnerability disclosure policy statement and security blog posts (Fig. 2). I also collected any supplemental content that more transparently addressed the companies' perspectives (i.e., an infographic from HP on disclosure options and a video transcript from Microsoft encouraging private disclosure).

Although there was sparse direct commentary on commoditized vulnerabilities, we can infer the companies' ethical stances based on closely related topics like disclosure ethics. That is, if a company only condones hackers disclosing vulnerability information to them privately, then that company can be assumed to oppose the sale of vulnerabilities.

Company	Length of Corpus	Disclosure Policy	Security Blog Posts	Authors
IBM	2442 words	Disclosure Policy (326 words)	"Mikko Hypponen at TrustyCon: Governments as Malware Authors" (661 words) 2014 "Underground Cybercrime: Exploits for Sale" (531 words) 2014 "When Lack of Disclosure Can Kill You" (924 words) 2013	• Zubair Ashraf, Security Researcher • Dana Tamir, Director of Enterprise Security at Trusteer, an IBM Company • Diana Kelley, Executive Security Advisor
Amazon	644 words	Disclosure Policy (644 words)	N/A	N/A
HP	2787 words	Disclosure Policy (813 words)	"The Vulnerability Market Decoded" Infographic (525 words) 2014 "Deep impact - The ZDI Disclosure Policy" (1449 words) 2013	• Jewel Timpe, Research Communications Manager
Microsoft	4460 words	Disclosure Policy (454 words) Disclosure Ethics Video (545 words)	"Who Exploits Vulnerabilities: The Path from Disclosure to Mass Market Exploitation" (582 words) 2014 "Coordinated Vulnerability Disclosure: From Philosophy to Practice" (435 words) 2011 "Coordinated Vulnerability Disclosure: Bringing Balance to the Force" (1622 words) 2010 "Community-Based Defense: Looking Outward, Moving Forward" (822 words) 2010	• Tim Rains, Director, Trustworthy Computing (TwC) • Matt Thomlinson, General Manager, TwC • Katie Moussouris, Senior Security Strategist Lead, TwC • Dave Forstrom, Director, TwC
Google	5173 words	Disclosure Policy (384 words) Vulnerability Rewards Policy (1747 words)	"Disclosure Timeline for Vulnerabilities Under Active Attack" (361 words) 2013 "Quick Update on Our Vulnerability Reward Program" (1313) 2010 "Rebooting Responsible Disclosure: A Focus on Protecting End Users" (995 words) 2010 "Improving Web Browser Security" (373 words) 2009	• Chris Evans, Eric Grosse, Neel Mehta, Matt Moore, Tavis Ormandy, Julien Tinnes, Drew Hintz, Michal Zalewski (Google Security Team)
Apple	N/A	N/A	N/A	N/A

Figure 2. Technology company blog posts, policies, and other relevant artifacts; collected between October and November 2014. Authors refer to blog posts, disclosure policies are unattributed.

To study the hacker perspective, I compiled commentary from two prominent vulnerability vendors: VUPEN and Netragard. Both advertise on their websites that they specialize in "offensive" and "defensive" security techniques and both have been mentioned in news coverage on this topic. Focusing on these two entities provided a sample of the hacker perspective from two prominent, and sometimes opposing, vulnerability seller perspectives. Of note, it's impractical to study the buyer-side of these transaction, as these entities are often kept anonymous, not wishing to disclose that they buy exploits. For example, by parsing through Freedom of Information Act documents, the media learned that the National Security Agency (NSA) subscribed to VUPEN in 2012 (Franceschi-Bicchierai). I focused exclusively on the seller side for the hacker perspective.

First off, VUPEN is a French security research company that was founded in 2004 and calls itself "the leading provider of defensive and offensive cybersecurity intelligence and advanced vulnerability research" ("About VUPEN Security"). The word "offensive" in this statement is emblematic of the overall tension surrounding this company (i.e., its goal is not just to develop tools to improve a company's defenses against external hackers, but to allow those entities to potentially hack others). In VUPEN's case, it was particularly useful to collect commentary from its CEO Chaoki Bekrar because he is an outspoken defender of the practice of selling vulnerabilities in the news and on social media. As an example, Andy Greenberg of *Forbes* interviewed Bekrar following an annual hacking competition called Pwn2Own that tasks researchers with breaking into specific browsers and operating systems for cash prizes. Greenberg quoted Bekrar emphasizing that he would not share the Chrome vulnerability VUPEN found with Google for "chump change," i.e., Google's $60,000 offer. Such statements fly in the face of industry expectations, making Bekrar and his company an interesting ethical case study.

Netragard is a U.S. based security company that was founded by Adriel Desautels in 1998. It offers a broad array of security services couched as "anti-hacking" as well as a less publicized wing called the "Exploit Acquisition Program." Though vulnerability sales are noticeably downplayed on the company's website, it does state that the EAP "augment[s] Netragard's advanced service offerings…to satisfy specific and unique client requirements" and that the public can rest assured that exploits "will only be provided to vetted U.S. buyers who have a legitimate need for such technology." This is in contrast to VUPEN, which sells vulnerabilities internationally instead of only domestically in France.

The hacker corpus included text from the two companies' websites explaining their business models in their own words (e.g., "About Us" and pages delineating their "offensive" security offerings), as well as ten blog posts for each company that either alluded to or overtly discussed their vulnerability sales or demonstrated how the companies position themselves within the security field. For Netragard, I collected ten blog posts out of a total of 81 possible posts since January 2007 (as of October 15, 2014). I gave first preference to blog posts that directly discuss the company's vulnerability sales model. There were three explicit pieces on this topic. The remaining selected posts focused on positioning the company against other security vendors, elevating its own ethos, and attempting to convince potential customers that other hackers-for-hire are less ethical or advanced in their methods. For VUPEN, collecting blog posts was more difficult as the company doesn't overtly discuss its vulnerability sales in this venue. Rather it writes infrequently about specific exploits it has developed. Accordingly, I selected 10 of these blog posts (out of 16 total as of October 15, 2014). I gave preference in selection to blog posts that included more editorialized content—framing and explaining exploits and VUPEN's relationship to other hackers and companies.

To further investigate VUPEN's perspective, I transcribed an online podcast with Ryan Naraine of *SecurityWeek* interviewing Bekrar. As this artifact includes his own words in defense of his business model, it is helpful supplemental content.

Company	Length of Corpus	Corporate Documents	Security Blog Posts	Authors
VUPEN	20,000+ Words (including code demos) 2,800 words (without code demos)	"About VUPEN" "About Vulnerability Research Team" Video Demo: "Google Chrome Pwned by VUPEN aka Sandbox/ ASLR/DEP Bypass" *SecurityWeek* Podcast with CEO	• "Advanced Exploitation of VirtualBox 3D Acceleration VM Escape Vulnerability (CVE-2014-0983)" • "Advanced Exploitation of Windows Kernel Privilege Escalation (CVE-2013-3660 / MS13-053)" • "Advanced Exploitation of Mozilla Firefox Use-After-Free Vulnerability (Pwn2Own 2014)" • "Advanced Exploitation of Internet Explorer 10 / Windows 8 Overflow (Pwn2Own 2013)" • "Advanced Exploitation of IE MSXML Remote Uninitialized Memory (MS12-043 / CVE-2012-1889)" • "Advanced Exploitation of Internet Explorer Heap Overflow Vulnerabilities (MS12-004)" • "Technical Analysis and Advanced Exploitation of Adobe Flash 0-Day (CVE-2011-0609)" • "Technical Analysis of Exim "string_vformat()" Buffer Overflow Vulnerability" • "Technical Analysis of the Windows Win32K.sys Keyboard Layout Stuxnet Exploit" • "Criminals Are Getting Smarter: Analysis of the Adobe Acrobat / Reader 0-Day Exploit"	Security Researchers: • Florian Ledoux • Jordan Gruskovnjak • Arno • Nicholas Joly • Matthieu Bonetti • Sebastien Renaud
Netragard	8792 Words	"About Us" "Exploit Acquisition Program"	• "Netragard on Exploit Brokering" • "Selling Zero-Day's Doesn't Increase Your Risk, Here's Why" • "Exploit Acquisition Program – More Details" • "How to Find a Genuine Penetration Testing Firm" • "Netragard's Badge of Honor (Thank you McAfee)"	Adriel Desautels, CEO (only listed author on blog posts)

			• "Fradulent Security Experts" • "Finding the Quality Security Vendor (Penetration Testing, Vulnerability Assessments, Web Application Security, etc)" • "Professional Script Kiddies vs. Real Talent" • "Verify Your Security Provider — The Truth Behind Manual Testing" • "Whistleblower Series – Don't be Naive, Take the Time to Read and Understand the Proposal"s	

Figure 3. Hacker corpora including blog posts, website positioning, and other relevant artifacts.

Coding the Corpus

Once I collected the texts for the three corpora, I saved each example article, blog post, and policy as a plain text file and stripped out author names, dates, and any other metadata that was irrelevant to the ethical arguments the various rhetors advance. Before beginning the process of coding, I uploaded the files into Voyant Tools, a basic text analytics program, to look for word frequency trends. Looking at each corpus at the word level helped me speculate about potential argumentative structures for the different groups, as well as track interesting terminology as I began my qualitative analysis.

After looking at simple word frequency trends, I did a preliminary read-through of the corpora, taking notes on possible categories that would emerge. This step gave me clues as to possible coding structures before beginning the formal coding process. I then uploaded the files into Dedoose, a web-based qualitative data analysis tool. Upon uploading the files, I practiced open coding—systematically reading each article and assigning codes to the ethical arguments I saw, adding codes as I went. As this was a previously unexplored ethical debate, it was important to approach the data without preconceived assumptions or theories in place. As Glaser and Strauss argue, "[E]mergent categories usually prove to be the most relevant and the best fitted to

the data. As they are emerging, their fullest possible generality and meaning are continually being developed and checked for relevance" (37). Following this principle, I added a new code each time the text revealed an instance of a unique ethical argument. Units of analysis varied from words, to phrases, to whole paragraphs. Instead of focusing on the size of the unit, I captured every iteration of an ethical argument about vulnerability disclosure and exploit sales. I also recorded memos (Corbin and Strauss 422) to myself in Dedoose to keep track of my thoughts and impressions as I coded.

As I recorded more codes, I periodically returned to a previous article or blog post to add or merge codes, practicing an "iterative, back-and-forth style" (Johnson 5) or reflexive axial coding, the second phase of grounded theory code analysis. An essential principle of this theory is not being married to the first codes one creates; as Corbin and Strauss state, "No matter how enamored the investigator may be of a particular concept, if it does not stand up to continued scrutiny through its repeated proven relevance to the phenomenon under question, it must be discarded" (420). In this study, I noticed that reporters were often citing the Stuxnet security incident (in which the United States and Israel reportedly used a vulnerability in Windows to break into an Iranian nuclear facility). Though at first I wasn't recording every specific exploit incident that the reporters mentioned, I began to realize that reporters were using this infamous incident to demonstrate the possible nation-state or critical infrastructure implications of the exploit trade. Consequently, I returned to the corpus and added a code for each time Stuxnet was mentioned. Lastly, I used selective coding to identify the most prevalent and significant coding categories in order to draw my conclusions.

In the reporter corpus, one challenge I faced in coding the articles was how the unique journalistic stance affects coding. Reporters typically do not write an entire piece from their

perspective, rather they assemble quotes from various other parties in an attempt to present multiple sides of the same story. Given the complexity of their articles, within this corpus I coded the text by rhetor group instead of attributing every comment back to the reporters themselves. I assigned parent codes to any third-party, hacker, or technology company that was quoted. I also used a *Reporter Point of View* code to categorize instances when the reporter either expressed a direct ethical stance, implied his or her view, or made an interesting rhetorical move to influence the reader's perspective. As a result, I typically assigned at least two codes for each excerpt: one indicating the particular party or parties making the argument and one that attempted to capture the specific ethical argument(s) he or she made.

Whereas the reporter corpus was largely homogeneous (20 similar news articles), making it a more natural fit for quantitative analysis, there was a lot of variability in the company corpus as far as the frequency and style of communication on vulnerability topics. Therefore, in my results, I address each company individually and more qualitatively. I still used Dedoose to identify primary trends and codes for each company, but the distinctiveness of each company's discourse prevented me from making apples-to-apples comparisons across the whole corpus. This is especially true because there are two primary genres in which the companies talk about vulnerability ethics: security blog posts and vulnerability disclosure policy statements.

Lastly, in order to code the hacker corpus, I broke it into two subsets: one for Netragard and one for VUPEN. Like the company corpus, I was more interested in the individual companies' rhetoric than the sum of their codes. It was particularly important to look at Netragard and VUPEN separately because they frequently disagree and position themselves as ethically or technically superior to each other. Using Dedoose to look at trends within each hacker company and then comparing them proved to be the most useful method of analysis.

Chapter 2: Results

In this chapter, I document the primary ethical arguments and supporting tactics that emerged in the two halves of my analysis, first in the world-level analysis I performed using text analysis software and secondly, by conducting a line-by-line qualitative analysis of the rhetorical frameworks of the debate.

Word-Level Trends

My quantitative analysis of the reporter corpus reinforced the word-level trends I expected, but also revealed a few more intriguing patterns. Top words (after the removal of prepositions and articles) included: exploits (163), vulnerabilities (124), software (114), zero-day (80), hackers (68), sell (67), and information (53). More noteworthy word trends I noticed included the prevalence of "government" (77) as the reporters focus on who is buying the exploits, and "VUPEN" (97), mentioned so frequently due to the polarizing and public nature of the firm's views. By comparison, journalists only mentioned Netragard 14 times, Google 36 times, and Microsoft 35 times. These figures provide clues as to the most vocal and notorious players and show the technology companies' relative reticence to enter into the debate. Though these companies proactively discuss disclosure ethics, they are less likely to directly engage in exploit sales discourse.

In the company corpus, the top words included: vulnerability/ies (274), security (152), disclosure (114), vendors (65), and software (60). Of note, we can see a subtle difference in the focal point between reporters and technology companies. Whereas the companies are more concerned with vulnerabilities or weak spots in their own software (274), the reporters are more intrigued by the exploitation (163) of these vulnerabilities. Similarly, reporters mention "zero-

days"[2] more frequently, showing a more incident-based focus. The company blog posts and policies react less to specific exploits and instead attempt to set ongoing precedents for ethical hacking behaviors.

Also worth noting, at a relatively high frequency in the company corpus was the word "researchers" (46). Technology companies, in their quest for political correctness, will typically refer to ethical hackers as "researchers" and those performing outside of societal norms as "criminals" or "attackers." "Hackers" did not make the most frequent words lists for companies like it did for reporters (68). Assumedly, this is because the companies make every effort to endear hackers to their cause in their materials, so the term "security researcher" can be seen as legitimizing certain types of hacking practices.

Finally in the company corpus, there was the frequency of the word "responsible" (41), referencing the industry standard of private disclosure often called "responsible disclosure."[3] Throughout the company disclosure policy statements and the security blog posts I collected, vendors react to or support this industry standard with high frequency. Whereas some vendors like IBM espouse the standard unquestioningly, others like Google reinforce it with recommended modifications.

As the hacker corpus was composed of two robust and often conflicting perspectives, versus a more homogeneous corpus like the reporters, I examined Netragard and VUPEN separately. Within the Netragard corpus, the most common words were "exploit" (68), "testing" (64), "security" (63), "penetration" (58), and "vulnerability" (46). Exploit was mentioned most commonly in the context of the company's "Exploit Acquisition Program" as well as the

[2] Zero-day refers to a previously unknown vulnerability that has been public disclosed. Therefore the affected technology company has *zero days* to prepare mitigations or patches before hackers are aware of the flaw.
[3] Any time where I discuss the "responsible disclosure" policy, I will instead use the phrase "private disclosure" to avoid adopting the loaded industry vernacular.

company's explanation of its "exploit brokering" practices. Netragard seems to be using these official terms to normalize its business operations. Other words that come up in Netragard's corpus include "vendors" (44) and "quality" (28). The emphasis on vendors exhibits the company's frequent positioning of itself in partnership with or against software companies. In some instances, Netragard applauds certain vendors for building security measures into their software development process; in others, the company blames vendors for the insecurity of their products. "Quality" was often paired with "testing" and "penetration," as much of Netragard's corpus talks about the company's thorough and sophisticated vulnerability discovery and exploit development methods. This evaluative language often appears in the context of questioning the merit of other security researchers. The quality argument helps the company build its ethos in an environment that is often antagonistic toward vulnerability sellers.

From a basic word count perspective, VUPEN's corpus was more complicated to analyze. This difficulty arose because the company's blog posts were nearly 90 percent code demonstrations for particular exploits (17,200 words devoted to demos). As a result, VUPEN's top word results, when looking at the whole corpus include such words as "text" (515), "eax" (371), and "mov" (293). As Voyant cannot distinguish between editorial content and lines of code, I decided to do a word-level analysis on just the company's more overt website positioning and a podcast transcript in which the company's CEO defends its business model.

After making these adjustments, VUPEN's top words were: "Exploit/s" (49), "vulnerability/ies" (40), "research" (25), and "security" (23). Of perhaps greater interest were words that appeared less frequently but reveal more about the company's rhetoric. The word "customers" (14) was an important indicator, demonstrating VUPEN's frequent positioning of its services as protecting or serving customers. "Offensive" (13) appeared in corporate positioning

statements such as: “VUPEN’s offensive IT intrusion solutions and government grade exploits enable government agencies and the Intelligence community to achieve their *offensive* cyber missions and critical network operations using VUPEN’s industry-recognized vulnerability research.” Offensive is the lightening rod word for this debate, and this word count shows VUPEN’s transparent acknowledgement of its controversial model. Unlike Netragard, it doesn’t downplay its exploit development practices.

In comparison to the technology company corpus, for the hackers, disclosure is a non-issue. Netragard and VUPEN are most concerned with justifying their practices to the broader security and IT community, not debating the finer points of private disclosure. These companies know that they are not following private disclosure, so instead of trying to convince others that they are, they place blame on fear-mongers and on software companies that build insecure software. From a word-level perspective, we can also see evidence of the hackers reinforcing the idea that their work benefits their customers and is sophisticated and high-quality in nature. VUPEN consistently emphasizes that its work is “advanced,” “world-class,” and “industry-recognized.” The company is not hesitant to gloat.

Reporter Corpus Analysis

Moving into qualitative analysis, I first analyzed the reporter corpus. The first finding was that they frequently shatter the guise of journalistic objectivity by expressing their perspectives on vulnerability selling. I assigned the *Reporter POV* code 125 times—including directly expressed opinions and more implicit ethical stances. For instance, they often include statistics or historical examples that would lead readers to view an exploit transaction as unethical. References to Stuxnet were the most common rhetorical tactic that suggested an ethical bias. By comparing vulnerability sales transactions with one of the most notorious

successful exploits in history—governments using the Stuxnet malware to interfere with the operations of a nuclear facility—the reporters imply that if left unchecked, the exploits that VUPEN and Netragard are selling could have major destructive potential. Though this is the exception and not the rule with exploits, by drawing attention to the extreme, reporters attempt to alarm readers. As an example, *TechWeek Europe* asserts, "Now they have seen the damage cyber tools can do, from Stuxnet to the super-sophisticated spy tool Flame, governments know what is at stake." The reporters frequently elevate the cybersecurity stakes to the level of nation-state nuclear conflict.

By and large, the coding process revealed that reporters are generally against the practice of vulnerability sales. This was evident both in the co-occurrence of the reporter code with resistive ethical positions and, more subtly, in the types of perspectives they chose to include. The hackers themselves were quoted 33 times in the corpus, whereas third-parties (e.g., privacy advocates, anti-virus software company representatives, prominent security experts) who typically disagree with commoditizing vulnerabilities were quoted 56 times. In particular, Chris Soghoian of the ACLU was a prevalent protester included in coverage (14 instances), presumably because his sound bites are polemic and one-sided—excellent fodder for controversy. For example, *Forbes* reporter Andy Greenberg juxtaposes Soghoian's perspective with VUPEN's: whereas Bekrar describes his company's practices as "transparent," Soghoian's characterizes them as "shameless" and calls VUPEN "the Jersey Shore of the exploit trade." In this article, he accuses VUPEN of being a publicity hound that seeks fame instead of doing what's right. Another example of Soghoian's ethical presence in the news cycle was his quote in *Slate* where he calls VUPEN "modern-day merchants of death" selling "the bullets for

cyberwar." In these quotes, reporters relay ethical arguments that compare exploit selling to physical war conflicts and accuse companies like VUPEN of shameful business practices.

Under the broader parent codes, I identified 22 ethical argument codes within the corpus. I will now enumerate and explicate the five most significant arguments upon which the reporters build their case: (1) *Money or Morality* (53 instances), (2) *Falling into the Wrong Hands* (24), (3) *War and Weaponry* (26 instances), (4) *Greater Good* (26 instances), and (5) *Shady and Secretive* (21).

Money or Morality

When looking at the *Reporter Point of View* pairings with these ethical positions, I found that the lucrative code or *Money or Morality* was the most prevalent at 45 co-occurrences. These instances appeared in 16 out of 20 articles, so this theme cannot be attributed to a single long article focusing on the lucrative nature of the trade; rather, reporters consistently focus on the growing market for vulnerabilities and the high sums of money a single exploit can command from a government buyer. Third-party perspectives also mirror this fixation on the sticker shock of exploits. Along these lines, Bruce Schneier, an independent security guru, is quoted in *TechRepublic* calling the market for commoditized vulnerabilities "dangerous" and very "lucrative." He argues that selling vulnerabilities keeps them unpatched and undisclosed in the long-term. He then speculates that as a result of this growing market, in-house technology developers may actually intentionally create flaws in their software in order to make money by selling them later; however, this conspiratorial point of view only appeared in two other articles, showing that most reporters don't subscribe to the idea that technology companies could be purposely building flaws into their own software.

The *TechRepublic* reporter then editorializes, "For once, I'm hoping Bruce Schneier is wrong. But, I doubt it. I've already read where high-level contestants who normally compete in Pwn2Own aren't any more. They would rather keep what they found secret, and make the big bucks." In such perspectives, we see that reporters are arguing for a moral choice, either implying or directly stating that hackers would rather make money than do what's in the best interest of broader internet users. Their continual focus on the lucrative nature of the market frames the ethics as a binary choice—money or morality—and they believe that the hacker companies choose incorrectly.

Emil Protalinski of *ReadWrite* make a comparable case for hackers choosing cash over morality, writing:

> It turns out government agencies are willing to pay six figures for exclusive details on exploitable flaws in software and operating systems, and there are plenty of companies and bug brokers ready to sell to the highest bidder. But with so much backdoor trading, who is watching to make sure the bad guys—from criminals to terrorists or hostile nations—do not get this valuable information? The answer is no one.

Here Protalinski ties the market to inherent risk, framing exploit sales as "backdoor trading" and arguing that it can lead to "bad guys" getting access to the security holes. Of particular interest is his mention of "criminals to terrorists or hostile nations." He defines who these bad guys are and implies that not disclosing vulnerabilities to technology companies gives them greater access to tools to do evil. This leaves the reader with a question: would any moral person really want to give cybersecurity secrets to terrorists? From this point of view, VUPEN and Netragard may be unintentionally aiding the likes of Al-Qaida or ISIS. This either/or choice of morality or money is presented in coverage constantly.

Falling into the Wrong Hands

The second significant ethical argument I'd like to explore is the ominous idea of exploits *Falling into the Wrong Hands*, also present in the Protalinski quote. In this case, morality is framed based on the trustworthiness of the receiver of the exploits. This position assumes that it's ethically acceptable to create an exploit, but moral ambiguity arises when these exploits are transmitted either to unknown parties or to known repressive regimes and terrorist groups. *Reuters* ties the *Wrong Hands* argument back to an incident with U.S.-developed malware named Duqu. Like the Stuxnet mentions, the reporter uses a past incident as a predictor of what could happen with commoditized vulnerabilities. In the case of Duqu, reportedly the malware was designed to steal information about industrial facility designs in Iran, but hackers copied its code and subsequently used it on the broader public. *Reuters* includes data from the security firm F-Secure showing that, as a result of the malicious code leaking, Duqu was used in 16 out of every 1,000 attacks on U.S. computers that year.

For many of the reporters in this sample, their ethical concern is not so much that the vulnerabilities are being sold, but to whom they are being sold. Again, such reasoning fears unknown actors and motivations. *Slate* captures this sentiment posting, "[B]ecause sales are unregulated, there are concerns that some gray market companies are supplying to rogue foreign regimes that may use exploits as part of malicious targeted attacks against other countries or opponents. There is also an anarchic black market that exists on invite-only Web forums, where exploits are sold to a variety of actors—often for criminal purposes." Some reporters use this fear of the unknown to argue for regulation of the vulnerability market.

Under the same *Wrong Hands* code, I captured the related idea of *Wrong Motives*. Reporters are not just concerned with who would have these vulnerabilities, but about how they

would be used. For instance, *Threatpost's* Dennis Fisher asserts that many governments can't be trusted with advanced malware capabilities. He argues that they may attack other countries or spy on their citizens and that the vulnerabilities are also being bought by government contractors "for their own uses." Spying was a frequent concern of reporters—that repressive governments would use such exploits to spy on and then persecute their own citizens as well as to spy on other governments.

War and Weaponry

Thirdly, to further their case against vulnerability and exploit sales, reporters frequently use analogies that equate such practices to arms dealing and war tactics. The corresponding code aligned with the reporter perspective 19 times in the corpus. However, in contrast to the prevalent *Money or Morality* argument, many of the *War and Weaponry* instances were concentrated in five main articles. This finding indicates that some reporters buy into the idea of cyberwar more wholeheartedly than others in this debate. To establish the war analogy in their coverage, reporters and the third-parties they quote often compare exploits to guns or talk about them being "weaponized." After establishing the metaphor alongside the facts of the exploit trade, they use it to suggest ethical implications of the sales. For instance, *Slate* includes a quote from Robert Graham of Errata Security asking, "If we're going to have a military to defend ourselves, why would you disarm our military? If the government can't buy exploits on the open market, they will just develop them themselves." This is a case of a third-party defending the sale of exploits by appropriating the war analogy; yet, in the same breath, Graham contradicts the metaphor upon which his premise is built, saying, "Plus, digital arms don't exist—it's an analogy. They don't kill people." In this, we see an awareness of the inflammatory nature of the language and a desire to qualify his suggestion.

Another interesting instance of this code was a section in *TechWeek Europe* where the staff reporter takes creative liberties with the war metaphor and compares vulnerability exploitation to the *Star Wars* scene where the rebel force finds a defect in the Death Star. The reporter jokes, "Remember how Luke Skywalker slotted a bomb from his X-Wing down the Death Star's exhaust port to blow the spherical space-station apart? Well that port is much like a zero-day vulnerability, and the rebel force's attack was a carefully constructed zero-day exploit." The reporter also includes a picture of toy soldiers crawling over a computer keyboard (Fig. 4) and a keyboard with a lit fuse. Clearly, such articles employ both visual and verbal rhetoric to reinforce the idea of the hacking world as an ongoing war. With the prevalence of terms like "attack," "cyberwar," and "vulnerability" in the cybersecurity world, it's no wonder that reporters draw the connection between exploits and digital arms.

Figure 4. Toy soldiers crawling over keyboard as a demonstration of war analogies in coverage. Source: TechWeek Europe. "Sell Out Hackers: The Zero-Day Exploit Market." October 2012.

Greater Good

Next, there was the *Greater Good* argument, which aligned with the *Reporter Point of View* 18 times. The *Greater Good* argument appeared in 15 articles, making it more prevalent across the corpus than the war analogy. It's also important to note that this was one of the only

argumentative threads that appeared throughout all three corpora. It represents underlying logic that is a foundation for many of the other rhetorical strategies and tactics in this debate.

This notion of protecting the *Greater Good* proved to be a primary motivation why reporters are against selling vulnerabilities—the idea that doing so means that the average computer user is left open to unpatched vulnerabilities, and at times, fully developed exploits in the hands of oppressive governments and terrorists. An example of the rhetoric of *Greater Good* appears in *Dark Reading.* The article notes that despite market forces that incentivize exploit selling, "there's still room in the world for researchers willing to make a smaller amount of cash while helping *the public good* through responsible disclosure to vendors" (emphasis mine). Here we also see an association between perceived public good and the industry standard of private disclosure.

Altogether, the responsible disclosure code co-occurred more often than any other code with the *Greater Good* argument (a total of eight times). The *Dark Reading* article further reinforces this perspective by quoting a technology company representative, Brian Gorenc, manager of TippingPoint DVLabs at HP. He argues that "there's always room for the people operating in the white market. Not everybody's a bad guy. Not everybody's weaponizing and using the vulnerabilities for evil. There's always going be people out there who want to do that research, want to be compensated well for that research and get the bugs fixed and improve the overall security posture of the industry." Here Gorenc paints the vulnerability market in terms of moral imperatives, using the common hacker black and white hat terminology. In this case, the moral imperative is fixing the core vulnerabilities in order to protect end users, and in his rhetorical frame, this is how one becomes a good guy.

Another example of this link between the private disclosure argument and reducing risk to end users arose out of an incident with another vulnerability seller, Exodus Intelligence. In this case, the vendor announced that it would disclose a particular vulnerability directly to the affected company, Tails. Darlene Storm of *ComputerWorld* explains that despite Exodus Intelligence's core business model, the company's CEO, Aaron Portnoy announced that he would help Tails fix the vulnerabilities. But she also adds her perspective that "it's not quite clear if the vulnerability broker's decision was for *the greater good* or due to backlash from the security community" (emphasis mine). Again, vendor disclosure is held up as a standard of positive behavior and linked with reducing risk to average computer users. Likewise, *The New York Times* quoted Howard Schmidt, a former White House cybersecurity coordinator, emphasizing that the tradeoff of governments buying exploits is that "we all fundamentally become less secure." Such arguments juxtapose individual or governmental gain against collective risk. The protection of the many is espoused over the hackers' desires.

Shady and Secretive

Returning to the other code that was linked to *Reporter Point of View* 18 times, they often used words like "shady," "secretive," "shadowy," "opaque," or "black" to describe the exploit trade. Whereas I applied other codes at the instance level, which could include phrases, sentences, or paragraphs, this trend I marked at the word level. Reporters' consistent use of terms that indicate that the exploit market is dark imply their moral disapproval. Even though selling exploits is currently legal, such words make a subtle argument for outlawing the practice. Antone Gonsalves of *ReadWrite* even titled his article "The Shadowy World of Selling Software Bugs—And How It Makes Us All Less Safe" and goes on to emphasize this point with a fictional secretive exchange where an exploit broker whispers, "Pssst, wanna buy some software bugs?"

Comparably, *The Washington Post* focused on the NSA's interactions with vulnerability sellers, commenting, "But the NSA is also reaching into the Web's *shadier* crevices to procure bugs the big software vendors don't even know about—vulnerabilities that are known as 'zero-days'" (emphasis mine). Reporters frequently position the market as clandestine, and in so doing, delegitimize its practices and players. This being said, there is a real layer of secrecy that exists in the market beyond the discourse. Vulnerability sellers are typically discreet about their customers and techniques. As their income is based on brokering exclusive intellectual capital, they are not motivated to disclose their exploits to the public, lest the exploits lose value to their customers. In addition, many vulnerability buyers demand strict confidentiality. The U.S. government, for example, doesn't want the public to know if it is using something like Stuxnet against Iran—such information leaks could alert enemies to U.S. military plans or cause public uproar. Hence, reporters' framing of the market in murky terms is to be expected.

Hacker Perspective in Coverage

Outside of chronicling the reporters' perspectives, it's also important to discuss the appearance of the other two rhetor sides within coverage. Altogether, the hacker company perspective was included in some form in 16 out of the 20 articles, usually as a balancing point after the reporters make arguments against vulnerability selling or as "color" for the story if a hacker (usually VUPEN) says something controversial. Out of the 33 total hacker code instances, the most frequent co-occurrence was with the *We Only Sell To* code, at 11 instances. This code picks up instances of hackers arguing that their business practices are justified because they only sell to certain entities. In VUPEN's case, these entities are NATO governments and partners; quotes from Bekrar emphasize the company's internal screening process to ensure it only sells to democratic nations. This argument, of course, assumes that "democratic nations" equal good

guys. It is not concerned with what those governments do with the exploits, just in the ethos of the governments. This philosophy caused a staff writer at *Dark Reading* to joke that VUPEN only sells exploits to "what it deems the more cuddly variety of nation states." Similarly, ReVuln is quoted in *The Register* insisting that it only sells to "customers from reputable countries."

Another provision of the *We Only Sell To* argument is that these cuddly nation states shouldn't be on someone's naughty list. For example, *Threatpost's* Fisher clarifies that VUPEN does not sell exploits to countries under U.S. or E.U. embargos. Ryan Gallagher of *Slate* then complicates the simple equation of good guys to NATO. He assigns real names to the 60 countries that are members or partners of NATO to show that they aren't all unquestionably virtuous from a Western perspective; i.e., Iran, North Korea, and Zimbabwe may be off of Bekrar's list, but in theory, the company may still be selling to "the likes of Kazakhstan, Bahrain, Morocco, and Russia." By calling out these countries, reporters once again cast doubt on VUPEN's business model. This said, Gallagher balances his perspective by noting that VUPEN doesn't automatically work with a country just because it lacks sanctions.

In comparison, Netragard got off easier in coverage as reporters mention the company less frequently and don't openly criticize it. For instance, *The Economist* cites Netragard's argument that it carefully vets the hackers from whom it buys exploits behind the scenes, ensuring they are not also selling to criminal groups. Likewise, *Fast Company* notes that Netragard only sells to "vetted U.S. based buyers who have a legitimate need for such technology." It's worth noting that reporters and hackers are vague about what constitutes a "legitimate need," but overall, they seem to be more comfortable with the idea of inner-U.S. transactions.

As far as hacker arguments in direct favor versus defense of their businesses, Bekrar makes the argument that his company is doing good by helping its customers achieve their missions. He is quoted in *Reuters* asserting that "[e]xploits are used as part of lawful intercept missions and homeland security operations as legally authorized by law…to protect lives and democracies against both cyber and real world threats." Bekrar rejects the idea that his company is inherently doing something wrong and paints a picture of protection.

Vendors Don't Pay Enough

An interesting divergence in coverage from labeling actions as simply good or evil was the more pragmatic stance that the hackers took, making the argument, *Vendors Don't Pay Enough.* This code appeared seven times in the reporter corpus, three of which were the same quote: Bekrar insisting that VUPEN wouldn't provide Google with a vulnerability for its $60,000 bug bounty offer. This quote was picked up multiple times due to Bekrar's assertion that such a bounty is "chump change." As part of this ethical argument, the hackers contend that they can't pay their bills based on a tip of the hat from a technology company or a relatively small "bug bounty." Along these lines, *The New York Times* quotes ReVuln's founder, Luigi Auriemma, saying that "Providing professional work for free to a vendor is unethical. Providing professional work almost for free to security companies that make their business with your research is even more unethical." *The New York Times* reporter remarks that Auriemma's argument felt more like union organizer lobbying for its members' rights. Here, we see a reversal of the ethical argument and hackers insisting that *they* are not the ones being unethical, rather it is the software companies who don't pay outside researchers enough to incentivize them to hand over the vulnerabilities. A ReVuln spokesperson is also quoted in *The Register* attacking the software companies' reputations, saying that many of the companies not only don't pay enough, but they

also don't express gratitude. In such arguments, we see the issue reduced to a simple case of supply and demand in which the hackers argue that if the software companies really want cooperation, they need to pay bigger bounties.

Likewise, hackers transfer blame back to the software companies by asserting that technology creators should build more secure software in the first place. A tweet from Charlie Miller, a famous bug finder, was picked up in *TechWeek Europe*. Miller stresses that "Exploits aren't the problem, vulnerable programs are" and adds, "Let's make our devices unbreakable and end the discussion." Comments like these help the hackers distract readers from the core issue of the morality of selling vulnerabilities. However, perfectly secure software, though ideal, is not a likely reality in the near future.

War and Weaponry

A final interesting argument that surfaced in the reporter corpus as associated with the hacker perspective, was Netragard's direct engagement with the rhetoric of cyberwar. In an excerpt in *Slate*, the company's CEO Adriel Desautels adopts the weapon analogy as a reason why firms like VUPEN should not be allowed to sell their exploits to a variety of countries. He accuses the firm of being "greedy and irresponsible" and suggests, "If I take a gun and ship it overseas to some guy in the Middle East and he uses it to go after American troops—it's the same concept." Conversely, in a podcast with Ryan Naraine of *SecurityWeek*, VUPEN's Bekrar asserts that exploits cannot be used to kill or torture people. He instead defers the blame to the oppressive governments that perpetrate such violence. In this way, we see Netragard emphasizing the risk of zero-days to position themselves as virtuous arms dealers who only sell to U.S. buyers, whereas VUPEN denies responsibility for any potential harm caused by their exploits. This jockeying for moral high ground shows careful attention to the two companies'

moral and competitive positioning, and a recognition of the ethical precariousness of their business models.

Technology Companies in Coverage

It was also important to look at the technology company perspective in coverage. Overall, it is only lightly represented in the reporter corpus, either because the companies affected decline to comment or because reporters do not ask them as frequently how they feel about this ethical gray area. It's likely that the companies are intentionally avoiding ethical debates that distract from their core products and services. Altogether, in this corpus there were eight instances of company comments included.

The most common code associated with the company perspective in coverage was *Responsible Disclosure is Best.* For example, in *The Next Web*, a Microsoft spokesperson is quoted saying, "We continue to encourage researchers to participate in Microsoft's Coordinated Vulnerability Disclosure program to help ensure our customers' protection." Coordinated Vulnerability Disclosure (CVD) is Microsoft's specific disclosure policy, a modification of the classic private disclosure model in which researchers are expected to disclose any vulnerability findings directly to vendors so that they can fix them (without public disclosure while the flaws are addressed). Microsoft's CVD requires that:

> …finders disclose newly discovered vulnerabilities in hardware, software, and services directly to the vendors of the affected product; to a national CERT or other coordinator who will report to the vendor privately…The finder allows the vendor the opportunity to diagnose and offer fully tested updates, workarounds, or other corrective measures before any party discloses detailed vulnerability or exploit information to the public…If attacks are underway in the wild, and the vendor is still working on the update, then both the

finder and vendor work together as closely as possible to provide early public vulnerability disclosure to protect customers. ("Coordinated Vulnerability Disclosure")

So when Microsoft reinforces its policy in a reporter statement, it is condemning other courses of action such as public disclosure or sale of vulnerabilities to third parties.

Similarly, *Dark Reading* reported that following the Pwn2Own hacking competition, VUPEN refused to provide Google with the vulnerability information for a Chrome flaw. Then Google pulled its sponsorship of the HP event, showing a clear ethical stance on required disclosure. Likewise, *Forbes* captures an incident in which VUPEN released a video showing an active exploit in Chrome without providing assistance to Google to address it. Google shifted the blame by asserting that VUPEN's exploit really targeted Adobe Flash plug-ins instead of its browser. Then on Twitter, Bekrar accused Google of being "pathetic" and downplaying the vulnerability in its products, to which Google responded that Bekrar is an "ethically challenged opportunist." This is an interesting exchange because out of all the tech companies, Google is the most likely to do a little mudslinging (as compared to companies like Apple, Microsoft, and Cisco), and VUPEN is more likely to do the same (as compared to other hacking companies like Netragard). Thus, these two more feisty companies have been prone to public squabbles in recent years, despite technology companies' general hesitance to ostensibly participate in this debate outside of reinforcing disclosure ethics. Though Google may be willing to support the public hacking of its products in the name of making them more secure, if the flaws are not eventually reported back, it believes that a moral line has been crossed.

Company Corpus Analysis

By and large, my examination of software company discourse reveals that they are mostly silent on the specific issue of selling vulnerabilities, with only a few exceptions. Rather,

they make their positions clear by outlining what they believe is the appropriate way to handle vulnerability information. Examining company disclosure policies (which typically preclude exploit selling) and key security blog posts yielded the following results for the five companies I studied, broken down into sub corpora.

IBM

I applied codes 24 times in the IBM-specific corpus, which was straightforward in its ethical stance as compared to others. Its disclosure policy was brief (326 words) and implies an assumed code of private disclosure. We can see this emphasized in the company's use of the word "directly" in the following disclosure policy sentence: "Security researchers, industry groups, government organizations and vendors concerned with product security can report potential security vulnerabilities *directly* to IBM PSIRT" (emphasis mine). The policy does not acknowledge or allow for other types of disclosure outside of private disclosure. IBM's brevity indicates that the company does not feel the need to elaborate or get into the nuances of the disclosure debate like Microsoft and Google, likely because its products are far less frequently targeted by hackers as compared to other industry behemoths.

Throughout the IBM-specific documents, the company indicates that *Responsible Disclosure is Best* four times. In one post by the company's executive security advisor Diana Kelly, she emphasizes that she doesn't believe in "supporting vulnerability cowboys that publicize attacks outside of the parameters of responsible disclosure" and maintains that this type of public disclosure puts users at risk. Here, the use of the word "cowboys" labels hackers that practice public disclosure as renegade agents, untrustworthy and unstable. In this analogy, there is an assumed rule of law in the Wild West of the online security world, and such hackers aren't following this code.

One of the few direct condemnations of such cowboys emerged in another blog post by IBM security researcher Zubair Ashraf. In it, he summarizes the informal points of a speech by the company's CEO at a security conference and called out VUPEN directly, saying, "There are various entities with their business success depending on being able to break our systems (VUPEN, Hacking Team, Defense Contractors, etc), they clearly are not here to make our systems securer, and can't be classified as malicious parties either?" Here we see that VUPEN is listed as a party that is not interested in reducing risk to end users. This is one of the few examples of technology companies taking on vulnerability sellers directly in their discourse.

Secure by Design

Outside of reinforcing private disclosure, IBM's blog posts urge vendors to build more secure software *before* they are hacked. The company makes an argument for *Secure by Design* seven times, as compared to larger company corpora that make this argument only once or twice. Within these seven instances, IBM never takes personal responsibility for building insecure products, making it seem like a finger-pointing strategy at other technology companies. An example of this rhetoric, reinforcing private disclosure alongside the need to build more secure software, appeared in Kelly's post. She notes, "Researchers are finding the vulnerabilities the software producers didn't and, when done properly, helping vendors get those problems fixed. Vendors can help reduce vulns in the final product by building security in and defining security requirements up front then testing security features pre-launch." This argument disperses blame across hackers that don't disclose what they find and the vendors that create insecure code in the first place.

Kelly also raises the stakes on this argument by underscoring the most extreme possible scenarios for a successful hack of an insecure product (much like reporters drawing attention to

Stuxnet as the most notorious successful exploit in recent years). Kelly links hacking with the ability to kill by mentioning hacks of cars, pace-makers, and an insulin pump. She asserts, "Failure to require authentication on a shopping site could lead to an attacker ordering things on your account. No authentication on an insulin pump can mean an attacker stealing your life." In this sentence, she draws the reader's attention first to a fairly mundane example of hacking for online shopping and then juxtaposes it with the shocking idea of someone hacking an insulin pump. (In 2011 an IBM employee demonstrated a successful insulin pump attack.) This exaggerated example nudges the reader (likely a serious technology user or information worker), to side with IBM and pressure other vendors to build more secure software.

Calls for Regulation

Finally, within the selected corpus, IBM was the only company that called for external regulation on vulnerability issues. The company argued that the "community has to continue to uncover, track and educate on APT / government malware, and work with policy makers, human right groups, international peace organizations to set up policies, procedures, accountability and consequences for violations." This comment appears in the context of a narrative asserting that governments are increasingly engaging in cyberwarfare and authoring malware, with APT standing for Advanced Persistent Threat—typically meaning a highly specific attack on a chosen target. In this section of the blog post, IBM's CEO proposes that policy should temper governmental malware usage, which would have a direct effect on the companies selling malware to these governments. In this way, though IBM is not holding itself responsible for vulnerabilities in its products (at least in this sample), it is calling for greater industry regulations and for security researchers to practice private disclosure.

Amazon

As a major player in the cloud services sphere, not to mention its vast online shopping empire, Amazon appears in *Fortune's* top technology company list. As cloud providers more frequently deal with outages and data reliability issues than security, Amazon's online communication on vulnerabilities is sparse. Though I didn't locate any relevant blog posts or press releases from the company, it does have a vulnerability disclosure policy. In the policy, it outlines two main ethical arguments: *Responsible Disclosure is Best* and *We Take Security Seriously*. I applied six total codes within the policy.

With regards to private disclosure, the company lists its possible affected services and the types of incidents that might occur and asks anyone who identifies a suspected issue to notify the company via email. At the end of the post, the company reinforces this message more explicitly, writing, "In order to protect our customers, AWS requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed." Here it does not address the more nuanced debate about selling vulnerabilities, rather the company condemns public disclosure practices. Additionally, the *Greater Good* theme continues to come through; Amazon positions its instructions as the necessary steps "in order to protect our customers." Much like reporter commentary on commoditized vulnerabilities, companies frequently espouse private disclosure in the name of posterity.

The other theme that emerged in Amazon's post was building up its own ethos by emphasizing that it cares about the security of its customers. Three times during the post I applied the code *We Take Security Seriously*. An example of this credibility messaging is the word "commitment" in "AWS is committed to being responsive and keeping you informed of

our progress as we investigate and / or mitigate your reported security concern." In another line, the company declares its dedication even more overtly, "Amazon Web Services takes security very seriously, and investigates all reported vulnerabilities." Though the policy statement is a brief sample for the company, it shows a clear preference for the established ethical code of private disclosure and a desire to quickly reassure customers that Amazon can be trusted with their data, without getting too "committed" to the debate itself.

HP

HP is first and foremost a technology vendor that sells hardware, software, and services, but in 2010 it acquired TippingPoint, a security company that runs the annual Pwn2Own hacking competition through its Zero Day Initiative (ZDI). ZDI buys zero-day vulnerabilities and reports them back to impacted technology companies and then builds protections for the flaws into its own products. As TippingPoint has a pre-existing online footprint, I focused my analysis specifically on HP branded discourse on this topic. I examined a HP disclosure policy, corporate blog post, and infographic on disclosure. The HP corpus was 2787 words long and its disclosure policy was fairly robust at 813 words.

Out of the 28 code instances I applied, the most frequent was again *Responsible Disclosure is Best* with eight applications in the corpus. Within the company's disclosure policy statement, it uses the words "responsible" or "responsibly" four times—showing no hesitation to adopt the security community's assumed standard of conduct for disclosure. We can see this private disclosure preference in its explanation of the Pwn2Own contest, meant to "responsibly unearth new vulnerabilities and empirically demonstrate the current security posture of the most prevalent products in use today so that the affected vendor(s) can address them." The policy adds that winning vulnerabilities will be disclosed directly to the impacted vendors, then the winners

will be credited, but "Until then, the actual vulnerability will be kept quiet from the public." This positioning maintains the conduit between vulnerability finder and technology vendor and doesn't allow for companies like VUPEN to keep the exploits it demonstrates after the contest ends. In fact, it's likely that the following line was added to the policy in direct response to VUPEN refusing to give Google a vulnerability in Chrome during the 2012 contest: "This is a required condition of entry into the contest; all entrants must agree to the responsible disclosure handling of their vulnerability/exploit." In order to maintain its credibility as an ethical company, HP asks everyone to play by the generally accepted disclosure rules.

As a Vulnerability Finder

One difference between HP's policies and those of other vendors is that it primarily discusses its approach to vulnerability information it *finds*. Given its relationship with TippingPoint, HP is in both the position of a vendor with vulnerable products and a vulnerability finder. Overall, the company takes the historic position on disclosure, but draws a harder line on vendor responsiveness. Its disclosure policy explains that if HP "exhausts all reasonable means in order to contact a vendor" then the company may decide to post a public advisory about the flaw after fifteen days. The company also claims that it is justified in releasing a public advisory if the vendor does not fix the reported vulnerability within four months, assuming the vendor is not responsive to timeline negotiations. Such advisories usually include an explanation of the vulnerability and suggested mitigations/protections customers can apply. So even though HP primarily toes the party line on disclosure, it makes provisions for public disclosure in order to encourage quicker bug fixes.

As another example, in its security blog post, HP states emphatically, "In no cases will an acquired vulnerability be 'kept quiet' because a product vendor does not wish to address it." The

company advocates for working with vendors to address issues with their products, but also positions its vulnerability finding team and disclosure practices as a catalyst for quicker fixes. Another rhetorical move it makes in the blog post is giving examples of how it has worked with other vendors in the past to quickly rectify flaws. The company boasts that 300 bugs have been patched through the ZDI program—93 percent during its established vulnerability fixing timeline. It then praises Microsoft for patching quickly and pats itself on the back because "nearly half of all Microsoft's critical vulnerabilities patched in 2013 [we]re ZDI's."

In an unconventional move, the post then mentions that ZDI disclosed 17 zero days affecting HP, its parent company. Essentially, by highlighting this decision, HP shows that it did not shield itself from rigorous security examination and deadlines to fix problems with its code. This move builds its credibility as a morality enforcer in the community. The company's discourse about vendor responsibility augments its own ethos, showing that it is exceeding its own performance standards. It emphasizes this point further by claiming that "HP's Zero Day Initiative (ZDI) Disclosure Policy positively affects the ecosystem and prods vendors into further securing their software." Accordingly, it claims that its efforts benefit society and lead to more flaws being fixed more quickly.

Disclosure Infographic

HP's preference for private disclosure is evident in its decision to release an infographic on bug disclosure; in it, the company delineates six possible disclosure options for hackers and categorizes them according to white market, gray market, and black market. It's clear that part of the purpose of releasing this infographic is to highlight that its own modes of operation "hacking competitions and direct vendor communication" are white market activities (Fig. 5). It classifies companies like VUPEN and Netragard as gray market and reserves black market for hackers

who use exploits to "disrupt public or private groups." In this figure, the difference between gray market and black market seems to be to whom the vulnerabilities are sold because presumably, governments are also using the vulnerabilities they buy to disrupt their public and private targets.

Figure 5. HP representation of ethical markets and disclosure practices. Source: Hewlett Packard. "The Vulnerability Market Decoded." April 2014.

The infographic goes on to discuss the following disclosure options: submit flaw to third-party bug bounty program, enter hacking competition, submit flaw directly to vendor, sell flaw to private broker, sell flaw to the highest bidder, and publicly disclose flaw. The company then lists the "result" of each type of disclosure and uses statistics to bolster its ideologies.

The HP-approved methods of disclosure comes first. According to the infographic, the result of entering a found flaw into a bug bounty program is that it is fixed and the researcher gets paid. HP augments this ethical line of action by noting that HP ZDI has paid out 10 million to researchers for such flaws. Essentially the company is arguing that hackers can both do the right thing and make lots of money by submitting discovered vulnerabilities to HP.

To push hackers toward option two as another viable choice, the infographic states that entering a hacking competition wins researchers "fortune and fame" and that its baby,

Pwn2Own, has prizes of up to $150,000. It also calls out a particularly lucrative pay-out for an Android flaw of $50,000. In this way, the company is trying to incentivize hacker participation in its contest by calling out the biggest possible prizes.

Option three is direct-to-company disclosure. HP underscores that one researcher received $12,500 from Facebook for disclosing a flaw to the company. It also attaches the Facebook "Like" icon of a thumbs-up near this figure, reinforcing it as a positive course of action with a visual cue. The result of this action, according to HP, is that the bug in question is repaired. It also includes an arrow to option six from here, indicating that if the vendor does not respond in a timely fashion, researchers will often choose public disclosure. This again, puts the onus on other technology companies to be responsive to bug reports.

Option four addresses vulnerability sales directly, noting that selling to private brokers leads to uncertainty about where a flaw will end up. However, HP does offer a stamp of approval for companies that claim to operate ethically within this space. The infographic asserts that "some grey market brokers have policies which will only sell to ethical and approved sources." The vagueness of this statement prevents HP from picking fights with any particular vendor as it does not define who is the appropriate body to "approve" these sales and what constitutes an "ethical" transaction. The possible outcomes of these sales is equally murky from a moral standpoint. HP notes that these transactions can lead to "spy[ing] on private citizens suspected of crimes" and to "shut[ing] down suspected terrorist operations." Most people would agree that foiling terrorists is a nobler cyber mission, but the first option is riddled with moral ambiguity. As the 2014 NSA internet tapping scandal reveals, the United States citizenry is divided on the moral implications of government spying even in the name of protection ("The NSA Controversy"). Overall, the infographic keeps commoditized vulnerabilities at arm's length,

calling out the possible implications but refusing to pass clear judgment. This reluctance is also apparent in HP's designation of these activities as gray market. Whereas reporters overtly chastise vulnerability sales, technology companies try to keep their communication as broad as possible to maintain their relationships with security researchers.

Finally, the company addresses the black market, which it defines as selling vulnerabilities "to the highest bidder." It concludes that such actions lead to cybercrime, stealing money, and corporate secrets. It also includes imagery with sinister looking black hatted figures buying the bugs and using them to take over a computer and make it similarly evil (Fig. 6). In this case, HP is literally using "black" and "white" ethical frameworks to classify types of disclosure.

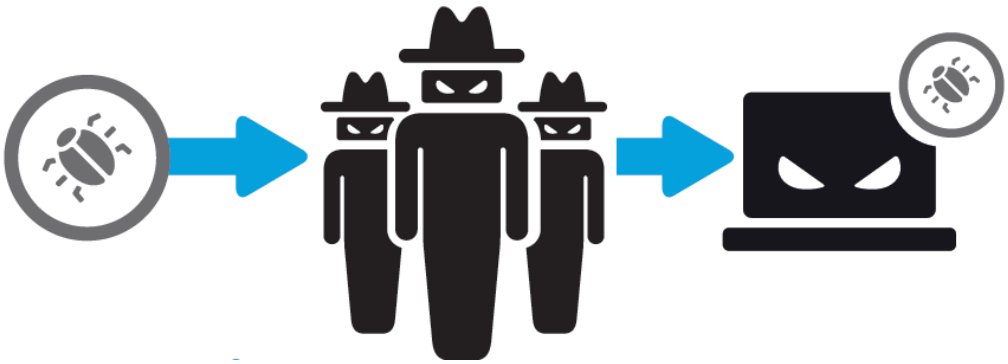

Figure 6. HP representation of black market buyers and sellers. Source: Hewlett Packard. "The Vulnerability Market Decoded." April 2014.

Microsoft

The Microsoft corpus was the second longest by word count at 4460, with 93 applied codes. The company has historically been vocal about disclosure issues as its products are often at the center of security incidents and debates. Because of its ubiquity in the technology world, Microsoft is in a position of influence when it lays out security policies and moral frameworks. For the purposes of this study, I collected its disclosure policy, a disclosure ethics video transcript, and four security blog posts.

Of note, a blog post by Tim Rains, director of the security division, offered one of the only overt vendor reprimands of companies like VUPEN. In his post discussing Microsoft's Security Intelligence Report, which tracks malware trends, Rains argues, "Vulnerability disclosures originate from a variety of sources, from dangerous disclosures (such as from malicious exploit developers and vulnerability sellers) to limited beneficial disclosures (such as the affected software vendors themselves and security researchers who are committed to coordinated vulnerability disclosure)." Here he juxtaposes vulnerability sellers doing "dangerous disclosures" with "beneficial disclosures" that follow the guidelines of CVD. Granted, Rains might have been referring to people who sell vulnerabilities on the black market instead of to governments, but the sentences reads like a blanket reproof of selling vulnerabilities instead of disclosing them to companies.

Coordinated Disclosure is Best

Additionally, in the Microsoft corpus there continued to be a theme of private disclosure as the prescribed method of behavior (13 codes). The company espouses private disclosure in its policy statement, writing:

> We ask the security research community to give us an opportunity to correct a vulnerability before publicly disclosing it, as we ourselves do when we discover vulnerabilities in other vendors' products. This serves everyone's best interests by ensuring that customers receive comprehensive, high-quality updates for security vulnerabilities but are not exposed to malicious attacks while the update is being developed.

In this statement we see a clear connection between private disclosure and the *Greater Good* theme, meaning that selling vulnerabilities is outside of the scope of actions that will help keep

the broader populace safe online. Microsoft identifies direct-to-company disclosure as serving "everyone's best interests." This makes the case that other types of disclosure will put internet users at risk.

This being said, in 2010 Microsoft recognized the loaded rhetoric inherent in "responsible disclosure," i.e., that all other types of disclosure are irresponsible. In response, it conducted a public reframing campaign called Coordinated Vulnerability Disclosure (CVD). The ultimate policy was similar to private disclosure, with minor provisions that relaxed acceptable behavioral standards. In her blog post, Katie Moussouris, senior security strategist lead, positions the change as "a renaming of Responsible Disclosure that provides expectations and a process for Microsoft and researchers to work together without either party clouding the discussion with a term that is easily misinterpreted, even in cases where disclosure philosophies may not be entirely in sync." Microsoft's revised policy continues to advocate primarily for private disclosure but allows security researchers to disclose vulnerabilities to third-parties such as government security organizations (CERTs) as intermediaries who eventually work with the vendor to rectify the issue. The modifications also allows for public advisories (or full disclosure) in the case of active attacks "in the wild."

We Collaborate

With this CVD framework in mind, Microsoft's new leading message became collaboration. The collaboration code was actually even more prominent than private disclosure at 29 instances. This theme manifested itself throughout the corpus (in blog posts, reporter statements, and a disclosure video). The company assiduously positions itself as a team player—a positive contributor to the wellbeing of internet users. Instead of shining a light on its vulnerable products or chastising inappropriate disclosures, the company's discourse shifts to

focusing on its efforts to protect customers in tandem with others. In fact, Moussouris performs an interesting discursive maneuver by including the names of 19 third-parties who "reviewed" the concept of CVD in her blog post (e.g., Cisco, Symantec, McAfee, Intel PSIRT). Doing so shows community support for Microsoft's concept of disclosure and lends further credence to the idea of the vendor as a collaborator.

To further develop the collaboration angle, Moussouris explains, "[W]hat's critical in the reframing is the heightened role coordination and shared responsibility play in the nature and accepted practice of vulnerability disclosure. This is imperative to understand amidst a changing threat landscape, where we all accept that no longer can one individual, company or technology solve the online crime challenge." In this sentence, she uses communal language like "we all accept" and "shared responsibility." This method normalizes Microsoft's perspective; positioned this way, everyone agrees with Microsoft and will naturally want to work with the company to help secure its products. Also, by drawing attention to the overwhelmingly large online crime problem, which is not Microsoft's sole responsibility to solve, the quote encourages a collective approach to stopping the bad guys.

Matt Thomlinson, general manager of Microsoft's security division, reinforces collaboration and the *Greater Good* message a year later, stating, "Collaboration between security researchers and vendors is ultimately about preventing attacks and protecting the computing ecosystem…. We encourage others to adopt this philosophy in the interest of creating a safer and more trusted internet for everyone." Here Microsoft extends the invitation beyond what it is doing and asks others to follow the CVD model. Doing so, according to Thomlinson, reduces risk and protects the computing ecosystem. I marked instances like these with the *Greater Good* code 19 times. Of note, "ecosystem" is a common term in the security world, and

it serves to associate internet security with environmental rhetoric. Thus, practicing CVD is akin to reducing the risk that the spotted owl will become extinct. The internet is painted as a natural system in delicate balance and only by practicing certain disclosure practices can it be protected from damage. Similarly, HP uses the term three times in its corpus as a means of expressing how its ZDI program positively affects the environment of the internet. Such language helps vendors support their *Greater Good* arguments by talking about the internet as a single system.

Disclosure Ethics Video

Microsoft's perspective is even more clearly evolved in a disclosure video that it embedded with its CVD policy. In it, the company refers to a generic security researcher named John who thought that full disclosure was the best way to get technology companies to fix vulnerabilities but then learned the error of his ways. The narration reads like a cautionary bedtime story to train hackers about the ethical way to operate. "Meet John, an experienced security engineer," it begins:

> Over the years, he reported problems to software companies, but sometimes it seemed like nothing happened. So, he took it upon himself to pressure vendors to act more quickly by publicly publishing the vulnerability details for all to see…. But, John's disclosure method, inadvertently shifted advantage to the criminals who could use the information to impact the wellbeing of individual and business computer users around the world.

The phrase "took it upon himself to pressure vendors" is inherently negative, implying that it wasn't his place to move companies along in their patch timeline. Then Microsoft makes the *Falling into the Wrong Hands* argument that so often appeared in the reporter corpus. In this

case, by not practicing CVD, John "shifted advantage to the criminals," which leads to increased risk to end users, the *Greater Good* argument.

After explaining the possible implications of public disclosure, John learns his lesson. The narrator comments, "These days, John feels differently. He sees that vulnerability information must be protected because criminals will seize any opportunity to commit crime online, and he doesn't want to be responsible for contributing to criminal activity." Here we see disclosure painted in terms of a moral binary. Either he works with vendors or he is contributing to criminal activity. This is similar to the money or morality binary of the reporter corpus.

The narrator then takes a turn toward the extreme by highlighting the scariest possible scenario for public disclosure. He continues, "Plus, John knows that software runs on more than just home and business computers. The same code may now run airlines, power stations, even heart monitors. Full disclosure could have serious, real-world consequences." These examples are paired with an image showing critical infrastructure, a plane, and a hospital patient (Fig. 7). The red X's signify that a vulnerability is being used to disrupt these services and threaten people's lives and livelihoods. John, as a presumably good guy, figures out that he doesn't want to have anything to do with killing people with public disclosure. With this visual appeal to pathos, Microsoft targets people's natural instinct to protect each other from harm. The red X's imply that public disclosure could lead to problems of apocalyptic proportions.

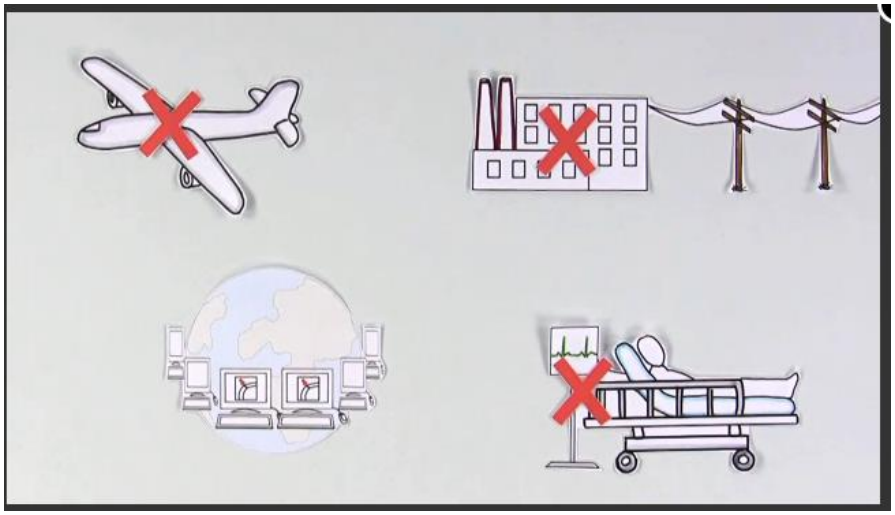

Figure 7. Microsoft video graphic showing the possible ramifications of the public disclosure of a vulnerability. Source: Microsoft Security TechCenter. "Coordinated Vulnerability Disclosure" 2011.

The video ends with the final moral of the story and one additional message—that vendors should not be held to arbitrary deadlines for developing patches. The narrator concludes that "John knows that holding software companies to a one-size-fits-all deadline to deliver an update, doesn't make sense" and "…creating updates for potentially hundreds of millions of systems still takes time." Whereas other vendors like HP and Google advocate for bug fix deadlines, Microsoft, given the volume of security flaws in its queue, tends to resist these deadlines. The video establishes the complexity of developing patches for millions of systems as a reason to eschew patch deadlines. Similarly, Moussouris calls out the diversity of security issues as contributing to the bug fix timeline. She explains, "The security testing for simple vulnerability classes like buffer overflows is typically very fast. More complex attacks that rely on a multistep exploitation process, or vulnerabilities with multiple vectors to reach the vulnerable code require more security testing time. If security testing was all vendors had to do, we wouldn't have as many timing disagreements." Microsoft's resistance to patch deadlines is in

direct opposition to other vendors that have attempted to establish universal norms for addressing vulnerabilities.

Google

Out of the five company corpora, Google's was the longest, at 5173 words. It included four blog posts, a disclosure policy, and a vulnerability bounty program policy that were germane to this research.[4] Altogether, I applied 65 codes within the corpus. Among them, the strongest theme was *Greater Good* with 19 instances. For example, Google wrote its disclosure policy directly to the end user, vowing that "we recognize how important it is to help protect your privacy and security. We understand that secure products are instrumental in maintaining the trust you place in us and strive to create innovative products that both serve your needs and operate in your best interest." Like other vendors, Google highlights that its actions are motivated by the "best interest" of internet customers. The company uses phrases like "make users safer," "more secure browser," and improving "the state of web security" to drive this theme throughout its discourse.

The policy goes on to call for private disclosure and "reasonable disclosure deadlines" as the best measures for protecting end users. This caveat about disclosure deadlines is the main rhetorical difference between Google and Microsoft. The company makes the argument that vendors should be held to patching deadlines 11 times in its corpus. It defines a reasonable timeframe for patching as 60 days in most cases and seven days if a vulnerability is known to be under active attack in the real world. Like Microsoft encouraging broad adoption of the CVD policy, Google calls for other vendors to begin holding themselves to the 60-day rule. They

[4] These resources were attributed to various authors on the Google Security Team versus one spokesperson, so I will refer to quotes and commentary corporately.

attribute this sense of urgency to "[c]reating pressure towards more reasonably-timed fixes [that] will result in smaller windows of opportunity for blackhats to abuse vulnerabilities. In our opinion, this small tweak to the rules of engagement will result in greater overall safety for users of the Internet." Again, adopting the vendor's policy here is tied to the *Greater Good* of internet users. We see that each vendor has its own philosophy on the best course of action for disclosures, and each argues that its policy is in the best interest of customers.

As part of its discussion of disclosure deadlines, Google also challenges the rhetoric of "responsible disclosure." In this excerpt, the company refers to an assumed code of conduct regarding private disclosure:

> So, is the current take on responsible disclosure working to best protect end users in 2010? Not in all cases, no…We've seen an increase in vendors invoking the principles of "responsible" disclosure to delay fixing vulnerabilities indefinitely, sometimes for years…. The important implication of referring to this process as "responsible" is that researchers who do not comply are seen as behaving improperly. However, the inverse situation is often true: it can be irresponsible to permit a flaw to remain live for such an extended period of time.

This assertion that vendors are sluggish about patching vulnerabilities provides Google with grounds for calling for vulnerability deadlines. In one of its blog posts, the company calls "responsible disclosure" a "two-way street" that requires researchers to disclose vulnerabilities directly to vendors and vendors to fix them in a timely fashion. The tension between Microsoft's and Google's positions is clear. For Microsoft, CVD is the Promised Land for end user safety; for Google, it is quick fixes.

Google again mentions this proverbial "two-way street" in its vulnerability reward program literature and clarifies that only direct-to-vendor disclosure is approved. The company argues that "[v]ulnerabilities that are disclosed to any party other than Google, except for the purposes of resolving the vulnerability (for example, an issue affecting multiple vendors), will usually not qualify [for a bounty]. This includes both full public disclosure and limited private release." Such verbiage clearly precludes companies like VUPEN and Netragard from participating in Google's financial incentive program.

We Collaborate

Despite the differences in their disclosure philosophies, like Microsoft, Google makes a strong case for collaboration in its materials (10 instances). As an example, when discussing its vulnerability reward program, the company boasts, "We already enjoy working with an array of researchers to improve Google security, and some individuals who have provided high caliber reports are listed on our credits page. As well as enabling us to thank regular contributors in a new way, we hope our new program will attract new researchers and the types of reports that help make our users safer." Once more the *Greater Good* theme is linked with this message. Similarly, in another blog post the company states, "Together as a security community, our combined efforts to find vulnerabilities in browsers, practice responsible disclosure, and get problems fixed before criminals exploit them help make the Internet an overall safer place for everyone." Looking across Microsoft's and Google's corpora, the *Greater Good* and *Collaboration* code co-occurred 16 times—showing a strong connection between the two themes. The other major co-occurrence trend across all vendors was *Greater Good* and private disclosures with 11 instances across Microsoft, Google, and IBM.

Hacker Corpus Analysis

Netragard

The Netragard corpus contained 8792 words, and within it, I identified 110 code instances. Of these, the most commonly applied code was *Competing with Other Hackers* (25 instances). In Netragard's blog posts and company "About Us" page, the company repeatedly establishes its own ethos by taking shots at other security researchers. Instead of positioning itself in opposition to technology companies, Netragard most often chooses to differentiate itself from its peers in terms of skill and trustworthiness. This code usually corresponded with two other ethos-building codes, *We're Trustworthy* (co-occurred four times) and *We're Sophisticated/Advanced* (co-occurred 10 times). In one Netragard blog post, for example, the company asserts that "[t]he Good Guys in the security world are no different from the Bad Guys; most of them are nothing more than glorified Script Kidies. The fact of the matter is that if you took all of the self-proclaimed hackers in the world and you subjected them to a litmus test, very few would pass as actual hackers." In this case, the company contrasts itself as a collective of *real* hackers with people *playing* at being hackers. It appropriates the hacker terminology as a badge of honor and simultaneously questions the aptitude of other hacking firms.

Comparative Ethos

In another post, the company's technique involves expounding upon its corporate motto. It argues, "Here at Netragard We Protect You From People Like Us and we mean it." The quote continues with a competitive flair, reading, "We don't just run automated scans, massage the

output, and draft you a report that makes you feel good. That's what many companies do. Instead, we "hack" you with a methodology that is driven by hands on research, designed to create realistic and elevated levels of threat." Here the implication is that other security researchers are using simple scanners to do security testing versus rigorous individual testing methods. Throughout the company's corpus, it builds its ethos by reinforcing its quality services and questioning the practices of other hackers for hire. Simultaneously, it implies that customers will be safest if they trust Netragard to test their products (co-occurred 10 times with the competitive code).

Another example of this rhetorical strategy is the decision to include a *CRN* top hacker ranking in one of the blog posts that showed that Netragard's Kevin Finisterre is a top mind in the field. This is strategically positioned after an admonishment of hacking companies that don't do active research in the field and are thus not up-to-date on the latest exploit techniques. Much like academics who show their merit by producing an ongoing stream of publications, Netragard underscored its research frequently as evidence of its integrity as a truly talented hacker company. In fact, as highlighted by its many blog posts on the topic, the company seems almost defensive as it continually reinforces its ethos.

War and Gun Analogies

One of the most interesting ways that Netragard enacts its competitive positioning is by drawing on war or gun analogies. In fact, it uses the same metaphor of a company trying to use a squirt gun against an imagined adversary three times in the corpus. In a blog post titled "How to Find a Genuine Penetration Testing Firm," Netragard offers this illustration: "a Vetted Automated Vulnerability Scan is about as effective as Penetration Testing a bulletproof vest with a squirt gun. We're not sure about you but we wouldn't want to wear that vest into battle. These

types of services provide little more than a false sense of security." In this excerpt and the two others like it, Netragard accuses other hackers of doing the weakest possible penetration tests against customer systems. The water gun is an analogy for automated scans that are offered by other companies and will not help the customer prevent more devastating cyberattacks.

The company utilizes war or gun analogies to make an ethical argument six times in the corpus. Another particularly vivid example of this metaphor is the assertion that other companies' penetration services are like shooting tanks with toy guns. One post argues:

> …we don't test our tanks against fire from bb guns and .22 caliber pistols…We test the tanks against a threat that is a few levels higher in intensity than what they are likely to face in the real world. As a result, the tank can withstand most threats and is a very effective weapon. Doing anything less isn't going to protect you when the threat tries to align with your risks; you'll end up being an expensive casualty of war.

All of this ethos-building is important in the context of Netragard's broader business model, which entails vulnerability selling. The company works hard to establish its credibility by emphasizing the defensive side of its business model. When it does discuss its offensive side, it makes two strategic rhetorical moves: downplaying the possible risks of zero-day sales and positioning itself against less ethical vendors.

Ignore Whistleblowers

One of its strategies to reduce the perception of risk is to discredit alarmists (four code instances) in the security world who typically speak out against zero-day sales, such as Chris Soghoian. In one blog post, the company builds a case that malware most frequently spreads via social engineering scams that target user gullibility (e.g., clicking on a malicious link in an email). The company draws on an iteration of the Microsoft Security Intelligence Report to show

the small percentage of malware infections that spread via vulnerabilities and then further emphasizes that known vulnerabilities are more dangerous than brand-new zero-days. This post relies heavily on logos, citing a key piece of evidence that 99 percent of all computer compromises cannot be attributed to zero-day vulnerabilities. Netragard argues that any known vulnerability is dangerous even if patched as IT administrators and the public are often slow to apply security updates. The company also directly refutes Bruce Schneier's point about the danger of zero-days and chastises reporters who over-emphasize the risks of the market. For example, the company argues, "Finally, we are hopeful that people will do their own research about the zero-day exploit markets instead of blindly trusting the largely speculative articles that have been published recently." By calling reporter commentary about their business model *largely speculative*, the company discredits journalists and implies that they don't understand the full picture of the zero-day market.

As part of the company's argument that its participation in the zero-day market does not increase end user risk (nine instances), Netragard asserts that an exploit is merely a tool that takes advantage of vulnerable software. In one post it makes the argument that "Buying an exploit is much like buying a hammer in that they can both be used to do something constructive or destructive." It implies that exploits themselves are not evil; their use determines their virtue. The company frequently emphasizes that its customers are thoroughly vetted, thus trustworthy to wield these tools.

Taking on Technology Companies

Secondly, to defend its business model, Netragard often attacks technology companies (seven instances), typified by the comment: "The software vulnerabilities that exploits make use of are created by software vendors during the development process. The idea that security

researchers create vulnerability is absurd." Though Netragard tips its hat to technology companies like Microsoft that have robust security processes built into their software development, it does not hesitate to remind the public who made the vulnerable code in the first place.

The company also cites technology companies' historic reluctance to pay security researchers for discovered vulnerabilities, as well as relatively low bounties, as a justification for its place in the market. Netragard comments that vendors have even threatened researchers with legal action in the past for pointing out software flaws in their products. Though the company doesn't cite the specific case to which it refers, it argues that vendors have been a large part of the problem in creating vulnerabilities and deincentivizing private disclosure. It equates this threat for legal action with someone being sued for pointing out that a bus's brakes are faulty. By making this analogy, it builds a case for the ethics of hacking as a whole.

Taking on VUPEN

Interestingly, Netragard positions itself specifically against VUPEN. After ensuring that it has established its credibility as a genuine research firm and reminded the public whose fault software vulnerabilities really are, Netragard makes an ethical spectrum argument. The company points out who is on the low end of the ethical spectrum to whiten its hat by comparison. One post asserts, "Unlike VUPEN, Netragard will only sell its exploits to US based buyers under contract. This decision was made to prevent the accidental sale of zero-day exploits to potentially hostile third parties and to prevent any distribution to the Black Market." Netragard's main differentiator is that it only sells zero-days to domestic buyers. The logic is that people within the U.S. are trustworthy and anywhere else is too uncertain. Netragard equates *the other* with risk, but like other companies in this business, will not disclose anything specific about its buyers.

The post takes another polite nudge at software vendors, noting, "Netragard also welcomes the exclusive sale of vulnerability information to software vendors who wish fix their own products. Despite this not one single vendor has approached Netragard with the intent to purchase vulnerability information. This seems to indicate that most software vendors are still more focused on revenue than they are end-user security." In this instance, Netragard takes up the *Greater Good* argument and puts the onus on vendors to protect the broader internet ecosystem. It is more than happy to help out if they will just buy back vulnerabilities.

Along these lines, Netragard frames its Exploit Acquisition Program as follows: "[It] was created to provide ethical researchers with the ability to receive fair pay for their hard work; it was not created to keep vulnerable software vulnerable." Again the company casts itself as a noble benefactor, paying the good guys for their hacking. It refutes the idea that it is keeping vulnerabilities in software by not disclosing them, although, logically, its business of selling to third-parties does this. So by nature, it *wasn't created* to keep people vulnerable, but ultimately it keeps vulnerabilities open.

In summary, Netragard makes a large number of diverse arguments to support its offensive and defensive models. The company is throwing the proverbial spaghetti at the wall to see what sticks, but the common thread throughout this sample is building up its credibility and discrediting technology companies and other hackers. By reminding IT professionals of its high quality research and casting doubt on everyone else, it bolsters its position in the market. Though it does not discuss its offensive model as frequently, when it does, it downplays the risk of the zero-day market and highlights its domestic selling.

VUPEN

Altogether the VUPEN corpus was over 20,000 words—the large volume due to all the code demonstrations and exploit notes in the blog posts rather than expository content. If we count only the "About Us" content, the CEO podcast, and other website notes, the corpus contains only 2,800 words. These artifacts are more telling as the technical blog posts are 90 percent composed of exploit how-tos. Therefore, my analysis focuses primarily on narrative content as it is imbued with more overt ethical stances. That being said, a few trends in the code notes are worth mentioning. For example, the technical blog posts almost always started with a nod toward how advanced the exploit technique was that the VUPEN researcher was about to explore (e.g., the title reads "Advanced Exploitation of VirtualBox 3D Acceleration VM Escape Vulnerability (CVE-2014-0983)"). In fact, the VUPEN corpus uses the word "advanced" 15 times and "sophisticated" nine times. Though brief, these verbal commendations in the midst of technical blog posts are one way VUPEN builds its image as a highly talented firm.

Another interesting point about the code notes is that often the author would point to a place in the code and editorialize, "crash here!" or "pwned!" Though it's important for the author to point out where the crash will happen during the exploit process, the enthusiasm of the exclamation point can be interpreted as containing a degree of pride or bragging. The code notes are just one example of the company's persistent attempts to prove its capabilities. In fact, the most common code I applied for VUPEN was *We Are Sophisticated/Advanced* at 27 instances. Whereas Netragard often called into question the skills of other "script kiddies," VUPEN instead praises itself to build its credibility.

We're the Best

An example of VUPEN's frequent self-applause is in its "About Us" section in which it points to industry awards, lists the Pwn2Own competitions it has won, and emphasizes the

prestige of its hackers. The company asserts that the "VUPEN Vulnerability Research Team (VRT) is the most active security team in the world. VUPEN security researchers daily discover and exploit unpatched and critical vulnerabilities in prominent and widely deployed software, applications and operating systems. Frost & Sullivan has recognized VUPEN as the leading provider of exclusive vulnerability research." Pointing to the Frost & Sullivan designation is another example of ethos building. In VUPEN's case, with the controversy surrounding its brand, it's not surprising how much time it devotes to legitimizing its research.

Another example of the *Advanced/Sophisticated* code was the company's allusion to its Pwn2Own winnings in the midst of a technical blog post explaining an exploit technique. The researcher notes, "In this blog we will share our analysis and advanced exploitation technique of an integer overflow vulnerability we have discovered and exploited at Pwn2Own 2013 as first stage (CVE-2013-2551 / MS13-037) using dynamic ROP building and without any heap spray to achieve code execution in the context of IE10 sandboxed process, which is the first step needed to put a Pwn2Own jacket in your closet." Here the company references the Pwn2Own jacket in an offhand way to highlight its win. By and large the company does not try to participate in the ethics argument, rather they project an attitude of "we're the best, can you deny that?" They have an unapologetic style and a certain swagger in the security world.

Exploits Don't Kill

Though VUPEN does not address the ethical implications of its business model on its website, its ethical stance was more overt in an interview Bekrar did with *SecurityWeek's* Ryan Naraine. In it, Naraine asks him directly about the controversy and Bekrar uses a few rhetorical strategies to defend it. First, when Naraine asks a leading question about exploits falling into the wrong hands (a frequent reporter argument) and being used for "terrible purposes" by

"repressive governments," Bekrar responds adamantly that the argument "doesn't worry me because it's not true. Exploits do not kill, computers do not kill; if a repressive regime wants to kill people they have old-school methods: they spy on their phones, they spy on their homes, they go to their homes, they install cameras, they spy on their work, so they don't need zero-day exploits." The argument here is that the bad guys will do bad things regardless of whether they have a zero-day to use. Bekrar believes that selling zero-days does not increase risk to end users because repressive governments will harm and spy on people regardless. If we buy the war analogy, this argument is akin to insisting that arms dealers have no responsibility for selling guns to repressive governments.

We Only Sell to Good Guys

Elsewhere in the interview, Bekrar clarifies that his company sells vulnerabilities not to criminals but to governments. He puts a positive spin on his business model as helping customers, noting, "When we sell an exploit as part of offensive service to government agencies, it help them to fight crime. So they use these exploits during criminal investigations; they don't use it to spy on people." Repeatedly throughout the VUPEN corpus the company equates its business model with fighting crime, law enforcement, and helping good governments. Six times in the corpus, the company mentions these types of entities in conjunction with its customers. There is also mention on the website of selling to private entities, so the law enforcement angle seems to highlight just the most palatable customers to whom they sell.

Another important argument that comes up in the podcast and several other times in the corpus (seven instances) was VUPEN's insistence that it vets its customers carefully. Like Netragard, the *We Only Sell To* argument is paramount to its ethical stance. In Netragard's case, it only sells to U.S. buyers, for VUPEN, it relies on outside standards to determine the

trustworthiness of its customers. It only sells to NATO and its partners and won't sell to any country under embargo. To underscore this point, the company frequently reminds the reader about its "Know Your Customer" program, a process of vetting it goes through when deciding whether to sell to a particular customer based on U.S. government regulations. So outside of building its ethos, it washes its hands of responsibility for how exploits are used but insists that it only sells to the good guys.

Results Summary

Overall, though there are some similarities across the three groups' argumentative tactics, they are largely talking past each other at this point in the discourse lifecycle. The technology companies position themselves as the collaborating good guys looking out for the little guy. The reporters side with the technology companies but represent the hackers' perspective for balance. The hackers deny that they are increasing risk and claim that they need to pay their bills and help their own customers, who are debatably, the good guys as well. As long as there is unclaimed money on the table of commoditized vulnerabilities and as long as software continues to contain holes, these parties are unlikely to agree. In the end, this investigation can help policymakers and regulators understand their arguments better, learning where to step in (or not to), based on the course and intensity of the discourse.

Chapter 3: Discussion & Conclusion

The world of online security is convoluted and often changing, but it is subject to the shaping forces of rhetoric just like our physical society. Yet, it's difficult for computer scientists to speak about cybersecurity outside of the framework they've inherited. Even the word "security" carries with it the idea of a computer as a locked safe or a house, and hackers as burglars or intruders. By examining such underlying rhetorical constructs, we can bring new terminological clarity from an external, critical perspective. As Martin Rein and Donald Schön point out in their discussion of discourse's impact on policy, "The complementary process of naming and framing socially constructs the situation, defines what is problematic about it, and suggests what courses of action are appropriate for it. It provides conceptual coherence, a direction for action, a basis for persuasion, and a framework for the collection and analysis of data" (153). As vulnerability selling is an emerging ethical gray area, studying this naming and framing process can enlighten policymakers.

Cybersecurity regulation is relatively uncharted territory, so lawmakers are currently grappling with various courses of action to curb attacks and strengthen governmental response. A recent example was the Cybersecurity Information Sharing Act, drafted by Senate Intelligence Committee Chairman Dianne Feinstein in June of 2014. It is a controversial bill pertaining to information sharing between the private and public sector, and so far it has made little forward progress. Because of renewed discourse in the United States following the 2014 Sony hack by North Korean hackers, Feinstein was able to put it back on the table for discussion. It's evident

that public rhetoric and media coverage have a profound effect on real legislation, providing an exigence for discussion and incentive for ratification.

In this final chapter, I will focus on the most prominent and significant arguments that emerged amongst the three groups I studied. Though across the corpora arguments were diverse, there were two primary rhetorical strategies that arose as central to the debate: 1) arguments based on a utilitarian ethical framework and 2) ethos-construction to bolster the groups' respective positions. These two strategies can also serve as containers for sub-arguments (e.g., arguing that an exploit could fall into the wrong hands is contained in the larger umbrella framework of *Greater Good*, assuming that evil actors may harm the average person).

Utilitarianism as an Ethical Framework

It's clear that the rhetors in this modern debate about cutting-edge hacking technique are largely using centuries-old argumentative strategies. One of the primary moral frameworks that people from all sides of the argument employ relies on utilitarianism, which was first systematically developed by Jeremy Bentham in the eighteenth century and whose precursors can be seen in moral argumentation throughout history (Driver). In the reporter corpus, this argument showed up 26 times, in the company corpus 43 times, and in the hacker corpus 18 times. Markers of this type of argument include collective references like "us all" and references to the faceless, innocent "end user at risk."

Utilitarian appeals equate the correct moral choice to the action that will benefit the greatest number of people. To define benefit, often utilitarian philosophers equate morale choices with increased happiness. In the case of computer security, then, happiness can be defined as a computer performing the actions a user wants (e.g., surfing the web, online shopping, business transactions) without disruption by malicious ads, crashing systems, or information theft.

When I examined the co-occurrence of codes within both the technology company and the reporter corpora, I realized that utilitarianism undergirded the rhetors' primary call to action: private disclosure. Encouraging this type of disclosure is the main reason software companies put out communications on this topic—they want hackers to help them fix their products and they don't want public relations cherry bombs going off with each new vulnerability that surfaces. The *Responsible Disclosure is Best* code, therefore, co-occurred with the *Greater Good* code eight times for reporters and 11 times for technology companies. In this argumentative structure, there is a clear link between private disclosure as a prescribed behavior and benefit to the greatest number of users. An example of the connection between these two codes was the *Dark Reading* quote that "…there's still room in the world for researchers willing to make a smaller amount of cash while helping the public good through responsible disclosure to vendors."

Quotes like these show reporters enacting the role of "political orator" as defined by Aristotle and explained by Ronald Duska: "The political orator aims at establishing the expediency or the harmfulness of a proposed course of action: if he urges its acceptance, he does so on the ground that it will do good; if he urges its rejection, he does so on the ground that it will do harm" (124). Their role in this debate is to accurately represent all the relevant perspectives, but they also endeavor to shift public opinion against commoditized vulnerabilities. Their techniques for accomplishing this are to frequently quote security activists like Chris Soghoian who demonize the practice in the name of the *Greater Good*. Likewise, they often characterize vulnerability selling as "shady" or "secretive," draw attention to potential nation-level cyberwar consequences, and present vulnerability selling as a binary with a lucrative pay out on the one end and morality on the other. To choose vulnerability selling is to choose the risk

that exploits will *Fall into the Wrong Hands* (e.g., terrorists, criminals) over the wellbeing of all end users.

However, it's important to define the nameless masses who are invoked by *Greater Good.* For the reporters and the company representatives, who are generally against the practice of vulnerability selling, they frequently frame end users as helpless victims. Though scholars like Elizabeth Schneider have argued against victimization rhetoric because it denies individual agency, it is an essential component to the *Greater Good* logic. Schnieder explains that "…victimization claims make powerful appeals for sympathy, solidarity, compassion, and attention" (395). It's noteworthy that much of this debate is built upon the premise of a naïve end user that needs technology companies and hackers to protect him or her. Policymakers should consider, therefore, how the victimization rhetoric inherent in this argument can play on their emotions, positioning technology companies as saviors, hackers as villains, and the end user as helpless.

It's also important to complicate how the *Greater Good* notion was adapted for this discourse. There were two types of *Greater Good* audiences that the rhetors tended to summon up. There is the general public good and there is the good of a subset of the population, i.e., the hackers' customer base. Walton categorizes this ethical reasoning as a "representationalist ethic" versus a "communitarian ethic" (125). Though a representationalist ethic protects a company's ability to make a profit, Walton argues that it makes that business less sensitive to the needs of society. In the case of vulnerability sellers, they have been criticized for putting the needs of their constituents over the needs of the average end user. In response, they defer to the good they are conveying upon those who are willing to pay and note that they must also make an appropriate living for themselves.

This tension calls to mind one of the classic objections to utilitarianism, that is, how do we define good, and who are the end audiences about whom we are making such decisions? Duska crystalizes this critique, writing, "[T]here is not one canonical view of what the good is, and consequently any appeal to the greatest good or the greatest happiness or the greatest pleasure, is simply an appeal to a preference" (120). Because of the essential malleability of this position, it is easy for the hackers to make counterpoints in which they emphasize the good of their customers and their own needs. For example, Netragard cites that its "Exploit Acquisition Program was created to provide ethical researchers with the ability to receive fair pay for their hard work; it was not created to keep vulnerable software vulnerable." Bringing in the word "fair" here implies what is stated more explicitly elsewhere in the corpus, that technology companies are shorting the hackers financially in private disclosure transactions. Similarly, VUPEN's Bekrar explains that one of the reasons for the genesis of his company was that vendors did not offer enough money to cover the costs of exploit development. So to Walton's point, on the spectrum from representationalist ethics to communitarian, the hackers fall toward the former.

It's also helpful to understand the supporting rhetorical tactics that feed into these larger strategies including: hackers and reporters using war analogies to sensationalize and exaggerate their premises (e.g., Soghoian's reference to vulnerability sellers being "merchants of death" selling "cyber bullets"; Netragard's references to less talented hackers trying to use squirt guns against tanks). Likewise, reporters citing the famous Stuxnet hack of a nuclear facility draws attention to the most extreme possible consequences of selling vulnerabilities. Though hacking is becoming an important part of real-world war strategy, by commonly imbuing actions like cyber vandalism, identity theft, and hacktivism with the same violent connotations as physically

shooting someone, offline and online dangers are conflated. Moreover, inflated cyberwar speculation departs from what prominent computer scientists calculate is currently possible at the national scale.

In the midst of all these verbal tactics, it's also important to think about motivation. Ultimately we can follow a trail of money that reveals each entity's interests: the reporters are intentionally crafting inflammatory headlines to draw in more page clicks, the technology companies are bolstering sales by protecting the perceived safety of their products, and the hackers want to be free to sell exploits to the NSA for six figures. Thus we are left with a carousel of blame that points fingers at the hackers for selling vulnerabilities, the technology companies for not paying enough and for having vulnerable software, and the reporters for sensationalizing the issue (Fig. 8). No one is innocent, but all are involved in shaping the ongoing ethical narrative. Understanding this narrative and its elements is the first step to empowering decision makers in these conflicts.

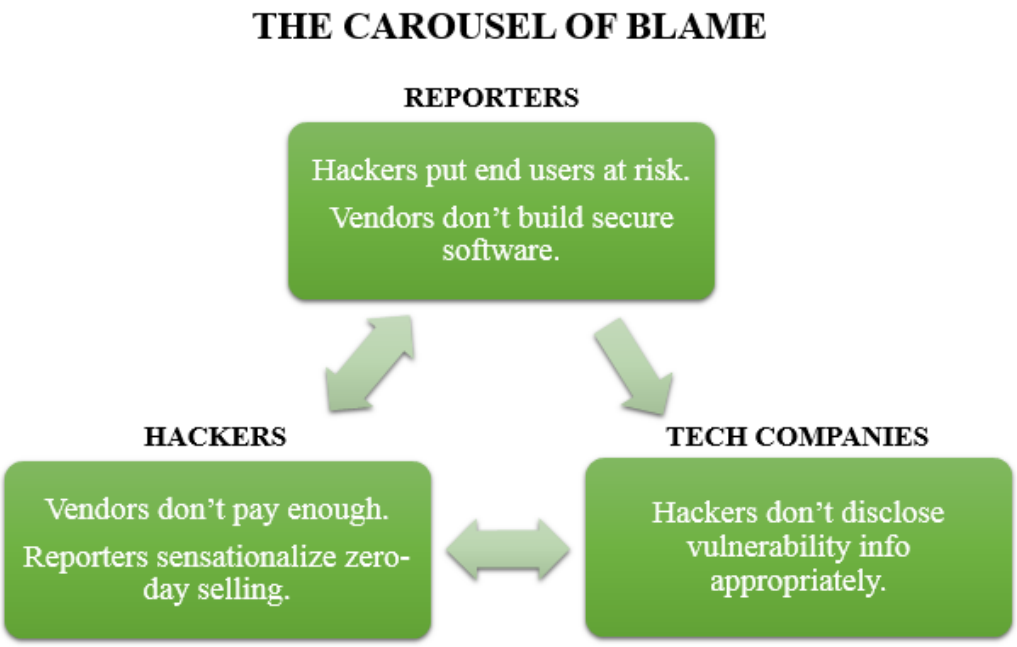

Figure 8 "The Carousel of Blame": All parties blame each other for any possible harm.

Ethos Construction in the Discourse

The millennium old Greek concept of ethos is also alive and well in the disclosure statements, blog posts, and reporter statements of this study. In order to argue for the *Greater Good*, it is necessary that IT professionals, reporters, and general consumers believe that each company is of sound character. Isocrates explains, "The man who wishes to persuade people will not be negligent as to the matter of character; no, on the contrary, he will apply himself above all to establish a most honourable name among his fellow-citizens; for who does not know that words carry a greater conviction when spoken by men of good repute than when spoken by men who live under a cloud" (56, line 278). Given all the negative press, vulnerability sellers must work to displace the dark cloud above their name, so ethos-building is vital to the survival of their business. This is also true for software companies who view vulnerabilities as black marks on their records; ethos-building becomes an essential function for maintaining their corporate image. As Yong-Kang Wei explains, it's helpful to think of corporate image in terms of a corporate "self" that is socially constructed or innate to a particular company (272). From this perspective, Isocrates' principle of establishing an honorable name is just as applicable to corporate selves as to individual selves. Wei goes on to explain that this corporate self is built largely through corporations' appeals to their own credibility and character.

Beginning with the technology companies, the most common way they build a positive image is by framing themselves as team players and collaborators (44 instances across all the companies). For example, in Google's disclosure policy statement it argues, "Working together helps make the online experience safer for everyone," tying collaboration to *Greater Good*. So instead of these companies focusing on the mea culpa of having vulnerabilities in their products,

one of their common positive messages is that they are adept at working with others in the industry to address security problems.

Another common ethos-building strategy across all the companies is explicitly stating that they are "committed to" security or "take it seriously" in their blog posts and disclosure statements. From here, the ethos construction strategies differ based on the companies' primary strengths. Though Microsoft focuses mainly on collaboration, Google calls for vendors to fix vulnerabilities quickly (developing its ethos as a speedy responder), IBM espouses companies building more secure software (an easier argument as it is not a major software producer), and HP emphasizes that it adheres to private disclosure in its Pwn2Own competition and when it finds problems in other vendors' software (drawing on its strength as a major vulnerability researcher).

With regard to the hacker companies, their ethos-building strategy most typically involves emphasizing their technical prowess. Instead of ostensibly asserting that they are not playing in a moral gray area, they choose to focus on being the best at what they do. This is akin to Aristotle's concept of amplification or *auxēsis* as a rhetorical strategy. He explains that amplification "aims to show superiority, and superiority is one of the forms of the honorable. Thus, even if there is no comparison with the famous, one should compare with the many, since superiority seems to denote excellence" (1.9 line 39). By comparing themselves to less skilled hackers, VUPEN and Netragard place themselves on the winning side of a particular argument; in a way, superiority translates into respect or nobility.

This self-praise strategy is also evident in Netragard's "whistle-blowing" blog post series, in which the company distinguishes itself from less skilled "script-kiddies." In this series, the company sets itself up as a "genuine" penetration testing firm, implying that others in the

industry are just *playing* at testing, whereas Netragard is in the adult league. One of the primary differentiators that the company frequently mentions is that it performs systematic manual testing, whereas other testers merely test customer systems with automatic scanners. It also juxtaposes itself with VUPEN, quoted in *TechWeek Europe* calling the company "irresponsible and unethical," to bolster its ethical position by comparison. Of course, VUPEN's Bekrar responded in true form on Twitter telling CEO Desautels to "Stop promoting yourself and your s**t by trolling about us, you don't know a s**t about us nor our customers, teenager," and equally poignantly, "We're a 100% research compny while u're just another broker compny without balls to do your own 0Ds. [*sic*]"

In this example, we can see that VUPEN devotes most of its energy not to dispelling the moral mists that surround its business, but to highlighting its skills and accolades. On its website and in its blog posts it frequently mentions its previous winnings of the Pwn2Own hacking competition. It also uses terms like "sophisticated" continuously when referring to its exploit development methods. Also worth noting, its blog posts, though mostly lacking in overt justification of its business, are a strategic ethotic move in and of themselves. VUPEN posts the technical details of some of its top exploits to demonstrate its skills and to proactively displace the community's reservations about the its legitimacy as a company. As Cheney and Christensen note, "In rhetorical terms, issue management means that the organization attempts to both "read" the premises and attitudes of its audience and work to shape them…the issue becomes a universe of discourse designed, managed, and ultimately, shaped by organizational rhetors and strategists in an attempt to shape the attitudes the audience hold toward the organization or its concerns" (16). In VUPEN's case, it defends its business model both proactively (through messaging, branding, and exploit technique blog posts) and reactively (answering *SecurityWeek's* criticisms

via podcast). The image that it wants to portray is of highly skilled, slightly dangerous hackers who nevertheless follow the law.

Though the hackers redefine the *Greater Good* to be their customer base, they still want to persuade the public that they aren't harming the everyday end user. The last thing that VUPEN and Netragard want is to be perceived as the bad guys in this debate, because corporate image is currency. For this reason, they frequently assert that their businesses are doing good in the long run by working with the good guys. For instance, VUPEN contends, "Exploits are used as part of lawful intercept missions and homeland security operations as legally authorized by law…to protect lives and democracies against both cyber and real world threats." In such arguments, they are intentionally drawing a link between themselves and the indisputable good guys, the authority figures. They must prove that though they aren't cooperating with the technology companies, they carefully vet their customers.

We see this principle on a repeated basis in the *We Only Sell To* code, which appeared 11 times in the reporter corpus as associated with the hacker code, four times in the Netragard corpus, and four times in the VUPEN corpus. In Netragard's case, it reminds the public frequently that it only sells domestically and it condemns VUPEN for its international transgressions. On the other hand, VUPEN emphasizes that it only sells to NATO partners and doesn't work with countries under embargo.

Conclusion

In the cybersecurity sphere, the vulnerability-selling debate is an example of a timely, situated, evolving discourse. In the end, my investigation has implications for various audiences that need to better understand the framing of this topic: policymakers creating new online security legislation, reporters attempting to accurately frame the debate, and professionals in the information technology and security fields whose livelihoods and daily tasks are affected by these evolving social norms. Studies like these can illuminate some of the primary rhetorical strategies of such debates.

Instead of approaching the whole debate for a left-to-right view, future research could go deeper, conducting a comprehensive study of one group like the hacker companies and include additional players like ReVuln or Exodus Intelligence. Additionally, to help lawmakers, more research is needed in the computer science field to determine the real risks of selling vulnerabilities, i.e., tracking them after their sale to see if they ultimately become public or "fall into the wrong hands," as was so often argued by reporters.

As the conversation continues, in some respects we may see the opposing sides come closer together. The technology companies have already begun to eschew the term "responsible" when attached to disclosure, recognizing its polarizing nature. They have also begun to offer contests and increasingly lucrative bounty programs to incentivize cooperation between money-minded hackers and themselves (e.g. Google, PayPal) (Kirsch 386). Additionally, some vulnerability sellers have left the market. A 2014 *Forbes* story chronicled Endgame Systems' move out of the vulnerability-selling business. The article quotes the company's new CEO, Nate Fick, noting, "The exploit business is a crummy business to be in… If we're going to build a top-tier security firm, we have to do things differently." Public rhetoric has clearly exerted pressure

on Fick and others like him, but whether companies like VUPEN react to these ethical discourses remains to be seen. Despite the strides toward making white hat hacking more lucrative, hacker companies can still make decidedly more by selling exploit subscription packages to government buyers. This economic dynamic encourages hacker collectives to stay in the bug market long term. Consequently, as evolving regulation has the most potential to impact the actions of these passionate gray hat hackers, discursive studies like this one, combined with pragmatic risk-assessment and legal scholarship, are the best avenues to help lawmakers decide whether regulation is practical or necessary in this heated debate.

Works Cited

Aristotle, and George A. Kennedy. *On Rhetoric: A Theory of Civic Discourse.* New York: Oxford University Press, 1991. Print

Arora, Ashish, Nandkumar, Anand, and Rahul Telang. "Does Information Security Attack Frequency Increase with Vulnerability Disclosure? An Empirical Analysis." *Information Systems Frontiers* 8.5 (2006): 350–362. Web. 5 Apr. 2014.

Arquilla, John. "Twenty Years of Cyberwar." *Journal of Military Ethics* 12.1 (2013): 80-7. Web. 18 May 2015.

Arquilla, John and Ronfeldt, David (1993) "Cyberwar Is Coming!" *Comparative Strategy*, 12.2 (1993): 141-165. Print.

Barton, Ellen. "Further Contributions from the Ethical Turn in Composition/Rhetoric: Analyzing Ethics in Interaction." *College Composition and Communication* 59.4 (2008): 596–632. Web. 14 Apr. 2014.

Berlin, James. "Rhetoric and Ideology in the Writing Class." *College English* 50.5 (1988): 477-494. Web. 17 Apr. 2014.

Bendrath, Ralf. "The Cyber-war Debate: Perception and Politics in U.S. Critical Infrastructure Protection." *Information & Security* 7.1 (2001): 80–103. Web. 5 Apr. 2014.

Benoit, William. "Isocrates and Aristotle on Rhetoric." *Rhetoric Society Quarterly* 20.3 (1990): 251-9. Web. 10 Mar. 2015.

Blank, Laurie. "Cyber War/Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace." *Cyberwar: Law & Ethics for Virtual Conflicts*. Eds. Jens David Ohlin, Kevin Govern, and Claire Finkelstein. Oxford University Press, 2014. Web. 25. Mar. 2015.

Blythe, Stuart. "Coding Digital Texts and Multimedia." *Digital Writing Research.* Ed. Heidi McKee and Danielle DeVoss. New York: Hampton Press, 2007. 204-226. Print.

Brinton, Alan. "Ēthotic Argument." *History of Philosophy Quarterly* 3.3 (1986): 245-58. Web. 10 Mar. 2015.

Brito, Jerry and Tate Watkins. "Loving the Cyber- Bomb? The Dangers of Threat Inflation in Cybersecurity Policy." *SSRN Working Paper Series,* 2011. Web. 5 Apr. 2014.

Cheney, George, and Lars Thøosger Christensen. "Organizational Identity: Linkages Between Internal and External Communication." *The New Handbook of Organizational Communication.* Ed. Fredric M. Jablin and Linda L. Putnam. Thousand Oaks, CA: SAGE Publications, Inc., 2001. 231-70. Web. 5 Mar. 2015.

Clarke, Roger. "Categories of Malware." *Roger Clark's Website.* Xamax Consultancy Pty Ltd., 21 Sept 2009. Web. 5 April 2014. <http://www.rogerclarke.com/II/MalCat-0909.html>.

Corbin, Juliet, and Anselm Strauss. "Grounded Theory Research: Procedures, Canons and Evaluative Criteria." *Zeitschrift für Soziologie* 19.6 (1990): 418-27. Web. 23 Mar. 2015.

de Graaf, Gjalt. "Discourse and Tractable Morality." *Handbook of the Philosophical Foundations of Business Ethics.* Dordrecht: Springer Netherlands, 2013. 581-602. Print.

"Definition of a Security Vulnerability." *Microsoft Developer Network.* Microsoft, 2015. Web. 18 May 2015.

Driver, Julia. "The History of Utilitarianism." *Stanford Encyclopedia of Philosophy*. The Metaphysics Research Lab, Center for the Study of Language and Information, 22 Sept. 2014. Web. 21 Mar. 2015.

Dunn Cavelty, Myriam "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of

the US Cyber—Threat Debate." *Journal of Information Technology & Politics* 4.1 (2007): 19-36. Web. 5 Apr. 2014.

Duska, Ronald F. "Why Business Ethics Needs Rhetoric: An Aristotelian Perspective." *Business Ethics Quarterly* 24.1 (2014): 119-34. Web. 10 Mar. 2015.

DelReal, Jose. "Eyes Turn to the Next Congress as Sony Hack Exposes Cybersecurity Flaws." *Washington Post.* The Washington Post, 18 Dec. 2014. Web. 19 Dec. 2014.

Engward, Hilary. "Understanding Grounded Theory." *Nursing Standard* (Royal College of Nursing (Great Britain): 1987) 28.7 (2013): 37-41. Web. 23 Mar. 2015.

"Feinstein Releases Draft Cybersecurity Information Sharing Bill." *Diane Feinstein United States Senator for California.* Internet Archive Way Back Machine, 17 June 2014. Web. 19 Dec. 2014.

Foss, Sonja. "Metaphoric Criticism." *Rhetorical Criticism: Exploration and Practice.* 2nd ed. Prospect Heights, IL: Waveland Press, 1996. 357-367. Print.

Frei, Stefan. "The Known Unknowns: Empirical Analysis of Publicly Unknown Security Vulnerabilities." *NSS Labs, Inc.* (2013): 6-14. Web. 5 May 2014. <https://www.nsslabs.com/reports/known-unknowns-0>.

Glaser, Barney G., and Anselm L. Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. New Brunswick, N.J: Aldine Transaction (a division of Transaction Publishers), 2006. Web. 22 Mar. 2015.

Greenberg, Andy. "Inside Endgame: A Second Act For The Blackwater Of Hacking." *Forbes.* Forbes.com, 3 Mar. 2014. Web. 30 Mar. 2015.

Helmreich, Stefan. “Flexible Infections: Computer Viruses, Human Bodies, Nation–States, Evolutionary Capitalism.” *Science, Technology, & Human Values* 25.4 (2000): 472–491. Web. 5 Apr. 2014.

Holt, Robert J. “Social Media and the ‘Perpetual Project’ of Ethos Construction.” *Young Scholars in Writing: Undergraduate Research in Writing and Rhetoric.* 10 (2013): 72-80. Web. 10 Mar. 2015.

Isocrates. “Antidosis.” *Readings from Classical Rhetoric.* Ed. Patricia Matsen, Phillip Rollinson, and Marion Sousa. Carbondale: Southern Illinois University Press Carbondale, 1990. 47-56, line 278. Web. 19 Mar. 2015.

Johnson, Lauren. “Adapting and Combining Constructivist Grounded Theory and Discourse Analysis: A Practical Guide for Research.” *International Journal of Multiple Research Approaches* 8.1 (2014): 100-16. Web. 10 Nov. 2014.

Kan, Paul Rexton. “Cyberwar to Wikiwar: Battles for Cyberspace.” *Parameters* 43.3 (2013): 111. Web. 18 May 2015.

Kirsch, Cassandra. “The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law.” *Northern Kentucky Law Review* 41.3 (2014): 383. Web. 18 May 2015.

Lawson, Sean. “Putting the ‘War’ in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States.” *First Monday* 17.7 (2012): n. pag. *firstmonday.org*. Web. 30 Mar. 2014.

Leff, Michael. “Perelman, Ad Hominem Argument, and Rhetorical Ethos.” *Argumentation* 23.3 (2009): 301-11. Web. 10 Mar. 2015.

Leyden, John. “Apple Lags MS in Security Response: Fear of a Black Hat.” *The Register.* 31 March 2008. Web. 31 Aug. 2014.

Libicki, Martin C. *Conquest in Cyber-space: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007. Print.

"The National Security Agency (NSA) Controversy: Timeline." *Discover the Networks: A Guide to the Political Left*. DiscoverTheNetworks.org, 17 Mar. 2014. Web. 12 Jan. 2015.

Maurushat, Alana. "Discovery and Dissemination of Discovering Security Vulnerabilities." *Disclosure of Security Vulnerabilities*. London: Springer, 2013. 21–33. Web. 2 Apr. 2014.

Rein, Martin and Schön, Donald. "Reframing Policy Discourse." Ed. Frank Fischer and John Forester. *The Argumentative Turn in Policy Analysis and Planning*. Durham, N.C: Duke University Press, 1993.

Rickert, Thomas. "Tarrying with the <head> : The Emergence of Control through Protocol." *From A to <A>: Keywords of Markup.* Eds. Bradley Rilger and Jeff Rice. Minneapolis, MN: The Regents of the University of Montana, 2010. 1-20. Print.

Rid, Thomas. "Think Again: Cyber-war." *Foreign Policy.* FP Group, 27 Feb. 2012. Web. 3 Apr. 2014.

Riley, Brendan. "A Style Guide to the Secrets of <style>. *From A to <A>: Keywords of Markup.* Eds. Bradley Rilger and Jeff Rice. Minneapolis, MN: The Regents of the University of Montana, 2010. 67-80. Print.

Rouse, Margaret. *SearchSecurity.com.* TechTarget, 2015. Web. 18 May 2015.

Saldaña, Johnny. *The Coding Manual for Qualitative Researchers.* 2nd ed. London: Sage Publications LTD, 2013. 246-260. Print.

Schneider, Elizabeth M. "Feminism and the False Dichotomy of Victimization and Agency (the

Sex Panic: Women, Censorship and "Pornography")." *New York Law School Law Review* 38.1-4 (1993): 387. Web. 21 Mar. 2015.

Tavini, Herman. *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology.* Hoboken, NJ.: John Wiley & Sons, Inc., 2004. Print.

"VUPEN Exclusive and Sophisticated Exploits for Offensive Security." *VUPEN Security*. VUPEN Security, n.d. Web. 14 Mar 2014.

Walton, Clarence. *Ethos and the Executive: Values in Managerial Decision Making*. Englewood Cliffs, N.J: Prentice-Hall, 1969. Print.

Wang, Jingguo, Nan Xiao, and H. Raghav Rao. "Drivers of Information Security Search Behavior: An Investigation of Network Attacks and Vulnerability Disclosures." *ACM Transactions on Management Information Systems* 1.1.3 (2010): 19-21. Web. 5 April 2014.

Wei, Yong-Kang. "Corporate Image as Collective Ethos: A Poststructuralist Approach." *Corporate Communications: An International Journal* 7.4 (2002): 269-76. Web. 5 Mar. 2015.

"Zero-Day Exploit Acquisition Program." *Netragard.com*. n.d. Web. 31 Aug. 2014.