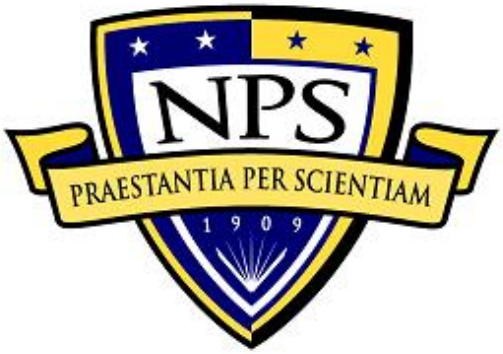
2019-03

ZERO DAYS, ONE OBLIGATION

Akil, Anthony

Monterey, CA; Naval Postgraduate School



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ZERO DAYS, ONE OBLIGATION

by

Anthony Akil

March 2019

Thesis Advisor:	Wade L. Huntley
Second Reader:	David M. Tully

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2019	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE ZERO DAYS, ONE OBLIGATION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Anthony Akil	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis set out to apply the moral principle of utilitarianism to the policy problem associated with zero-day vulnerabilities. These vulnerabilities can be understood as errors in coding that are potentially exploitable and unknown to either the creators or users of the software. If attack vectors related to zero-day vulnerabilities are completely dependent upon correctable coding errors, what should policy require when the U.S. government detects a zero-day vulnerability? Should it be disclosed publicly so it can be patched or restrict knowledge of it so it can be weaponized? This thesis applied revisionist John Stuart Mill's unique and nuanced description of utilitarianism to the Vulnerabilities and Equities Policy and Process (VEP) to evaluate what aspects of the policy fulfilled Mill's moral code and what areas could be improved. The improvement recommendation is made on strictly moral terms. This thesis acknowledges while moral policy has undeniable benefits, there are times where the moral can come at the expense of the strategic, and national interests can be compromised. Ultimately, much like the VEP, this thesis recommends balance.

14. SUBJECT TERMS zero-day vulnerabilities, vulnerability and equities policy and process, utilitarianism, moral obligation, USG policy	**15. NUMBER OF PAGES** 85
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ZERO DAYS, ONE OBLIGATION

Anthony Akil
Lieutenant, United States Navy
BA, University of Washington, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2019

Approved by: Wade L. Huntley
Advisor

David M. Tully
Second Reader

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis set out to apply the moral principle of utilitarianism to the policy problem associated with zero-day vulnerabilities. These vulnerabilities can be understood as errors in coding that are potentially exploitable and unknown to either the creators or users of the software. If attack vectors related to zero-day vulnerabilities are completely dependent upon correctable coding errors, what should policy require when the U.S. government detects a zero-day vulnerability? Should it be disclosed publicly so it can be patched or restrict knowledge of it so it can be weaponized? This thesis applied revisionist John Stuart Mill's unique and nuanced description of utilitarianism to the Vulnerabilities and Equities Policy and Process (VEP) to evaluate what aspects of the policy fulfilled Mill's moral code and what areas could be improved. The improvement recommendation is made on strictly moral terms. This thesis acknowledges while moral policy has undeniable benefits, there are times where the moral can come at the expense of the strategic, and national interests can be compromised. Ultimately, much like the VEP, this thesis recommends balance.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AI	artificial intelligence
CCI	Office of the Coordinator for Cyber Issues
CIA	Central Intelligence Agency
CED	Committee for Economic Development
DDoS	distributed denial of service
DHS	Department of Homeland Security
DISRF	Doctrine of Information Security of the Russian Federation
DNSSR	Defence and National Security Strategic Review
DoC	Department of Commerce
DoD	Department of Defense
DoE	Department of Energy
DoJ	Department of Justice
DoS	Department of State
EFF	Electronic Frontier Foundation
E.O.	executive order
ERB	executive review board
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
HE	hacker ethic
HPSD	Homeland Security Presidential Directive
H.R.	house resolution
IAD	Information Assurance Directorate
IL	international law
IP	intellectual property
NCIJTF	National Cyber Investigative Joint Task Force
NDA	non-disclosure agreement
NPSD	National Security Presidential Policy Directive
NSA	National Security Agency
NSC	National Security Council

NSCR	National Security Strategy Capability Review
NSS	National Security Strategy of the United States
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PRC	People's Republic of China
RF	Russian Federation
SASC	Senate Armed Services Committee
SMB	server message block
SSL	secure socket layer
TAO	tailored access operations
UK	United Kingdom
UN	United Nations
USG	United States Government
VEP	Vulnerabilities and Equities Policy and Process
VEP17	Vulnerabilities and Equities Policy and Process 2017

ACKNOWLEDGMENTS

While the journey was long and disjointed, fraught with rabbit holes and ill-conceived drafts, at the end, it was rewarding and fruitful. It was a journey that would not have enjoyed an ultimately favorable conclusion without the insightful guidance and inexhaustible patience of Dr. Wade Huntley. I sincerely thank him for his steadfast support even when my own focus waned. Additionally, I want to thank Katherine Egerton of the Graduate Writing Center. From the first meeting with Kate, I was immediately impressed with her insightful and constructive criticism. Her great work was rewarded with more of my drafts, mostly because I considered the meetings as enjoyable as they were edifying. Finally, I would like to thank my Ma, well … for obvious reasons ☺. I suppose I could express some gratitude for the Old Man as well. And Bro, there's no denying your pep talks kept me focused on the home stretch.

THIS PAGE INTENTIONALLY LEFT BLANK

I. GROUND ZERO

A. THE PROBLEM

There is a debate surrounding zero-day vulnerabilities and the exploits associated with them. A variety of attack vectors exist in cyberspace: spearfishing exploits human gullibility through email, brute force techniques like Distributed Denial of Service (DDoS) can overwhelm servers, and some less technical approaches simply take advantage of predictable or lackadaisical security practices. The attack vector, ominously referred to as a zero-day weapon, is something different. Zero-days weapons are not inherently violent, rather they represent the exploitation of an error in a program's coding. The error in coding is the vulnerability. Research scientists at RAND in their *The Defender's Dilemma* defined zero-days as, "those vulnerabilities for which no patch or fix has been publicly released" (Libicki, Ablon, & Webb, 2015, p. 44). An attack utilizing a zero-day weapon exploits the coding vulnerability. If a patch does not exist, no protection is available, and the zero-day weapon effectively becomes a cyber-silver bullet.

This thesis applies the moral principle of utilitarianism to the policy problem associated with zero-day vulnerabilities. That problem, simply put, is this: what should U.S. policy require when the U.S. Government (USG) detects a zero-day vulnerability on its own? Should the USG disclose the vulnerability information, to alert exposed users and prompt the software vendor to patch it, or should the USG retain private knowledge of the vulnerability, to exploit it for its own espionage or cyber operations? There is no simple answer to these questions. A number of factors must be considered: the benefits of disclosure versus restriction as well as how each option would affect USG stakeholders, public interest in cybersecurity, USG relationships with industry, and USG relationship with foreign countries. Essentially, zero-day policy must strike a balance. The USG recognized as much and released the Vulnerabilities and Equities Policy and Process (VEP), which seeks to make a consensus based decision regarding disclosure versus retention. In addition to the variety of stakeholders affected, there are a number of viewpoints to consider: moral, expedient, and strategic are but a few. This thesis is interested in analyzing the policy in moral terms. Specifically, this thesis addresses the

question: how would the moral principle of utilitarianism evaluate and inform the Federal Government's zero-day policy?

If a nation has numerous zero-day weapons in its arsenal, it also essentially has a long list of exploitable vulnerabilities. After all, the nation would not choose to weaponize the vulnerability if it could not produce a worthwhile effect, an effect that although advantageous for the user, is detrimental and dangerous for the victim. The problem is that nothing stops other nations from detecting and weaponizing the same vulnerability, which means one's own nation may also be the potential victim. Instead of exploiting and weaponizing the vulnerability, the nation could opt to notify the software manufacturer and recommend they patch the vulnerability. The threat would then be eliminated, but so would any usefulness from the zero-day.

Zero-day weapons create a trade-off situation for nations. They gain current and potential operational value, but make their citizens and infrastructure reliant on the associated software vulnerable to attack. While this trade-off can be evaluated in purely strategic terms, democratic governments are also concerned about the ethical basis for their policymaking. How can the U.S. government (USG) make ethical determinations about the retention of zero day weapons? This paper is concerned with answering that question, and uses the moral principle of utilitarianism to evaluate USG zero-day policy. Specifically, this thesis uses utilitarianism as defined by John Stuart Mill to establish the moral obligation of a nation-state in general. It then assesses the USG's zero-day policy in terms of Mill's moral principle to determine if the ethical duty is met.

B. WHY IT MATTERS

The last five years consisted of several high-profile and unflattering incidents involving cybersecurity and the USG. Many of these have drawn public attention to the government's retention of zero-day weapons. Edward Snowden leaked classified information allowing the press to publish 7,000 Top Secret classified documents, many of which exposed information about these capabilities. (Szoldra, 2016). The CIA was embarrassed by WikiLeaks (Smith, 2007). The NSA was suspected of involvement in HeartBleed (Sanger & Perlroth, 2014; Whittaker, 2014; Lee, 2014; Zetter, 2014), which

the USG denied (Daniel, 2014). The NSA was unable to deny involvement in the WannaCry ransomware attack (Holland, 2017). The FBI also engendered its fair share of zero-day vulnerability controversy with its actions related to the Playpen sting as well as cracking the iPhone of the San Bernardino shooter (Tierney, 2017; Zapotsky 2016).

These represent only the more high-profile incidents. Each of these incidents, some discussed in more detail in this thesis, resulted in part because the secrecy required for management of these cyber capabilities places management decisions in the hands of government agencies that are not necessarily considering all of the factors that may be relevant to U.S. national security and public interest. Such incidents affect not only the U.S. standing in the world, but perceptions of the U.S. government by the American people. That is to say, as more and more incidents occurred over a short period the American public's trust in their government on cybersecurity issues waned.

There are a number of factors that contribute to the legitimacy of government. Trust is one of them, transparency is another. An issue related to zero-day vulnerabilities, and cyber operations in general, is that many related aspects are almost always classified. Transparency is rarely if ever an option. The effective negation of transparency puts a premium on trust. If the USG utilizes a zero-day policy that conforms to a moral standard or revises their current policy to align with a moral standard, that will build trust and increase USG legitimacy in the eyes of the American public. This thesis evaluates whether the VEP is a step forward in this regard. Clear policy is as necessary as it is useful (Committee for Economic Development, 2017). If clear policy is always in need and the adoption of morality builds trust, then Mill's moral philosophy seems like the ideal foundation from which that policy could be formed, and that is why this thesis question matters.

C. LITERATURE REVIEW

This literature review addresses three primary questions: has the principle of utilitarianism already been applied to zero-day policy, what other principles or theories have been applied to zero-day policy aside from morality, and how have ethical standards in general been applied to issues in cyberspace? The section on cyberethics addresses five

major areas of concern: privacy, intellectual property, hacking, rule of law, and international law and cyberwarfare. The literature review can be best understood as a series of concentric and overlapping circles, with each circle representing an area of concern for the thesis, as the circles move farther from the center, the topic issue related to the thesis question broadens.

1. Zero Utility

One of the few instances of morality being applied to the zero-day debate was a post written by Michael Daniel while he served as the White House Cyber Security Coordinator. Mr. Daniel wrote the piece in response to Heartbleed, which was particularly problematic for the USG. The news cycle overflowed with claims that the USG had prior knowledge of Heartbleed, and could have stopped it from ever happening, had the vulnerability been disclosed (Sanger & Perlroth, 2014; Whittaker, 2014; Lee, 2014; Zetter, 2014). Mr. Daniel's post endeavored to both deny the accusations and to provide the concerned public with insight into how the USG decides retention or disclosure.

Daniel (2014) acknowledged there is no official policy nor are there hard and fast rules, but provided a list questions he needed answered before making the decision to retain. Many of the questions were derivative of familiar over-arching policy considerations like magnitude of need, potential value of intelligence earned, alternative options, and risk assessment. One question introduced the notion of morality into the zero-day decision. "How much harm could an adversary nation or criminal group do with knowledge of this vulnerability" (Daniel, 2014). A prevailing theme throughout moral philosophy is the do no harm principle. Although no moral theory was explicitly mentioned, Mr. Daniel's expression of an unwillingness to harm others provides an example of moral consideration being used in reference to zero-day policy.

This thesis is interested in developing Mr. Daniel's inchoate moral concerns through the application of the utilitarian moral principle; to explore how, if at all, utilitarianism would change the way the USG looks at the question of disclosure versus retention.

2. Zero and What Else?

RAND Corporation published *The Defender's Dilemma* and *Zero Days, Thousands of Nights,* providing two examples of a quantitative approach to the zero-day problem. In *The Defender's Dilemma,* Libicki, Ablon, and Webb applied the concept of white, gray, and black markets to zero-day vulnerabilities: "White-market buyers turn their purchases over to the vendor so that they can be fixed. Gray-market buyers tend to work for government or intelligence agencies. Black-market buyers use vulnerabilities for crime" (Libicki, Ablon, & Webb, 2015, p. 44). Libicki, Ablon, and Webb provided a detailed explanation on how the markets interact and affect prices in each other. White market programs like "bug bounties" and the "Zero Day Initiative" provide incentives for responsible disclosure and have potential move vulnerabilities into the white market and out of the more dangerous black market (Libicki, Ablon, & Webb, 2015). *The Defender's Dilemma* speaks more to how to deal with the existence of zero-days, as opposed to what a nation should do when they discover one. It provides methods to move zero-days away from criminal elements and towards nation-states.

In *Zero Days, Thousands of Nights,* Ablon and Bogart (2017) were concerned with the policy debate surrounding zero-days and examined how to make the determination regarding retention and disclosure based on the analysis of a 200 zero-day dataset. They used an algorithm primarily concerned with collision rates. A collision occurs when researchers, independent from each other, detect the same vulnerability (Ablon & Bogart, 2017). Effectively, a collision could be considered overlap. Ablon and Bogart (2017) maintained overlap, from a purely cost/benefit perspective, makes the disclosure versus retention decision fairly simple. Vulnerabilities suspected of having a high level of overlap should be disclosed and patched and ones believed to have low collision rates should be retained (Ablon & Bogart, 2017). The mechanical nature of the overlap-based decision can make it very appealing. However, Ablon and Bogart advised considering additional factors: "The decision to stockpile requires careful consideration of several factors, including the vulnerability itself, its use, the circumstances of its use, and other options that may be available to achieve an intended outcome" (Ablon & Bogart, 2017, p. XIV).

Ablon and Bogart's work provides, quite possibly, the most exhaustive mathematical guidance for how to make the release or retain decision, but stops short considering or even introducing an ethical consideration. This thesis seeks to determine how a moral principle can augment their assessment.

Bruce Schneier (2014), in an article for *the Atlantic,* provides an example of a differing qualitative approach. He also brought up the notion of collision rates and overlap but differed with Ablon and Bogart regarding their significance.

> If vulnerabilities are sparse, then it's obvious that every vulnerability we find and fix improves security. We render a vulnerability unusable, even if the Chinese government already knows about it. We make it impossible for criminals to find and use it. We improve the general security of our software, because we can find and fix most of the vulnerabilities. (p. 1)

Schneier seems to believe if vulnerabilities are sparse and the decision should be to disclose, each patch brings us closer to total software security, whereas if vulnerabilities are plentiful patching actually does little to increase security. Schneier, a lawyer, concluded the article making a case for choosing disclosure over retention, but allowed for exceptions to be made. "No matter what cybercriminals do, no matter what other countries do, we in the U.S. need to err on the side of security and fix almost all the vulnerabilities we find. But not all, yet" (Schneier, 2014). Schneier provided a judgement based interpretation of the quantitative approach analyzed by Ablon and Bogart, but there is no express indication that judgement can be attributed to an ethical principle. This thesis will introduce an ethics-based judgement to the zero-day decision.

3. Morality and Cyberspace

While a wealth of literature exists on morality and cyberspace, the majority of the works coalesce around more or less the same topics: privacy, hacking, intellectual property (IP), and rule of law. Additionally, this section will review nation-states' efforts to address cyberspace, cyberwarfare, and the significance of international law. Pieces related to information ethics tend to include a brief meta-ethical overview of morality, then proceed to list and define a handful of the more common first order normative moral philosophies.

For the purposes of this section, the specific moral principle is not as important as how morality, in general, was applied.

a. Privacy

There is near universal agreement that privacy is a core element of security and ought to be protected and preserved (Moore, 1997; Kang, 1998; Michelfelder, 2001; Tavani & Moore, 2000; Nissenbaum, 1997; Lessig, 2006). Cyberspace provides speedy access to a conveniently located marketplace, but also allows for the quick and convenient retrieval of personal information, creating uniquely paradigmatic ethical problems (Moore, 2001). On a daily basis, an individual conducts a myriad of transactions on the Internet, "but the very technology that enables these transactions also makes detailed, cumulative, invisible observation of our selves possible. The potential for wide-ranging surveillance of all our cyber-activities presents a serious threat to information privacy" (Kang, 1997, p. 1193). Individuals wary of unscrupulous actors on the web fear overvaluing privacy enables charlatans and fraudsters. Kang (1997) asserts this is not the case, "it can do so only if both the nature of the relationship between the individual and the information user, and the ethical or legal duties of disclosure inherent to that relationship, command an openness that information privacy prevents" (p. 1220). Overall, the problem with cyberspace is more information is gathered per transaction than any need-to-know principle can ethically justify (Kang, 1997).

Protections exist to protect privacy on the web. Legal protections with respect to privacy and cyberspace should be increased and derive their moral justification from the values of personal liberty and autonomy of decision-making (Michelfelder, 2001). Legal protection for privacy should be afforded to prevent unethical aggregate information collection in a public forum (Nissenbaum, 1997). In addition to legal protections, technological protections for privacy are available. Although still valuable, the consumer must use Privacy Enhancing Technologies (PET) with caution. Cookies present an ethical concern as some users are unaware of their significance and can be coerced or tricked into allowing them while having their access throttled or restricted if they block them (Tavani & Moore, 2000).

The fundamental concerns of privacy and cyberethics can be distilled to enhance the understanding of the zero-day debate. One of the major concerns of privacy and cyberspace is the unethical overstepping of boundaries by the sovereign, that is to say, the nation putting its interests ahead of the people. A similar concern is shared by critics of exploiting versus patching zero-day vulnerabilities. This thesis is interested in building upon current lessons of cyberethics and privacy to determine how the adoption of a utilitarian ethical standard would affect USG zero-day policy.

b. Intellectual Property

While privacy is concerned with a sovereign's unethical encroachment, intellectual property (IP) rights are concerned with the sovereign's unethical judgement. Some professionals, like Shelly Warwick, question whether or not the protections provided to IP are ethical in the first place. Although initially created to benefit both the creator and the general public, copyright law has dramatically shifted in favor of the creator as a policy decision, not a moral decision, and should no longer be considered ethical (Warwick, 2001). The advent of the Internet has transposed this issue over cyberspace, with the web's free flow of information making an already contentious situation worse: "The quarrel is between those who think that the Internet upholds the right to information and those who see it as a representative of the right to profit from intellectual goods" (Guha & Chatterjee, 2010, p. 253). Guha and Chatterjee (2010) believe that information is power and access to the free flow of information should be seen as a basic human right. It is immoral to deprive people of basic human rights. They contend if IP rights are used to inhibit the free flow of information while promoting excessive profiting, then IP rights are immoral.

Kimppa (2005) attempts to invalidate the current moral justification of IP rights by claiming the three most common normative moral philosophies, Lockean liberalism, utilitarianism, and deontology have all been misappropriated and at times redefined to unjustly validate IP rights. Specifically, regarding utilitarianism, "the 'as much good as possible' seems to have been misunderstood and the 'to as many as possible' seems to have been forgotten or has been claimed to be irrelevant" (Kimppa, 2005, p. 59). Intellectual property rights are not inherently immoral because the creator has a right to compensation

but, if the gap between the rich and poor is to be bridged and the intent is for all to stand on equal footing, then IP rights must be changed to encourage the free flow of information rather than profit (Guha & Chatterjee, 2010; Kimppa, 2005).

Bruno de Vuyst and Alea Fairchild are more sympathetic to IP rights, while Richard Spinello strongly advocates on their behalf. Bruno de Vuyst and Alea Fairchild (2005) contend that if IP rights are written in such a fashion as to facilitate excess rent-taking, they provide less value to society and therefore become unethical. Although the free flow of information facilitated by cyberspace is considered a boon by many, they advise wariness. Bruno de Vuyst and Alea Fairchild (2005) believe creators should not succumb to new temptations facilitated by cyberspace, as IP rights, if written equitably, can be ethical, while excessive rent-seeking is always immoral. Spinello (2007) maintains that not only are IP rights ethical, certain groups have used the advent of cyberspace to unethically and deliberately misinterpret the law. Spinello (2007) provided the example of the misapplication of the "fair use" principle by Napster when they claimed peer-to-peer networks constituted fair use.

Cyberspace has managed to add new ethical dimensions to debates over IP rights, while exacerbating already existing ones. The ethics of IP rights seem to boil down to the familiar battle of private versus public. IP rights are concerned with striking a balance between compensation for creator and value for society, while ultimately, the zero-day day decision is concerned with striking a balance between defensive value and offensive worth. The balancing of needs served is exactly what utilitarianism strives to do. If both parties are satisfied the greatest good is achieved, and that is precisely what the moral principle prescribes. This thesis seeks to further develop this notion of ethical balancing of needs, through the application of utilitarianism, to the zero-day decision.

c. Hacking

One of the most divisive topics in cyberethics is hacking. In *Hackers: Heroes of the Computer Revolution,* Steven Levy firmly entrenched himself in the proponent camp. Levy seemed to consider hackers equal parts libertarian and egalitarian. Levy (1984) claimed hackers believed in the free flow of information, harbored a mistrust of authority,

and a contempt for bureaucracy; he made the world aware of hackers attempt to codify these sentiments into a moral standard dubbed the "Hacker Ethic" (HE). Some were not as receptive to the adoption of an ethical code in cyberspace. An effort should be made to discourage any standard code to govern cyberspace, instead cyberspace should operate with variable ethics (Kirwan & Power, 2012). The concept is not to be confused with moral relativism. Each community in cyberspace will create its own moral code. Whether one is better or worse is a matter of preference. Consequently, a form of ethical pluralism can occur in cyberspace. This is variable ethics. (Kirwan & Power, 2012)

Opponents of hacking believe hackers partake in fundamentally immoral behavior and greet any notion of a HE with incredulous disbelief. One of the problems with hackers is their disregard for private space, just like there are places you do not belong in real space, there are places you do not belong in cyberspace (Spinello, 2000). Kirwan and Power (2012) remind the reader if an individual circumvented security at the White House, rifled through important documentation, but did not actually steal anything the behavior is still unethical and illegal. Cees Hamelink, in *The Ethics of Cyberspace,* provided instances where characterizing the morality of hacking is not as cut and dry: "It becomes more complicated when hackers contend to enter systems with constructive intentions: to demonstrate that the security is not foolproof" (Hamelink, 2000, p. 33).

Some believe hacking has political and social activist elements in addition to moral considerations. Thus, the term hacktivist was created. These advocates saw hackers and hacktivism as way to push back against capitalistic and conservative influence (Friesinger, Grenzfurthner, & Ballhausen, 2010). The notion of a "civic hacker" was also created. Civic hackers should be considered utopian realists, capable of wielding algorithmic power and shaping the ethics of technologic design (Schrock, 2016). Whittaker (2004) discusses the ethical nature of both hacking and hacktivism through an analysis of the "Hacker Ethic," as expressed in the *Hacker Manifesto* and the *Genocide2600 Manifesto.* Whittaker (2004) was contemptuous of both manifestos, referring to them as "infantile" and calling attention to what he considered "laughable" hypocrisies. He had higher regard for the HE but still remained critical. Whittaker believed the HE was "essentially a libertarian and individualist

code, a particular brand of anarchy that, at its best, fulfils some of the promises made by corporate capitalist meritocracy that are rarely achieved outside cyberspace" (2004, p. 22).

The debate surrounding the morality of hacking seems contingent upon cyberspace remaining free and open. As sovereign power in cyberspace grows, and rules and regulations experience a commensurate increase, the discussion relating to hacking and morality will likely evolve. The concern for morality may be replaced with the concern for legality. Although hacking and information ethics do not readily reduce to a useful zero-day parallel, hackers are directly involved in the discovery of zero-day vulnerabilities. Knowing their ethos can prove useful when crafting zero-day policy. An understanding of hacking ethics may help policymakers avoid drafting doctrine that perturbs the moral code of the group most likely to both detect vulnerabilities and weaponize associated exploits.

d. Rule of Law

No issue in cyberethics more directly applies to this thesis than rule of law. In *Code: And Other Laws of Cyberspace,* Lessig (2006) professes a deep mistrust of sovereign powers and their unethical practices: "Our government has already criminalized the core ethic of this movement, transforming the meaning of hacker into something quite alien to its original sense. Through extremism in copyright regulation, it is criminalizing the core creativity that this network could produce. And this is only the beginning" (Lessig, 2006, p. 8). In Lessig's view, cyberspace itself must also be recognized as an emerging omnipotent and omnipresent sovereign, and humanity must install limits on this sovereign like any in real space (Lessig, 2001). James Boyle in *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors* shared Lessig's sentiment. When Bentham created the Panopticon, what he considered the ideal prison, he was leveraging the coercive power of surveillance (Boyle, 1997). Unethical sovereigns, through the trappings of cyberspace, potentially have the power to condemn the world to that same prison (Boyle, 1997).

Despite his mistrust in the government, Lessig feared corporate avarice even more. The shift from a free and open cyberspace to something reminiscent of the Panopticon seems inevitable (Lessig, 2006). A vigilant nation can stave off the immorality and tyranny of unchecked commercial interests through working with their government to produce

ethical legislation sensitive to human rights (Lessig, 2006). Allison Powell, of the London School of Economics, agrees with Lessig. She advises working with the government can assuage any misgivings on moral terms favorable to both private and public interests, creating "an ethic of participatory knowledge creation… or a process of empowerment through appropriating science in a DIY ethic" (Powell, 2016, p. 613).

Richard Spinello is skeptical of Lessig's assessment and against further regulation: "Lessig assumes the Net will evolve in a certain way once it is in the firmer grip of commercial forces; he has little faith that responsible behavior is possible in cyberspace without the coercive force of government" (Spinello, 2000, p. 137). A decentralized approach, while always mindful of core moral values that should govern action in any space, should not be discounted. Before installing even more restrictive and cumbersome policies, all parties should be allowed to employ ethical self-regulation (Spinello, 2000). In a piece written for *The Modern Law Review,* Chris Reed concurs with Spinello's recommendation. The rule of law in cyberspace is weakened by increasing the volume and specificity of regulation. This practice both contradicts Fuller's internal morality of law and weakens the normative effect of cyberspace law (Reed, 2010). While it is hard to read Lessig and not have Chicken Little come to mind, it is equally difficult to not characterize Spinello's claim that corporations will ethically self-regulate as naive.

Lessig and Spinello are not the only two diametrically opposed scholars on rule of law and cyberspace. Goldsmith and Post were equally at odds when they respectively published *Against Cyberanarchy* and *Against "Against Cyberanarchy*." Goldsmith (2003) asserts both the descriptive and normative claims made by regulation skeptics are flawed: they fail to make a distinction between default and mandatory laws; they discount the potential of traditional legal tools; and they overstate the difference between transactions in real space and cyberspace. A governing body should be afforded the same ethical and territorial jurisdiction in cyberspace as in real space (Goldsmith, 2003). Goldsmith's stance of cyberspace's "Unexceptionalism" is misguided (Post, 2003). Although settled law, received principles, and established ethical standards should be respected, they are not precluded from reconsideration, and cyberspace is the precise territory were law warrants thoughtful revision (Post, 2003). Goldsmith and Post's irreconcilable differences reduce

down to the "if it ain't broke, don't fix it" claim versus the "square peg, round hole" observation. Both make valid claims and never challenge the other on ethical grounds.

Not all laws are necessarily moral, but the assumption is they ought to be. Consequently, the rule of law imposed by a nation-state and its corresponding moral obligation are closely related. Thus, lessons learned from the review of rule of law and cyberethics should be helpful when making the zero-day decision. This thesis will attempt to evaluate their usefulness.

e. International Law and Cyberwarfare

International Law (IL) has jurisdiction over an expansive category of topics, from issues relating to human rights, use of force, and conduct of war to regulating the global commons, international waters, and even outer space (United Nations [UN], 2018). The advent of cyberspace and the prospect of cyberwarfare have created numerous legal and ethical concerns for IL: sovereignty, jurisdiction, international responsibility, use of force, and conduct of hostilities (Schmitt, 2017). None of these issues are unique to cyberspace, but cyberspace does provide a unique set of complications for these issues. Nations are charged with reconciling the new domain with established law or creating new laws to fit the domain. The present state of literature indicates a consistent effort towards law and order in cyberspace. Global concurrence remains elusive and the resolution remains incomplete.

Cyberspace as a warfighting domain is a focal point in the security strategy of the United States, United Kingdom (UK), France, the Russian Federation (RF), and the People's Republic of China (PRC) (White House, 2017a; HM Government [HMG], 2018; Defence and National Security Strategic Review [DNSSR], 2017; Doctrine of Information Security of the Russian Federation [DISRF], 2016; Heath, Gunness & Cooper, 2016). The USG expressed an unwavering commitment to protect critical infrastructure, as well as political, economic, and national interests in cyberspace by identifying risk, deterring and disrupting malicious actors, and deploying layered defenses (White House, 2017a). The UK's National Cyber Security Strategy focused on eight core tenets. While the newly formed National Cyber Security Centre was charged with shouldering most of the burden,

the UK also endeavored to improve the cyber know-how of the general public through its national Cyber Aware campaign (HMG, 2018). France opted for a remarkably different approach in their strategic doctrine. Instead of outlining goals or core concepts, the DNSSR was focused on detailing the nature of threats. Their strategic review acknowledged, among other issues, U.S. dominance, the PRC's and the RF's emerging capability, and jurisdictional issues presented by privately owned trans-national ISPs (DNSSR, 2017). Cyber is one of the three core concepts of strategic deterrence along with nuclear and space in the PRC's national security strategy (Heath, Gunness & Cooper, 2016). The RF, rarely using the word cyber, preferring informational, information sphere, or military-technical, also considers informational security a core tenet of their strategic deterrence plan (Pynnoniemi, 2018). The DISRF enumerated five national interests of the information sphere, a variety of corresponding major information threats, and ten informational strategic objectives or key areas of concern (2016).

The French were most forthcoming in expressing the challenges of reconciling IL with cyberspace. "While France supports the applicability of international law to cyberspace and cyber operations, a principle that meets growing consensus, certain states continue to oppose it. Furthermore, the conditions for implementing and, above all, verifying the enforcement of these rules remain an unresolved issue" (DNSSR, 2017, p. 46). Although not as inclined to acknowledge the murkiness of legal issues in their strategic doctrine, the USG firmly believes cyberspace falls under the jurisdiction of international law (White House, 2017a; Koh, 2012). The DNSSR acknowledged complications involved with cyberwarfare or covert cyberattacks. Specifically, it recognized the difficulty of attribution in cyberspace, and the corresponding uncertainty of justifiably invoking Article 51 of the UN Charter (2017).

D. METHODOLOGY AND ORGANIZATION

This thesis employs an analytical and descriptive research methodology to evaluate USG zero-day policy on utilitarian terms as defined by John Stuart Mill. The research begins with a careful review of Mill's work, specifically focusing on *Utilitarianism, Considerations on Representative Government,* and *On Liberty*, to distil the core principles

of utilitarianism as they apply to nation-state governments. Analysis of these core tenets forms a general utilitarian moral obligation applicable to states and their governments. The thesis then extrapolates the overarching utilitarian obligation to evaluate specifically the USG's VEP, its governing doctrine on zero-day vulnerabilities. In addition to analysis of the doctrine, this examination includes a historically focused descriptive review of the policy, to include its members, processes, and procedures.

This thesis is organized into four chapters. This first chapter has explained the problem, described the value of asking the question, summarized the research methodology employed to answer the question, and provided a review of relevant prior literature.

Chapter II begins with establishing Mill's unique description of utilitarianism and identifying core tenets of the theory. It concludes with the formation of a nation-state's moral obligation derived from the extrapolation of the core principles of indirect rule utilitarianism.

Chapter III evaluates USG government zero-day doctrine, the Vulnerability and Equities Policy, in terms of indirect rule utilitarianism and the associated moral obligation. It includes a historical documentation of the policy's formation and influences, as well as an analysis of its purpose, threshold, exemptions, process, and Executive Review Board.

Chapter IV concludes with recommendations to address policy aspects that can be improved to better fulfill the utilitarian obligation, as well as recommendations to increase the permanence of elements that fulfilled the obligation. Additionally, the chapter includes suggestions for future research in the fields of morality and zero-day policy.

E. CONCLUSION

The topics of morality and justice have been the subject of extensive scholastic scrutiny for thousands of years, while scholarly consideration of cyberwarfare is embryonic in comparison. Consequently, very little of this literature takes on questions of the obligation of nation-states with respect to zero-days, and utilitarianism or morality in general. This thesis is intent on making a contribution to fill that gap in knowledge.

THIS PAGE IS INTENTIONALLY LEFT BLANK

II. THE UTILITY OF OBLIGATION

A. INTRODUCTION

Before determining a nation's moral obligation with regard to zero-day weapons, an understanding of a nation's obligations, in general, must be established. This thesis utilizes the ethical philosophy of utilitarianism as defined by John Stuart Mill to serve as the foundation for this determination, primarily focusing on three of his works: *Utilitarianism, Considerations on Representative Government,* and *On Liberty*. The chapter begins with an analysis of utilitarianism. It seeks to establish the tenets of utilitarianism, and from these core principles, deduce a nation's moral obligation. Additionally, an analysis of prominent critics of Mill's arguments will be considered to further refine an understanding of the obligation. Finally, the chapter will conclude with a determination of a nation's utilitarian moral obligation.

B. MILL'S UTILITY

Conventionally, utilitarianism is recognized as a form of consequentialism; this is where an act is morally justified by the result it produces. Consequentialism, ergo, utilitarianism, is a theory of morality more concerned with the ends than the means. In contrast, deontic or virtue-based morality is more in line with the normative conception of rightness and justice. In this view, utilitarianism is not interested in the means, only the ends that result in the most good, whereas deontic morality cares about the means. In other words, if it can be said utilitarianism is concerned with the good, then deontic morality would be more concerned with the right.

The classic philosophical example to illustrate the moral significance of ends versus means is "the Fat Man and the Cart" ("Deontology," 2016). There is a cart speeding down the track. An individual, let's call him Frank, is standing near the track and notices in the distance five individuals tied to the track who will die when the cart hits them. A fat man is standing next to Frank. Time is of the essence and neither Frank nor the fat man would be able to untie the people before the cart killed them. The notion pops into Frank's head that he could push the fat man onto the track and into the cart. It would kill the fat man, but

it would also stop the cart and save the other five people. Frank quickly dismisses the notion of killing the fat man because that would not be right. This example illustrates how a means-based ethics based on right action may supersede an ends-based ethics based on the greater good. As killing is wrong, deontology would hold Frank should not kill the fat man even if it saves lives. Any result that is derived from a wrong action is also wrong. Utilitarianism would disagree. Utilitarianism would say there is a net-gain of four lives. The greater good has increased. Therefore, killing the fat man would have been morally justified.

Mill's utilitarianism, however, is more sophisticated than this strictly consequential form. Mill's moral theory, while similar to the traditional conception in the sense that it still values the greater good, requires more than happiness to be considered when determining the morality of an action. Mill (2009c) defined utilitarianism as:

> The creed which accepts as the foundation of morals, Utility, or the Greatest Happiness Principle, holds that actions are right in proportion as they tend to promote happiness, wrong as they tend to produce the reverse of happiness. By happiness is intended pleasure, and the absence of pain; by unhappiness, pain, and the privation of pleasure (p. 14).

There are several aspects of this definition that require further explanation, to both refine general apprehension of the theory, as well as to clarify Mill's unique authoritative perspective.

First, the key tenet of utilitarianism must be established. It is the belief that happiness or some form of happiness is the only intrinsic good; only happiness is desirable for its own sake, and not as a means to something else. Although Jeremy Bentham is conventionally regarded as the father of utilitarianism, Mill, a protégé of Bentham, is largely credited with developing the principle into its most recognized form.

If overall happiness is the primary concern of Mill's utilitarianism, the preservation of individual liberty would be second, if not equal. Mill (2011) defines his liberty principle as "the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self-protection" (p. 26). Mill (2011) states the only justifiable reason to exert power over another against their will is to

prevent harm to others. Furthermore, while he allows for "remonstrating" with the person if the advised course of action is for their own good, Mill prohibits any coercion to affect compliance. Mill asserted his liberty principle was derived from utility.

This liberty principle engendered resounding scholarly consternation. Gray (1996) claims many regarded the problems associated with the liberty principle as insoluble. Conventional understanding of utilitarianism recognized it as a single principle theory. Not only did Mill's liberty principle challenge the notion of a single principle theory, it allowed for the rejection of an action as morally unjust even if it resulted in the largest increase in overall good. Ursula K. Le Guin's short story, *The Ones Who Walk Away from Omelas,* is an example. The town of Omelas is a utopia in all manners of the word. Every citizen of Omelas lives in a state of perfect contentment—almost everyone. In the basement of a building is a child. A child held against their will, if they could be said to have a will. The child's existence was objectively miserable, and comparably utterly abject. The thriving and idyllic village could only exist in this glorious state provided one child remains in that miserable state. Every citizen, at least once, must not only be made aware of the child's existence, but go down to the basement and see the misery for themselves. The ones that could not abide living in a paradise contingent upon misery, even if it is the misery of only one, are those who walked away (Le Guin, 1973). Le Guin's narrative is another form of "the Fat Man and the Cart" and asks the reader to decide if they would stay or walk away. A person that holds to a conventional understanding of utilitarianism would stay and be morally justified in doing so. Mill would walk away.

Early Mill scholarship concluded "that his moral and political writings cannot be expected to yield a coherent doctrine and that the argument of *On Liberty,* in particular, must inevitably prove abortive" (Gray, 1996, p. 2). This assessment of Mill comes off as reasonable and harsh. Mill studied classical antiquity in Greek and Latin at an age when most people were still illiterate. While the conflict between utility and liberty is apparent, some sort of coherent understanding of Mill should be possible. More modern revisionist Mill scholarship found a way to reconcile what was long considered irreconcilable. Gray (1996) advised an indirect application. Wright (2014) recommended an ecumenical approach. Indirect utilitarianism seems to be the largely accepted approach and will be

applied in this thesis. Indirect utilitarianism should be understood as a multi-faceted moral principle that urges a consideration of ends *and* means to affect the greatest good.

An understanding of happiness remains critical to Mill's morality. It is important to establish that his notion of happiness will be interchangeable with the conventional understanding of pleasure, good, and goodness in this thesis. One of Mill's more prominent breaks from Bentham was in regard to the nature of pleasure itself. Bentham (2017) believed one pleasure was as good as another and the difference was purely a quantitative matter. Mill (2009c) believed otherwise, and succinctly summarized the sentiment with his infamous claim, "it is better to be a human being dissatisfied than a pig satisfied; better to be Socrates dissatisfied than a fool satisfied" (p. 19).

The allowance for both quantitative and qualitative goodness in Mill's thinking is instrumentally important to both establishing the utilitarian moral obligation and to making the zero-day decision. A moral decision or a zero-day policy based exclusively on quantitative considerations would be simple. But people on the individual level and policymakers at the societal level require discretion for their judgement to be complete. An allowance for qualitative consideration provides that needed discretion (as seen in the discussion in Chapter III).

While Bentham and Mill did not agree that one pleasure was as good as any other, they did agree that the happiness of any one person was as important as any other. In utilitarian morality, when accounting for the greater good, one person's worth, whether they be a prime minister or a pauper, is identical to another. Mill (2009c) tidily summarizes this notion into what he calls Bentham's dictum: "Everybody to count for one, nobody for more than one" (p. 112). Mill further expounds on Bentham's dictum, claiming utilitarianism is a "mere form of words without rational signification, unless one person's happiness, supposed in equal degree (with the proper allowance made for kind), is counted for exactly as much as another's" (p. 12). It is important to clarify this notion of equality. Mill believed humans possessed a range in caliber and capability for both the aesthetic and the cognitive capacities (2009c). Mill did not believe humans were all created equally. Rather, he believed they should be valued equally. This understanding of equality will be

of vital importance in the next chapter when examining the interplay of justice, duty, and obligation in relation to government making the zero-day decision.

There are three classes of utilitarianism: act, rule, and sanction. Act utilitarianism is much like it sounds. This form is concerned only with the act in question and how much good it can create or pain it can prevent now. Each and every action is its own discrete matter and has a direct effect on utility (Crisp, 2002). Rule utilitarianism insists on a consideration of precedent and requires that history inform, guide, or determine the decision-making process through the establishment of and faithfulness to moral rules. Moral justice is not derived from the act but rather from adherence to a set of rules generally accepted to increase overall happiness (Crisp, 2002). Sanction utilitarianism is similar to rule utilitarianism as it uses precedent and rules to determine justice, but it is different from act and rule utilitarianism as it excludes certain actions from moral consideration. Essentially, if the agent does not feel an internal sanction, more simply guilt, from doing or not doing the act, then the act is outside the realm of morality (Wright, 2014). If the determination is made that the act is something the agent ought to do or hazard the sting of remorse, then the jurisdiction of morality is conferred, and rule utilitarianism is applied.

For example, a healthy and fit 25-year-old with no dietary restrictions or history of health problems is at an ice cream parlor. She cannot decide if she would like one scoop or two. She has exercised today. She will exercise tomorrow. If she opts for two scoops, she will feel no pang of compunction or remorse. The decision for the second scoop is discretionary, purely a matter of desire. Sanction utilitarianism holds her decision is extra-moral and thus morality need not be applied. Act and rule utilitarianism deem every action, even a decision based on the most innocuous scoop of ice cream, to involve some measure of utility. It is natural to question if sanction utilitarianism is actually utilitarianism or even consequentialism (Jacobson, 2008). However, the accepted belief is that ultimately, utility informs each decision. The remorse the agent feels is because, although they could have, they did not improve utility, thereby validating sanction as a form of utilitarianism (Lyons, 1994; Wright, 2014). With the definitions of the three classes established, now a determination of which Mill employed can be made.

The problem is Mill used all three forms in his description of the theory and never expressly said which one he favored. Unsurprisingly, there is no agreement amongst scholars which variety Mill intended to apply, or if only one applies. Fortunately, the form that is fundamentally important to this thesis is also the one that has near universal consensus on when it was used. More modern scholars maintain Mill's utilitarianism is best understood as indirect, holistic, or ecumenical (Gray, 1996; Jacobson, 2008; Wright, 2014). This modern revisionist understanding of Mill, that is to say indirect utilitarianism, is the version carried forward to evaluate USG zero-day policy and is described in detail in the subsequent section.

According to *the Stanford Encyclopedia of Philosophy,* Mill primarily used sanction utility in Chapter 5 of *Utilitarianism* ("Mill's Moral and Political Philosophy," 2018). Earlier chapters represent Mill's efforts to define, prove, and validate utility as the only worthy moral standard. Chapter 5, the final chapter, is where Mill explains how utilitarianism informs justice and the workings of the state. Moral obligation, duty, and justice are very closely linked, sometimes overlapping, and sometimes directly related to or contingent upon each other. As chapter five most directly relates to the moral obligation of a nation-state and sanction utilitarianism is used in that chapter, sanction-based utility will be the version used by this thesis moving forward to deduce a state's utilitarian moral obligation.

There are five key elements in the understanding of utility to carry forward. Mill's utilitarianism is best understood as indirect requiring a consideration of ends and means. Happiness is the only intrinsic good. Neither nations nor their governments experience happiness. Regarding a utilitarian-defined moral obligation with respect to a government, happiness should be recognized as the general welfare of citizens, or more simply the public good. Mill allowed for both quantitative and qualitative considerations of good. This affords a policy-maker discretion. Mill made no such distinction for the value of people. This notion emphasizes the importance of impartiality. While impartiality is a critical aspect of Mill's utilitarianism, it is also one of the main complaints lodged against it. This criticism will be addressed later on in the chapter. Finally, sanction utilitarianism directly relates to how Mill defines moral obligation and justice in terms of utility. It is important

to restate that once moral applicability has been established, sanction utility essentially becomes rule utility. As governments are bound by legality to maintain justice, rule utilitarianism is run by established precedent to improve overall welfare.

C. THE NATURE OF OBLIGATION

This section establishes a nation's overall moral obligation to the public good, and therefore a moral obligation to utility itself. Specifically, the government is morally obligated to foster virtue in its citizens and does so by example as well as by setting laws. Furthermore, not only are policymakers obligated to do good, they also must think true, that is not only must act be moral but the reasoning must be sound. As this section discusses, Mill contends that a government is not necessarily morally obligated to maintain justice, rather that moral obligation sets the jurisdiction of justice. Additionally, this section addresses how Mill's moral principle relates to foreign policy. Finally, as a point of clarification, the government in question is democratic and representative.

1. A State's Duty

Objectively, as nations and people are two distinct entities, it would be hard to say unequivocally the moral obligation of one is identical to the other. In fact, political philosophers of the Machiavellian school would reject the claim flatly. While this thesis holds, the obligations do not apply identically; there are varying degrees of overlap. Sometimes the obligations diverge or are entirely inapplicable, while other times they align or overlap. With regard to representative government, there are instances where individual obligation so closely overlaps with that of the government, times where they are so directly linked, that the obligation becomes effectively indistinguishable. An example is voting: "In any political election, even by universal suffrage, the voter is under an absolute moral obligation to consider the interest of the public, not his private advantage" (Mill, 2009a, p. 233). Although Mill directly levies this moral obligation upon the individual voter, it indirectly speaks to the overarching moral obligation of government.

Representative government comes from the people. The public votes for either a law or an agent to make or administer the law. If when casting their vote an individual is morally obligated to value public good, then by transitive property, the representative

government formed on the people's behalf, through the casting of their votes, is also morally obligated to value the same. If the government is morally obligated to value the public good, essentially it is morally obligated to value utility. This is a specific example of moral obligation. Additionally, Mill provided a more general rule of thumb description of the applicability of moral obligation.

Mill believed the truest test of good governments was, "how far they tend to foster in the members of the community the various desirable qualities, moral and intellectual" (2009a, pg. 41). Mill linked the goodness, effectiveness, and usefulness of a government to what values it promoted and how strongly those values were encouraged (2009a). These claims provide a more discrete example of the moral obligation of government to promote utility. Public good is specific in purpose, but an abstraction in regard to application. Therefore, if not expressly declared, public good is open to interpretation. Although Mill did not specify the good in an itemized or procedural sense, he did offer a symbiotic paradigm, making the people and the government better off. As representative government comes from the public, if a government nurtured virtuous characteristics in its people, the gain would be twofold. The government would increase the likelihood of capable elected officials and create a competent and capable constituency in their own right (2009a).

If public good is the government's ends, "by example" is its means. Mill maintains the government best fosters desirable values through conspicuous action: "By holding up to every citizen an example of morality and good conscience applied to difficult adjustments, and an evidence of the value which the highest authorities attach to them, [government] tends in an eminent degree to educate the moral sentiments of the community, both in respect of strength and of discrimination" (2009a, p. 34). Mill explains how good government should perform, and in doing so, shows how it meets its moral obligation. If government ought to foster established desired values in relation to their significance, the government best does so by example. The how portion is particularly important. It demonstrates the significance of qualitative consideration to utility, as well as providing an example of Mill's inclination towards sanction and rule utilitarianism.

Qualitative consideration allows for a scale or gradient of values to exist. Mill believed values, like pleasures, were not each as good as any other, and should be promoted

commensurate to their level of desirability. An exclusively quantitative evaluation, as advocated by Bentham, creates value impartiality. If one pleasure or good is as important as any other, values become fungible. Mill did not believe desirable values should merely be fostered, he believed they should be fostered in kind. If qualitative consideration was not allowed, discretion could not exist, and promotion in kind would be impossible.

Rule utility promotes greater good through commitment to established standards. These can be laws or informally socially agreed upon values. Rule utility is not as concerned with the many and varied ways a standard could be established. Rather, once it is established, adherence to the standard becomes moral obligation and fulfillment of the obligation results in not only increased utility but also the sentiment of justice being served. Consequently, when the government is confronted with what Mill describes as "difficult adjustments," in accordance with rule utilitarianism, it ought to defer either directly to those values or laws derived from them. In fact, it seems if laws were written in a strictly rule utilitarian fashion, the difficult adjustments would not be so difficult. Each law is written such that adherence promotes overall good. While there may a small group disproportionally disadvantaged, since each person counts for one and not more than one, and rule utility promotes the greater good, the government's action can only largely be positive.

Although the nature of a nation's moral obligation has become clearer, certain parts remain murky. How does a nation know what values are more desirable? The answer would seem the value that over time, consistently, and for the most people, results in the largest increase in utility. The question then becomes, how does a nation know which value provides the largest increase? Humans are fallible. Any government comprised of them is also fallible. An assessment of utility derived from an action can only occur after the fact. If the people and the government comprised of them are imperfect, wrong acts will occur, bad values will be fostered, and good values incorrectly ranked. If the moral obligation to act in a manner commensurate with the public good exists, how does a government know what it is?

The answer is that it cannot, at least in any specific sense. Indirect utilitarianism's requirement to consider ends and means makes the principle less consequentialist and more

intuitionist. Mill establishes virtue as the basis for intuition; “the love of money, of power, or of fame, that all of these may, and often do, render the individual noxious to the other members of the society to which he belongs, whereas there is nothing which makes him so much a blessing to them as the cultivation of the disinterested, love of virtue” (2009c, p. 69). In one sentence, Mill accomplishes two things indirectly. He emphasizes public good over private gain and addresses one of intuitionism’s main criticisms. Intuitionist theory suffers from the ontological crisis of uncertainty, a person strictly relying on intuition cannot be sure. While virtue does not entirely free Mill’s consideration of ends and mean from this criticism, it does provide some measure of surety. While there may be various magnitudes of virtuous behavior, what is and is not virtuous is easily distinguished.

Humans are not perfect, thus virtue cannot always be achieved. Mill acknowledges both man and government’s inherent fallibility. Bad taxes have been levied and unjust wars waged, this does not mean no tax shall ever again be levied nor any war ever again waged (Mill, 2011). Despite the perpetual potential of error, Mill insists, “it is the duty of governments, and of individuals, to form the truest opinions they can; to form them carefully, and never impose them upon others unless they are quite sure of being right” (2011, p. 35). Mill is allowing for the government to make mistakes. He even admits, “there is no such thing as absolute certainty” (2011, p. 35). Effectively, in addition to a moral obligation, Mill has also charged the government with an epistemic obligation. Not only must it act as good as possible, its policymakers must think as true as possible. This means that a policymaker or politician cannot willfully convince themselves something is true, when they strongly suspect or have reason to believe it is false, with the intent to curry favor, pander to their constituency, or engage in any action that prioritizes private gain over public good. Furthermore, an agency cannot knowingly misrepresent action with the intent of circumventing policy (an accusation levied against the FBI that will be addressed in the next chapter).

By allowing for mistakes Mill has not only built in a margin for error, he has created a moral framework where progress is permissible. Mill was one of the most liberal thinkers of the Victorian era. In his time, issues like universal suffrage and legal slavery were the topics of political debate. Mill infamously engaged in correspondence with Thomas

Carlyle, arguing against Carlyle's claim of moral grounds for Negro slavery. Thus, it is unsurprising that Mill crafted a theory that allowed for progress. Cyberspace is new and growing at an incredible rate. Its newness coupled with its high rate of change makes it an ideal domain for a moral framework that allows for adaptation or amendment to means. Due to cyberspace's inherently dynamic structure, many of the lessons learned in cyberspace will likely come from trial and error. Mill's description allows for error. While errors are allowed for, the government is morally obligated to acknowledge and correct them.

2. An Altogether Foreign Matter

Any discussion addressing the moral obligation of a nation-state would be incomplete if it exclusively addressed the obligation in a domestic context. Nations do not exist as solitary entities or in a vacuum; rather they share a space with other nations in a varying state of anarchy. The anarchy of nations relates to the lack of a sovereign power to establish order and mete out punishment for disruptions to that order. Nations temper any perceived or potential chaos associated with anarchy by forming contracts, which occur in a variety of forms. The United Nations Charter and the Geneva Convention are examples. While nations ultimately live in a state of anarchy, they have of their own volition, adopted mechanisms to bring about some measure of order.

In a state of relative anarchy, with no absolute governing power to impose and enforce law, judging what actions are right or wrong becomes much more complex than distinguishing between legal and illegal. Nations instead assess actions in terms of moral, expedient, and strategic value, or more simply, how the action effects national interest. A head of state with a politically realist persuasion, especially one with a Machiavellian inclination, could use utilitarianism to justify what would traditionally be considered bad behavior if the result increased the overall good of one's own state. In a strictly act utilitarian sense, the bad behavior would actually be morally sound, even if it victimized a foreign nation or its citizens.

John Stuart Mill was no political realist and he did not intend utilitarianism to justify bad behavior by governments any more than by individuals. Just as Mill discourages

prioritizing private gain on an individual level, he denounces the opportunistic pursuit of national interest on a global level: "To go to war for an idea, if the war is aggressive, not defensive, is as criminal as to go to war for territory or revenue; for it is as little justifiable to force our ideas on other people, as to compel them to submit to our will in any other respect" (2006, p. 7). Furthermore, while each resident of a community should conduct themselves in a virtuous manner, so should each nation of the global community. A virtuous state ought "to mediate in the quarrels which break out between foreign States, to arrest obstinate civil wars, to reconcile belligerents, to intercede for mild treatment of the vanquished… Not only does this nation desire no benefit to itself at the expense of others, it desires none in which all others do not as freely participate" (Mill, 2006, p. 1). It should be acknowledged Mill admits this ideal state has very little chance of existing, but it serves to illustrate how a nation ought to act. Mill very clearly levies the same moral responsibilities of greater good through virtue on states; his moral obligation is not bounded by borders. Mill is extrapolating his liberty principle to a global scale.

While being liberal, Mill does not believe war is always wrong: "But there assuredly are cases in which it is allowable to go to war, without having been ourselves attacked, or threatened with attack; and it is very important that nations should make up their minds in time, as to what these cases are" (2006, p. 7). This quote appears in a work intended to offer ethical insight regarding the debate on interventionism versus non-interventionism. It represents another instance of Mill advocating for something more than national interest or private gain. Mill extrapolates utilitarianism to a global scale suggesting that just as individuals should be concerned with the greater good of their community, nations should be concerned with the greater good of their shared anarchical community. Mill is not asserting that national interest is always wrong. He is denouncing the Machiavellian opportunistic pursuit of national interest.

D. THE NATURE OF OBLIGATION?

This section will analyze criticisms of utilitarianism and criticisms of Mills conception of moral obligation, in order to refine an understanding Mill's utilitarianism. First, the section addresses the claim that utilitarianism should be dismissed as dressed up

hedonism or egoism. Specifically, it references Mill discounting this notion and supporting the claim that happiness is the only intrinsic good. Second, the section acknowledges John Rawl's assessment that utilitarianism unrealistically values impartiality. Of the three criticisms addressed in this section, the one lodged against impartiality is the most problematic. Finally, the section will conclude with an analysis of utilitarianism's shortcomings with regard to distributive justice.

1. Hedonism

Mill (2009c) recognized one of the main criticisms levied against utilitarianism is the contention that utility is nothing more than indulgent egoism masquerading as moral theory. He acknowledged that opponents claimed happiness was not the only intrinsic good, and that satisfaction came from a blend of hard work, discipline, and stoicism. When extrapolated out to consider how or even if utilitarianism should inform governments and their policymaker's decisions, the criticism seems valid. A government ought to be externally concerned with protecting its citizens from foreign aggression and internally concerned with maintaining justice and preserving their rights. Happiness or pleasure should be regarded as secondary, tertiary, or even coincidentally anecdotal to those primary concerns.

This criticism rings hollow. Mill went to great lengths to discuss how good government ought to act in both foreign and domestic contexts covering a variety of topics: interventionism, colonialism, taxation, voting, education, welfare, and property rights. Mill (2009c) maintained critics that dismissed the criterion of happiness as trivial were shortsighted, asserting that their superior alternatives, in the end, actually served to make them happy and were in fact in line with utilitarian theory. Furthermore, he rejected the singularly selfish characterization of utilitarianism: "What the assailants of utilitarianism seldom have the justice to acknowledge, that the happiness which forms the utilitarian standard of what is right in conduct, is not the agent's own happiness, but that of all concerned" (2009c, p. 23). Not only does Mill's assertion refute the egoism characterization, it supports public good as the utilitarian moral obligation of government.

As discussed in the preceding section, Mill explicitly applies these principles to delineate the "virtuous" expectations for state behavior on the global scene.

2. Impartiality

John Rawls believed Mill's utilitarianism placed an unreasonable importance on impartiality, while not affording enough importance to individuality. Rawls is arguably the preeminent post-World War II political philosopher. His seminal work a *Theory of Justice* was written in part as a rebuke of Mill's utilitarian infused conception of justice. Utilitarian moral obligation, as defined by Mill, is contingent upon impartiality: "As between his own happiness and that of others, utilitarianism requires him to be as strictly impartial as a disinterested and benevolent spectator" (2009c, p. 31). Rawls (1999) strongly condemned the viability of the hypothetical impartial observer. Although also politically liberal and an advocate for public good, Rawls maintained Mill's notion of utilitarianism and consequent conception of justice did not do enough to respect the significance of individuality.

If Rawls's assertion is held as true, then the sanction of Mill's moral obligation is weakened, if not invalidated. An allowance for partiality makes the expedient permissible, if not just. To the degree Rawls's claim is fair and compelling, the interplay between the moral and the expedient presents a credible challenge to the value of utilitarianism's influence on policy. By allowing for the expedient, Rawls effectively validates political realism. Mill's liberalism-infused morality is antithetical to political realism, if not mutually exclusive with it. An endorsement of one is a criticism of another. In the following chapter's application of Mill's utilitarianism to U.S. zero-day policies, the certitude of the conclusions derived from the analytical methodology is tempered in proportion to the value attributed to individuality, including the individuality of states in the international system.

3. Distributive Justice

Utilitarian justice does not account for distributive justice (Crisp 2002; Lyons, 1994; Rawls, 1999). Rawls (1999) objected to utilitarianism's seeming disregard for distributive justice: "The striking feature of the utilitarian view of justice is that it does not matter, except indirectly, how this sum of satisfactions is distributed among individuals any more than it matters, except indirectly, how one man distributes his satisfactions over

time" (p. 45). Lyons (1994) acknowledges that when "faced with a choice between maximizing satisfactions and distributing them equitably, the utilitarian is theory-bound to choose the former" (p. 69). If these assessments are held as true, it would become very difficult, if not impossible, to determine if the government's utilitarian moral obligation to the public good was actually being met. An inability to allow for distributive justice makes catering to special interest morally permissible.

Imagine a situation where only one of two laws is able to be passed. The first law incrementally increases the utility of everyone resulting in a net gain of 100 units of utility. The second law greatly enhances the utility of a handful of people while leaving everyone else unaffected or slightly worse off, yet results in a net gain of 120 units of utility. Utilitarian morality would dictate the second law should be passed. Not only would this contradict conventionally accepted notions of justice, it directly contradicts what Mill himself has claimed regarding good government. If voters are driven by private interest or purchased by special interest, representative government becomes an instrument of tyranny and intrigue instead of a mechanism to protect against them (Mill, 2009a). The distribution criticism may be valid regarding utilitarianism in general, but is not as applicable to Mill's version of the theory. Not only did he allow for progress, he scoffed at those whose myopia was so severe they could not even conceive change.

> How much greater still, then, must the error be, of setting up such unbending principles, not merely as universal rules for attaining a given end, but as rules of conduct generally, without regard to the possibility, not only that some modifying cause may prevent the attainment of the given end by the means which the rule prescribes, but that *success itself may conflict with some other end, which may possibly chance to be more desirable* [emphasis added] (Mill, 2009b, p. 1149).

Mill did not merely allow for progress, he encouraged it. Allowing for and encouraging adaptation is particularly important to policymakers charged with the zero-day decision.

E. CONCLUSION

Mill's utilitarianism is best understood in the indirect and rule form. It requires a consideration of ends and means. A government's ends are the public good and its means are setting a conspicuous and virtuous example. Additionally, happiness, pleasures, and

goodness are to be valued in kind with discrimination paid to quality and quantity. While discretion is afforded to pleasure, no such allowance is made for people. As Bentham's dictum states, "Everybody to count for one, nobody for more than one." Mill intends for additional elements like liberty, freedom, and virtue to factor into evaluation on moral terms. These characteristics represent the normative elements of Mill's theory. The type of utilitarianism most used by Mill is sanction and rule. Through an analysis of his work and an understanding of these elements, a state's utilitarian moral obligation has been established. The obligation is to the public good of its citizens, effectively to utility itself. Specifically, a government is morally obligated to foster desirable values by demonstrating those values through action. Additionally, not only must policymakers do good, they must think true.

III. THE PUBLIC GOOD

A. INTRODUCTION

This chapter examines how the USG's zero-day policy measures up against the utilitarian moral obligation. The first section offers a detailed history of the VEP, with particular attention to how looming legislation both shaped policy and likely forced an unprecedented cyber-policy disclosure. Second, the chapter addresses moral issues that arise from the policy's focus and threshold statements. It also examines how the policy's exemption section affects its ability to fulfill the utilitarian moral obligation. The chapter concludes with an analysis of the Executive Review Board's (ERB) composition and function, specifically focusing on guidance from Annex B of the policy to determine if the Vulnerabilities and Equities Policy, in print and in practice, fulfills the moral obligation.

If the purpose of the VEP could be summed up in one word, it would be balance. The policy seeks to balance equities, to be understood as reconciling the competing interests of stakeholders. Say the National Security Agency (NSA) or the Central Intelligence Agency (CIA) is conducting what is known as a "follow the money" mission. One of them discovers a zero-day vulnerability in banking software that can be exploited to greatly enhance the mission. While the intelligence community sees clear added value through exploiting the vulnerability, other entities like the Department of Treasury or the Department of Commerce would likely have a strong interest in seeing this vulnerability patched. The VEP's ERB convenes to allow all members to address their concerns. Ideally, those parties with equities make a consensus-based decision to disclose or restrict knowledge of the vulnerability. The policy does have provisions if a consensus cannot be reached, as well as mechanisms for dissenting board members to appeal any determination.

B. A HISTORY OF THE VEP

The impetus for the VEP came from the George W. Bush Administration. In 2008, through National Security Presidential Directive (NPSD) 54 and Homeland Security Presidential Directive (HPSD) 23, President Bush directed the Secretaries of State, Defense, Homeland Security, the Attorney General, and the Director of National

Intelligence to create a joint plan for the coordination and application of offensive cyber capabilities (Jaikaran, 2017). While the process to create the VEP began in 2008, it would take over six years for the public to be made aware of the program. The Electronic Frontier Foundation (EFF) filed a Freedom of Information Act (FOIA) request and subsequent lawsuit to force the NSA to release documents related to the VEP (Crocker, 2015). On July 1, 2014, the NSA responded and released two declassified and heavily redacted documents: *Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities and Equities Policy and Process*, which would come to be known as the VEP, and the "Vulnerabilities and Equities Policy and Process Highlights" (Healey, 2016).

These documents established February 16, 2010 as the effective date for the VEP and defined the policy as:

> A process to ensure that dissemination decisions regarding the existence of a vulnerability are made quickly, in full consultation with all concerned government organizations, and in the best interest of government missions of cybersecurity, information assurance, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection (2010, p. 2).

The NSA was in charge of the VEP with its Information Assurance Directorate (IAD) as Executive Secretariat (Knake & Schwartz, 2016). Some in Washington believed the NSA operated the VEP in a fashion commensurate with its guarded and compartmentalized reputation and did not make use of the interagency process as the policy intended. In an interview with Columbia's *Journal of International Affairs*, a National Security Council (NSC) insider claimed from inception until 2014, the "VEP was dormant. NSA continued to run their own internal process but did not formally include outside agencies" (Healey, 2016).

The NSA's unquestioned control over the VEP began to weaken in 2013. The man responsible was Edward Snowden, who downloaded approximately 1.5 million files, allowing journalists to publish more than 7,000 Top Secret documents (Szoldra, 2016). After analysis of Snowden's leaked documents, the *Washington Post* reported that in fiscal year 2013 the NSA secretly spent over $25 million towards procurement of vulnerabilities

(Fung, 2013). The estimated volume of vulnerabilities purchased was between 100 and 625 (Healey, 2016).

In an effort to quell the growing tide of public resentment, President Obama commissioned the *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (Knake & Schwartz, 2016). The working group produced the report *Liberty and Security in a Changing World,* which admitted that overzealous pursuit of national interests can have the potential to erode privacy and civil liberties (2013). Much like the VEP as originally intended, the newly commissioned report sought balance. Unlike the VEP as actually implemented, the report also sought transparency. Specifically, Recommendation 30, while leaving the NSA's IAD in the role of Executive Secretariat, called for the VEP to be chaired by a representative of the National Security Council (2013). In addition to shifting the balance of power away from the perceived operational and espionage bias of the NSA, the new leadership role was a move toward transparency. Presumably, the NSC was inherently committed to the interagency process and would ensure all members of the VEP with equities related to a vulnerability would be consulted when one was discovered.

While many of the recommendations in the report ultimately did inform VEP policy, in 2013 they were still merely recommendations. A *Wired* article claimed, "Obama appeared to ignore the board's recommendations when, a month later, he announced a list of NSA reforms that contained no mention of zero-days or the government's policy about using them" (Zetter, 2014).

A subsequent incident served as the White House's impetus to turn the report's recommendations into policy. A media report by Bloomberg claimed that not only did the USG know about the Open Secure Socket Layer (SSL) exploit CVE-2014-0160, more commonly known as Heartbleed, but it had known about it for over two years and could have stopped it from ever happening (Riley, 2014). The SSL protocol encrypts data as it travels between browser and server. The Open SSL exploit is a vulnerability that allowed malicious actors unprecedented and unauthorized access to sensitive information like user names and passwords (Fruhlinger, 2017). The vulnerability existed on thousands of web servers, including servers used by major websites like Yahoo (Fruhlinger, 2017). The

White House flatly denied the accusation and the report was largely dismissed as false (Perlroth & Sanger, 2014; Zetter, 2015). But the public's misgivings remained largely unassuaged. The Obama Administration decided it was time for action.

In what, at the time, was considered a rare act of public disclosure, White House Cybersecurity Coordinator Michael Daniel wrote a blog post to both deny Bloomberg's reporting and shed light on how the USG handles vulnerabilities. Daniel (2014) admitted there were no "hard and fast rules" but also disclosed the existence of a "disciplined, rigorous, and high level decision-making" interagency process to determine how to handle vulnerabilities on a case-by-case basis. While saying there are instances where national interest and public good are best served by retaining the vulnerability, Daniel stated that the process "is biased toward responsibly disclosing vulnerabilities" (2014, p. 1).

The rhetoric of bias towards responsible disclosure became the consistent stance of the Obama Administration. The Office of the Director of National Intelligence (ODNI), following Michael Daniel's lead, reiterated this stance via a blog post. ODNI asserted, "this process is called the VEP. Unless there is a clear national security or law enforcement need, this process is biased toward responsibly disclosing such vulnerabilities" (ODNI, 2014). In a written statement in preparation for his confirmation hearing in front of the Senate Armed Services Committee (SASC), Admiral Mike Rogers stated "the default is to disclose vulnerabilities in products and systems used by the U.S. and its allies" (SASC, 2014, p. 17). He reiterated the claim during an appearance at Stanford University (Zetter, 2014). In 2014, the Obama Administration committed to reinvigorate the VEP, dispel the characterization of the USG as "hoarder of zero-days," and establish their prioritization of responsible disclosure.

If any public goodwill was accrued over the two-year, largely incident free span, it seemed entirely dashed in 2016 by the group known as the Shadow Brokers. The Shadow Brokers brazenly announced their existence to the world by hosting one of the Internet's most infamous auctions. In August of 2016, the Shadow Brokers expressed interest in auctioning stolen cyber-weapons, which they claim came from the Equation Group (EG), an entity suspected to be closely linked to or operated by the NSA (Solon, 2016). In early 2015, Kaspersky Labs (KL) published a detailed report on the EG. While evidence

presented in the report strongly indicated a link between the EG and the USG, the report stopped short of actually making the claim. Interestingly, around 2003, it was KL who gave the EG their name (Goodin, 2015). KL had been aware of and monitoring the yet unnamed group for some time; after noticing a "strong affinity for encryption algorithms, advanced obfuscation methods, and sophisticated techniques" they dubbed them "the Equation Group" (Goodin, 2015).

Who or what the Shadow Brokers are remains murky. Due to their impressive level of expertise and capability, as well as their seemingly high levels of funding, some experts believe the Shadow Brokers are actually a proxy entity acting at the behest of Russia or China (Perlroth, Sanger & Shane, 2017; Schneier, 2017). A blog post at *Cyber Security Intelligence* discounts the group's Russian-infused dialect as feigned and satirical (2017). The post claims the Shadow Brokers' familiarity with NSA's Tailored Access Operations (TAO) is the true tell and indicates they may be NSA insiders.

Regardless of actual identity, the Shadow Brokers' actions have been subversive and damaging. In April of 2017, the Shadow Brokers released NSA-designed malware that enabled the infamous WannaCry attack effecting over 70,000 devices across 74 countries (Holland, 2017). The exploit is a form of ransomware, allowing malicious actors to encrypt another user's files and then demand payment. Upon transfer of money, a key is provided that will decrypt the files and then return them to their usable form. Without the decryption key, there is effectively zero chance of the user getting a useful version of their files.

By itself, WannaCry is unrelated to the NSA. The agency's involvement stemmed from two exploits they previously developed - EternalBlue and DoublePulsar – stolen from them by the Shadow Brokers (Ng, 2017). EternalBlue targets a vulnerability in the Server Message Block (SMB) protocol of Windows machines (Fruhlinger, 2018). EternalBlue was particularly troublesome when coupled with the ransomware because it had the ability to beacon out to other potential target machines and self-propagate completely independent of any user interaction (Langde, 2017). EternalBlue's potential for devastating results also needed DoublePulsar. DoublePulsar allows hackers to bypass authentication systems and create a backdoor (Langde, 2017). This back door remained open to the hacker and provided remote access to the infected computer.

DoublePulsar provided access to install WannaCry. EternalBlue provided a means to spread the ransomware with no action required by the user. The hackers requested $300 to decrypt each machine with a steep price hike if the user dawdled (Langde, 2017). On July 31, 2017, according to a tweet from @actual_ransom, the largest dollar amount in the Bitcoin wallets associated with the ransomware attack, prior to any withdrawals, totaled $149,545.27 (Actual_ransom, 2017).

The WannaCry ransomware narrative has an interesting wrinkle, an aspect that tends to justifiably perturb the sensibilities of zero-day policymakers. The malware associated with WannaCry exploited a vulnerability; it was not a zero-day vulnerability because its existence was actually already publicly known. While the NSA is suspected to have known about the vulnerability for years, Microsoft promulgated a patch designed to correct the vulnerability associated with the Shadow Broker's exploit two months before the attack took place. If system administrators and end-users had not been indifferent, apathetic, or were just simply more aware, the volume of victims and magnitude of damage could have been drastically reduced if not entirely nullified.

Despite the public sharing some level of culpability, Microsoft executives wasted no time directing blame towards the NSA and the USG. Brad Smith, the company's Chief Legal Officer held little back in a blog post. Smith (2017) asserted, with CIA exploits discovered on WikiLeaks and vulnerabilities being stolen from NSA, a dangerous pattern had emerged. He believed WannaCry was the conventional equivalent of the U.S. military discovering some of its Tomahawk missiles were stolen. Smith claimed the two greatest threats to cybersecurity were nation-state action and organized crime, effectively equating the two. He concluded by urging nation-states to consider the damage done to civilians from hoarding vulnerabilities. The gauntlet was thrown; the public was outraged.

The Trump administration formally responded on November 15, 2017, with the public release of an updated VEP. The previous administration was notoriously guarded on all things cyber. When Michael Daniel (2014) wrote his blog post to refute the Bloomberg's article's claim, he never directly mentioned the VEP. Instead, he referred to a "rigorous and high-level decision-making process" (p. 1). Many cybersecurity professionals were surprised, yet pleased, with the Trump administration's unprecedented

departure from the norm (Crocker, 2017; Spring, 2017; Whittaker, 2017). As the VEP's disclosure was roughly a year after WannaCry, many also suspected the policy update was a response to the attack. The timing of the VEP's public release is telling, but perhaps more than WannaCry factored into the public disclosure decision.

Prospective legislation may have also forced the administration's hand. On May 17, 2017 Representative Ted Lieu introduced House Resolution (H.R.) 2481 the Protecting our Ability to Counter Hacking Act of 2017, or the PATCH Act of 2017. On the same day it was introduced, the PATCH Act was referred to the House Committee on Oversight and Government Reform. No subsequent action has been taken on H.R. 2481. But the 2017 VEP (VEP17) released by the Trump administration seemed to borrow heavily from recommendations found in the PATCH Act. They both allowed for annual publicly released reports, encouraged the highest level of transparency possible, favored responsible disclosure over restriction, and were structured near identically. H.R. 2481 proposed six permanent and four ad hoc members; VEP17 has ten permanent members, with nine of ten being identical to the PATCH Act.

A major difference between the policy and the legislation was who ran the process. The legislation gave primacy to the DHS and afforded no Executive Secretariat. VEP17 kept the NSA IAD as Executive Secretariat and control of the process at the NSC, with the Special Assistant to the President and Cybersecurity Coordinator or equivalent successor assigned as director. Respectively, these moves could be regarded as somewhat controversial and impressively prescient. The Executive Secretariat is an independent and neutral facilitator (White House [WH], 2017b). Some questioned if the NSA, with its track record, let alone its purpose for existing, would be capable of maintaining neutrality with disclosure or retention determinations (Knake, 2017; Crocker, 2017). The prescient part is with regard to "or equivalent successor." On May 15, 2018, the Cybersecurity Coordinator position was eliminated (Perlroth & Sanger). The job's responsibilities were split between two senior directors into offensively and defensively focused roles. Both report to National Security Advisor.

VEP17 is not law, nor is it an Executive Order (E.O.). The Trump administration's November 2017 release is an agreement between agencies (Knake, 2017). While it may

not have the permanence of an E.O. or law, it is still a binding agreement with a focused purpose. VEP17's purpose is to make the restriction or disclosure determination through the balancing of equities:

> The primary focus of this policy is to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes (WH, 2017b, p. 1).

The following section will address how VEP17 defines its purpose and sets its focus, transitioning from documenting the policy's history and influences to analyzing how it measures up against a utilitarian moral obligation.

C. VEP FOCUS, THRESHOLD, AND EXEMPTIONS

This section analyzes VEP17's focus and threshold statements as well as its policy exemption section. Specifically, it addresses the morally problematic issues created when the policy's focus is reconciled with its self-defined threshold of applicability, as well as ethical issues stemming from the policy's exemption section. VEP17's exemption section has two main troubling elements: non- disclosure agreements and sensitive operations. Incidentally, the FBI made headlines involving both. This section also evaluates the FBI's conduct in each case in terms of the utilitarian moral obligation defined in this thesis.

The FBI is the focus of the exemption section for a variety of reasons, primarily because it is an entity of the USG with a permanent seat on the ERB that also has a public record of recent uses of applicable capabilities. Additionally, whether a person's moral sensibilities skew utilitarian or deontic, the FBI's behavior in both instances is morally questionable. The analysis of their behavior in these instances will carry forward to the next section and serve as a guide to determine if the VEP, as written, and if the ERB, as constituted, fulfills Mill's utilitarian obligation.

1. Focus and Threshold

First, the framing and contextual element of scope should be addressed. VEP17 supersedes the Obama Administration's *Commercial and Government Information*

Technology and Industrial Control Product of System Vulnerabilities and Equities Policy and Processes but does not override any existing U.S. law, E.O, regulation, or directive (WH, 2017b). Barring the two exemptions that are addressed later in this section, the policy has across-the-board application to all personnel: government, military, and contractors, as well as software and hardware. How the policy sets its threshold criteria for vulnerability applicability effectively turns VEP17 into the USG's zero-day policy: "To enter the process, a vulnerability must be both newly discovered and not publicly known" (WH, 2017b, p. 5). The "newly discovered" stipulation has less to do with zero-days and more to do with extending a grandfathered exemption to any vulnerabilities currently in use. The "not publicly known" vulnerability requirement is exactly what makes this policy specifically apply to zero-day vulnerabilities.

If balance is the one word to describe the policy's purpose, transparency would be the second. While VEP17 defines public interest as the policy's primary focus, the policy's threshold criteria require the vulnerability not be publicly known. This means the policy requires the ignorance of the group whose interests in prioritizes. If more information is preferred to less, prima facie, a policy focused on the public interest yet requiring the ignorance of the public is troubling. However, the ignorance requirement is inherent to the nature of zero-day vulnerabilities. It is not an artificial requirement added by the government. Once the vulnerability is publicly known, it ceases to be a zero-day. Public ignorance is not required by policy. It is required by definition. Consequently, it would seem unfair to criticize VEP17 on that basis, when the whole point of the policy is to facilitate decisions on public disclosure. However, this predicament, albeit unfairly, is at the core of zero-day policy criticism. While the public release of VEP17 was a watershed event for cyber-policy in terms of transparency, the disclosure was still subject to criticism. While the response was largely positive, some in the private sector still questioned transparency.

Industry professionals agree that the public disclosure of the terms of VEP17 feels like a step in the right direction, but still claim too much of the policy is shrouded in secrecy (Spring, 2017). VEP17 does allow for annual public reporting, which is an improvement upon the previous policy. The public reporting should add to the "everything is above

board" notion the USG is interested in promoting. The problem is "the not publicly known" requirement, though undeniably justifiable, still makes some people wary. Cybersecurity watchdog, EFF, while pleased with the increase in transparency, remains suspicious: "Nevertheless, we still have concerns over potential loopholes in the policy, especially how they may play into disputes about vulnerabilities used in criminal cases" (Crocker, 2017). WannaCry and Heartbleed understandably increased the American public's skepticism relating to the USG and cyber-loopholes. Furthermore, it seems the EFF's concerns were merited. The next two sub-sections analyze high profile examples of how cyber-policy loopholes affected criminal proceedings, and how the loopholes can be judged in terms of Mill's utilitarian obligation.

2. Exemptions

The policy has two exemptions that put vulnerabilities "subject to restrictions by partner agreements" and vulnerabilities related to "sensitive operations" outside the jurisdiction of the VEP (WH, 2017b, p. 9). Both exemptions are troubling from the point of view of Mill's utilitarian principles.

The details of what exactly constitutes a "partner agreement" remain classified. Experts point to Non-Disclosure Agreements (NDA) as an example and disapprove of this exemption (Knake, 2017; Crocker, 2017). NDAs potentially pose a major national security threat and can work against the public interest. The "sensitive operations" clause provides a potentially large loophole due to sensitivity determinations being largely discretionary.

The previous chapter discussed the potential moral value offered to policymakers by Mill's qualitative allowance. However, discretion can also be dangerous. As the discussion of this section demonstrates, USG activities, specifically by the FBI, provide two examples, one related to sensitive operations and another related to NDAs, where ill-conceived judgement related to zero-day vulnerabilities resulted in the institution's failure to live up to the utilitarian moral obligation and arguably a failure of the institution as a whole.

a. Sensitive Operations—An Immoral Playpen

The FBI conducted a sting targeting child pornographers by running a site called "Playpen" on the Tor network, also known as the dark web (Tierney, 2017). The American judicial system confers upon the defendant the right to know how evidence against them was obtained. The process is called discovery. The judge in this case was not interested in making exceptions for "sensitive operations." He told the FBI to show how the evidence was acquired or the charges would be dropped (Newman, 2017). The evidence was gained through the exploitation of software vulnerabilities, malware, the FBI deemed too sensitive to disclose. Consequently, in March of 2017, they chose to drop charges, and the *United States v. Jay Michaud* was dismissed (Newman, 2017). In an interview with Gizmodo, NYU adjunct professor Zachary Goldman clarified the significance of the FBI's decision stating, "this doesn't mean that the FBI's investigation was unjust or unjustified.… The FBI is placing paramount importance on preserving the ability to use this technique in the future" (Nunez, 2017, p. 1).

On its face, allowing a child pornographer to go free is clearly not in the public interest. By putting "paramount importance" on preserving the secrecy of its broader activities, the FBI was effectively requiring the public to take on faith that the FBI acted on a more compelling judgment of the "public interest." The critical question this episode poses for this thesis is whether such a decision, and its incumbent secrecy, is justifiable in terms of Mill's utilitarian principles.

With regard to the VEP17 specifically, it would be unfair to hold the FBI to a policy standard that did not even exist. VEP17 was released in November. The decision to drop charges was made in March. Furthermore, while VEP17 established public interest as its focus, *Commercial and Government Information Technology and Industrial Control Product of System Vulnerabilities and Equities Policy and Processes,* the actual policy at the time, did not. Nowhere in the 15-page document was public interest or public good mentioned. In fact, on April 24, 2014, an FBI Equity Discussion on "the Use of Zero-Days & Policy" charged the ERB with the focus of making all disclosure versus retention determinations "in the best interest of intelligence collection, investigative matters, and information assurance" (Federal Bureau of Investigation [FBI], p. 9). If the FBI elected to

drop charges because it did not want to compromise current and prospective operations, then they made the decision in accordance with policy. This previously classified document, while being heavily redacted, still manages to give insight into the policy ramifications that inform ERB members' decisions. But it does not answer the underlying question of whether the FBI action satisfies a conception of the "public interest."

Act or direct utilitarianism holds it would be morally right to let one child pornographer go if that meant more would be arrested in the future. Ultimately, it is the result that matters; act utilitarianism is an ends-based morality. If the FBI was willing to sacrifice a small gain now, letting one child pornographer go, for a large gain in the future, arresting all child pornographers associated with the "Playpen" sting, then the decision is justified on doctrinal and moral grounds. In effect, this was a case of the FBI pushing the Fat Man in front of the Cart.

But Mill is no act utilitarian. Mill's utilitarianism is best understood as indirect. Part of Mill's utilitarian obligation requires the government set the example through conspicuous demonstration of virtuous behavior, especially in the most trying times. While remaining ultimately concerned with the greater good, Mill's utilitarianism also requires a consideration of the means. By itself, a government institution electing to drop charges would be difficult to regard as good behavior. However, while not strictly virtuous, both morality and virtue could be redeemed if a legitimate greater good was affected. The problem here is bigger than one child pornographer. It is not merely that the FBI let Jay Michaud roam free, it is that they did so because they refused to comply with discovery, a right of the public conferred by the Constitution's Sixth Amendment provisions that all accused persons may know the evidence against them. Refusing to adhere to a provision designed to ensure equitable adjudication, when the provision's exclusive purpose is the protection of American rights, means the FBI's decision to drop charges should be regarded as a failure to meet Mill's utilitarian moral obligation.

b. Non-Disclosure Agreements—A Public Disinterest

The other problematic VEP17 exemption is related to Non-Disclosure Agreements. NDAs have the potential to work against the public interest as well as national interest,

exemplifying how governmental agencies may fail to prioritize public interest over preservation of their own equities. Some believe certain agencies, namely the FBI, deliberately leveraged NDAs with the intent to circumvent the VEP (Brandom, 2016; Cox, 2016).

The case in point here is the FBI's interest in an exploit to unlock the iPhone of the San Bernardino shooter Syed Farook. The Department of Justice (DoJ), on behalf of the FBI, attempted to compel Apple to unlock Farook's iPhone. Apple was reluctant, citing privacy and public trust in the security of their products. The FBI was frustrated by Apple's equivocations and decided to purchase outside support. Subsequently, the DoJ abandoned the bid to force Apple to unlock the phone when the FBI successfully procured third-party assistance (Zapotsky, 2016). This situation, by itself, seems in keeping the utilitarian moral obligation. Syed Farook was a mass-murderer who went on a shooting spree that targeted his workplace's holiday party killing 14 people (Ahmed, 2014). Gaining access to his locked phone, with the intent of finding evidence to ensure all involved faced charges and prevent future attacks, would be in the public's interest. The problem is how the FBI did it.

The FBI paid a third-party private company to use their exploit. The purchase required signing an NDA. The agreement conferred sole legal ownership of the exploit to the company and barred the USG from disclosing the vulnerability (Hosenball & Menn, 2016). The NDA certainly protects the company's interests. Once the existence of the vulnerability is disclosed, the exploit no longer has value. Prohibiting the USG from disclosure allows the company to resell the exploit. But from the USG side, there are both public interest and national security concerns stemming from NDAs. Due to the NDA's potential asymmetric nature, cyber policy experts Ari Schwartz and Robert Knake called for government agencies to be prohibited from entering into NDA's with researchers and resellers of zero-day vulnerabilities: "The government must have exclusive rights to the vulnerability or tool. If it does not obtain these rights, including the right to disclose the vulnerability, it runs the risk that it could be sold or shared with other actors working against the national security interest of the United States" (p. 15).

VEP17 did not heed this recommendation. In fact, it did the opposite. It specifically provided exemptions for NDAs. NDAs are flawed when private gain has priority over public good. This does not mean all NDAs are morally problematic. The classification system is an example. Anyone with access to USG classified material must sign an NDA. In this example, national interest and public interest coincide. As NDAs relating to classification are both virtuous and aligned with the public interest, they fulfill Mill's moral obligation.

The critical factor that distinguishes the FBI's NDA from the classification NDA, with regard to fulfillment of Mill's moral obligation, is the signatory role of the USG. The USG role change affects whose information is being protected and from what. With regard to the classification NDA, the USG desires to share sensitive information with a private party, because in sharing the information, the USG's national and public interests are advanced. This form of NDA also serves to fulfill Mill's moral obligation concerned with the virtuous promotion of national interest. Once the information is shared with the individual, under the good faith presumption, the information is no less sensitive. Consequently, the individual must sign an NDA to legally bind the private party to never share the information with unauthorized entities or face severe statutory consequences. The NDA in this example restricts the individual's ability to disclose information on the basis of protecting the USG's national interests and the interests of the American public.

The roles are reversed in the case of the FBI's NDA. The restriction on the disclosure of information is no longer on an individual entity at the behest USG. Instead, the USG is the constrained party and the interests served by restriction are private. Rule utilitarianism calls for laws to be written to support the overall good. While the classification NDA can be said to do as much, the FBI's NDA is more problematic. Certainly, both NDAs involve an underlying transactional element, a service for compensation. That is to say, the FBI did not arbitrarily enter into the agreement; it signed the NDA with intent to gain access to Farook's phone to prevent further harm. This intent is both virtuous and in the public interest. The problem relating to Mill's moral obligation is not the FBI's intent. Rather, the problem is that the restriction placed on the USG, to serve the other party's private gain, resulted in a constraint on the overarching information

flow, changing the USG's role with regard to what information was being protected. The FBI's NDA protected information in part for reasons of private interest, and in doing so, failed to fulfill Mill's moral obligation of virtuous governmental behavior.

The previous two examples represented high-profile cases where the FBI failed its moral obligation to the public good in Mill's terms. They chose retention over disclosure and a child pornographer was set free. They signed an NDA barring them from disclosing an iPhone vulnerability leaving Americans at risk. The NDA also prevented the FBI from submitting the vulnerability to the VEP, a process designed to prioritize Americans' public interest. These incidents fall short of Mill's expectations because the FBI prioritized its own equities without a clear public accounting of how those actions advanced the interests of the American public, which the FBI is mission-bound to protect.

While these claims may seem to be a serious indictment of the FBI, the intent is to draw attention to the larger issue affecting the ERB as constituted. Not one of the ten permanent seats acts directly on behalf of the public interest, yet VEP17 defines public interest as its primary focus. The question then becomes, do the members of the ERB actually prioritize the public interest, or does the structure of the process leave them incapable of doing so? The problematic behavior of the FBI in the cases reviewed here raises larger issues for VEP17 and the ERB.

D. TRUST THE PROCESS?

All members of the ERB, to some degree, act on behalf of the public good. After all, they are institutions of a federal democratically elected representative government, not only of the people and by the people, but *for* the people. The issue at hand becomes to what extent? Some of the ERB's member's missions so closely align with that of the public good that any attempt to distinguish between pubic interest and that of their own would be rightly dismissed as a merely semantic distinction. For other ERB members, however, the convergence of those agencies' particular mission and the public interest in Mill's utilitarian sense is much more problematic. This section will evaluate each member of the ERB, based on mission and track record, to determine the likelihood of them keeping primary focus on public interest, rather than their own equities.

1. The ERB as Constituted

The Office of Management and Budget (OMB), the Treasury, the DHS, the Department of Energy (DoE), and the Department of Commerce (DoC) are the members of the ERB whose roles are most explicitly oriented toward public interest. OMB is essentially the business division of the Executive Branch. It is responsible for aligning the President's policies and programs with his budget (OMB, 2018). In addition to this primary responsibility, it manages the Executive Branch's information technology. Both the OMB's mission and responsibility to ensure safe and secure technology align its interests with the public's.

The Treasury's mission is also commensurate with the public good. It is not tasked with any cyber-specific items. The existence of a zero-day vulnerability would likely always be seen by it as a harm and not something to be exploited. Consequently, there is little chance any of its equities would not directly support the public good.

The DoC, DoE, and DHS missions are directly tasked with cybersecurity. "Enhance the Nation's Cybersecurity" is a core tenet of "Strategic Goal 3" in the *U.S. Department of Commerce Strategic Plan 2018–2022* (DoC, 2018). In addition to its own cybersecurity strategy, the DoE is responsible for the "Office of Cybersecurity, Energy Security, and Emergency Response" dedicated to addressing "the emerging threats of tomorrow while protecting the reliable flow of energy to Americans today by improving energy infrastructure security" (DoE, 2017). Of the five ERB members listed so far, none is more directly concerned with public interest than the DHS. Not only does DHS preside over 14 active cybersecurity programs on behalf of the American public, its cybersecurity strategy is written with public interest as the paramount concern. Consequently, the DHS is most likely to consistently prioritize public good.

The Department of State (DoS) is more difficult to classify with regard to propensity for consistently prioritizing public interest over zero-day related equities. The DoS has a cyber-specific mission. The "Office of the Coordinator for Cyber Issues" (CCI) carries out the tasking. The CCI's homepage enumerates five responsibilities; each bullet mentions some aspect of cyber issues, although no bullet mentions cybersecurity (CCI).

The absence anywhere on the CCI's homepage of the word cybersecurity suggests that, while the State Department is interested in cybersecurity, since cybersecurity is undeniably a cyber issue, the DoS is also interested in a broader range of cyber-related issues.

This claim feels more legitimate when considering the three aforementioned members of the ERB, with cyber related tasking and interests closely aligned with the public. All were focused specifically on cybersecurity, not an amorphous cyber issue. Of the previous five only the Treasury did not have a link to something cyber related. Of the four agencies that provided a link to something cyber related, that something was cybersecurity. Furthermore, the DHS and DoE publish their own cybersecurity policies.

The four most problematic agencies or institutions on the ERB are the NSA, CIA, FBI, and ODNI. They are not problematic in the sense that they cannot be trusted or fail at their mission. All four have a distinguished track record of defending Americans from all threats, foreign and domestic. All four also are tasked with missions inclining them to favor the protection of their cyber equities on the basis of more abstract and long-term conceptions of the "public good" that would lead to policies and behaviors falling short of Mill's standards for virtuous government behavior. The previous section discussed the shortcomings of the FBI's track record with regard to the "Playpen" and the San Bernardino shooter episodes. Similarly, the NSA had suspected involvement with HeartBleed and confirmed involvement with WannaCry. The CIA was embarrassed by WikiLeaks. These incidents, rooted in decisions to maintain rather than disclose vulnerability equities, raise questions concerning the roles these agencies can play on the ERB, which is ostensibly meant to prioritize public disclosure.

All together, the agencies comprising the ERB represent a spectrum of missions with varying degrees of institutionalized privileging of vulnerabilities non-disclosure. Some may be more inclined to make disclosure their primary focus on the ERB. Others have demonstrated the propensity to value their own equities over the broader interest of public disclosure. Consequently, no conclusive determination can be made with regard to how well the design and membership of the ERB will incline it to satisfy Mill's conception of moral obligation.

2. Considerations on Executive Review Boards

Annex B of VEP17 contains 25 considerations intended to inform the judgment of ERB members when making the restriction or disclosure decision. It is not an exhaustive list. Disclosure versus restriction "evaluations will not be limited to applying only these considerations, but these represent general concerns, which should apply to all vulnerability equity decisions" (WH, 2017b, p. 13). Annex B is divided into four categories: "Defensive Equity Considerations," "Intelligence, Law Enforcement, and Operational Equity Considerations," "Commercial Equity Considerations," and "International Partnership Equity Considerations" (WH, 2017b). Some of the guidance dispersed throughout these four categories is problematic. Through an examination of Annex B, this thesis seeks to gain insight into the actual primary focus of VEP17: public interest or institutional equity.

a. Defensive Equity Considerations

"Defensive Equity Considerations" is divided into four sub-sections: Threat Considerations, Vulnerability Considerations, Impact Considerations, and Mitigation Considerations. The Threat Considerations portion contains three considerations. The guidance in this section suggests the ERB consider where and how the product is used, the range of products and versions affected, and the likelihood of malicious actors exploiting the vulnerability (WH, 2017b). There are no problematic issues here. The guidance appears closely linked to the priority of disclosure and responsible governmental behavior, in keeping with the utilitarian moral obligation.

The Vulnerabilities Consideration portion is also very aligned with the moral obligation, just not as directly linked as the previous section. This sub-section is more concerned with the nature of the vulnerability than the potential magnitude of harm. It is still concerned with damage done, but it is more of a second order effect, only one consideration directly expresses concern for harm. This section asks questions like, "what access must a threat actor possess to exploit this vulnerability" and "how likely is it that threat actors will discover or acquire knowledge of this vulnerability" (WH, 2017b, p. 13).

The Impact Considerations and Mitigation Considerations sub-sections have problematic considerations with similar themes. The Impact section asks "will enough USG information systems, U.S. businesses and/or consumers actually install the patch to offset the harm to security caused by educating attackers about the vulnerability" (WH, 2017b, p. 13). The Mitigation section asks "if the vulnerability is disclosed, how likely is it that the vendor or another entity will develop and release a patch or update that effectively mitigates it" (WH, 2017b, p. 14). The mitigation section contains a similar question that reframes the consideration with an emphasis on timeliness, "if a patch or update is released, how likely is it to be applied to vulnerable systems? How soon? What percentage of vulnerable systems will remain forever unpatched or unpatched for more than a year after the patch is released" (WH, 2017b, p. 14). These considerations are not concerned with any intrinsic value associated with patches, but rather with the likelihood of the public installing them, companies creating them, and both being done in a timely fashion.

Objectively, there is nothing wrong with the ERB asking if the patch would be used. Strategically, it would be foolhardy to not consider a value-based decision. Even in conventional act utilitarian terms, if only a small fraction of the population would actually install the patch, and continued law enforcement and intelligence gains were obtainable with an unpatched vulnerability, not only would asking the question be ethically sound, choosing to restrict versus disclose would be morally justified.

However, while objective in the sense that it is impartial, Mill's utilitarianism is neither direct nor opportunistic. Indirect utilitarianism requires both the ends and the means to be considered. The moral obligation Mill levied upon the government was to set the example in action, to do what ought to be done. If a decision by the ERB to disclose and patch, on the basis of its basic obligation, becomes a decision to restrict knowledge due to skepticism related to likelihood of patching, then the ERB falls short of its moral obligation, in Mill's terms, to behave virtuously and lead by example. Setting the example and doing what ought to be done is irrespective of effect produced. This should not be construed as doing the right at the expense of the good. It is fair to question the efficiency of fulfilling such an obligation in the short run. But it is also fair to recognize the overall

good generated by improved public sentiment through the observation of government consistently setting a virtuous example.

b. Intelligence, Law Enforcement, and Operational Equity Considerations

Part two of Annex B, "Intelligence, Law Enforcement, and Operational Equity Considerations," has two sub-sections with seven total concerns. The troublesome issues in this section relate to the nature of focus, which is to say, whether or not the public interest is more often than not the primary focus or relegated to an additional or tangential concern. The public good, in these two sub-sections, cannot unequivocally be considered the primary focus. This reality was recognized by a Presidential working group commissioned with a mandate to reconcile situations where the pursuit of national interest compromises privacy and civil liberties. The working group determined "excessive surveillance and unjustified secrecy can threaten civil liberties, public trust, and the core processes of democratic self-government" (WH, 2013, p. 14). It also acknowledged "at the same time, the United States is deeply committed to the protection of privacy and civil liberties—fundamental values that can be and at times have been eroded by excessive intelligence collection" (WH, 2013, p. 16). The working group statement is not merely acknowledging that privacy and civil liberties erosion has occurred, but that it has occurred because of "excessive" activities beyond justification on national security grounds. The agencies associated with this sub-section are the ones associated with the erosion. Consequently, the potential for public interest to be something other than the primary focus of these agencies has the greatest potential of occurring here.

Determining whether or not the considerations in this subsection fulfill Mill's moral obligation is not as clear-cut as previous sections. With significant overlap between national and public interest, while allowing for the potential of mutually exclusive interests, it can only be said that there are times when considerations in this section will put national security interest over the public privacy and civil liberty interest, and possibly leave Mill's moral obligation unfulfilled. This is assessed as possible because there may be times where the overall good increased by prioritizing the pursuit of national security interests over those of public disclosure and privacy protection is so large that it meets the obligation.

A means-based analysis largely validates the considerations in the two sub-sections on Mill's moral grounds. Mill expects the government to set the example and to do what ought to be done. The agencies in this section are expected to accomplish their mission and the considerations in this section are mission focused. If the agencies conduct themselves in good faith with no ulterior motive, then the moral obligation is fulfilled. If they deliberately leverage loopholes and knowingly misrepresent intentions, then they fail Mill's moral obligation of virtuous and exemplary conduct.

c. Commercial and International Equity Considerations

Part three, Commercial Equity Considerations, and part four, International Partnership Equity Considerations, will be addressed together as they both only have one concern. The guidance offered in both, while having different subjects, shares the same problem: a potential compromise of civil liberties and privacy. The commercial equity section asks, "if USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG relationships with industry," while the foreign equity section is concerned with "if USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG international relations" with other countries (WH, 2017b, p. 14). Neither consideration mentions public good or public interest. The claim is not that USG interests are consistently divergent with protection of the American public's interest in civil liberties and privacy, but it is undeniable that they can be. Moreover, history shows that USG activities can be captured by parties seeking private gain, trumping the public good for all. Ultimately, any assessment of fulfillment of moral obligation can only be done after the fact, with knowledge of intent, means, and effect. While it cannot be said that this section fails to meet the moral obligation to the public good, it can be said with the acknowledgement of potential for interests to diverge, that the section would be more in line with Mill's obligation if some specific public element was added.

d. Filled… But Not Fulfilled

Of Annex B's 25 total considerations, most are consistently in the public's interest and align with the utilitarian moral obligation, but not all of them. In a traditional utilitarian sense, "not all of them" is a non-issue. Utility seeks overall good, which can be achieved

through majority satisfaction. If the majority of considerations focused on the public interest and support the public good, then Annex B would fulfill the utilitarian moral obligation. But, as elaborated in Chapter II, Mill's utilitarianism is not traditional. His version requires concern for both achieving the greater good and how the good was achieved. Indirect utilitarianism requires the consideration of factors in addition to happiness. The preservation of freedoms and liberty, as well as proper conduct, are among them.

Utilitarianism, as defined by John Stuart Mill, is rule and sanction based, applied indirectly. Under those terms, Annex B does not fulfill the utilitarian moral obligation. As described in the previous chapter, after the jurisdiction of morality has been established, sanction-based utility essentially becomes rule utility. Rule utilitarianism states that overall utility is best increased through the creation of, and adherence to, a set of rules designed and agreed upon, to increase overall utility. Where act utilitarianism evaluates each individual action on its own terms, rule and sanction utility advocate for a broader rule or law-based determination. This approach better suits the machinations of government and the creation of policy.

VEP17 began on nearly ideal rule utilitarian terms. The second sentence of the policy's first page established public interest as its primary focus. If Annex B was written with each consideration not necessarily primarily focused on the public interest, but with the intent of increasing the overall public good, then Annex B could be considered commensurate with rule utilitarianism. It would be hard to justifiably claim USG policy was written for something other than the American public good without evidence of it being used otherwise. In fact, under a good faith presumption, all USG policy would satisfy rule utilitarian terms. In representative government, the likelihood of good faith and the consistency with which faith is unbroken is largely dependent on the public (Mill, 2009a).

Mill knew as much, which is why he believed the government should set the example through action, value liberty and freedom, and cultivate virtue in its citizens. As the government is formed from the people, if it is a government that achieves all three, then it will assuredly and consistently produce policy in good faith, commensurate with rule utility, and in fulfilment of moral obligation. The minds of the policy makers that produced

VEP17 cannot be known and the policy is not without flaws. It cannot be said to strictly conform to rule utilitarianism and only time will tell if the obligation is fulfilled.

E. CONCLUSION

The USG has repeatedly maintained that the restriction versus disclosure determination was heavily biased towards responsible disclosure. Yet, government agencies and institutions have been repeatedly caught in compromising situations that cast doubt on this claim, regardless of how frequently or vociferously the USG has made it.

The American people complained the policy was shrouded in secrecy and lacked transparency. VEP17's public release answered both criticisms. But scrutiny of the policy indicates potential for interests other than public good to be served.

Moral policy is important, but so is strategic policy; likewise, so is balance. One does not have to come at the expense of the other. Rather, as Mill's utilitarianism mandates a choice that considers ends and means, good policy should consider both moral and strategic dimensions. VEP17 is not a fundamentally flawed policy if it does not fulfill every aspect of Mill's very exacting moral obligation. However, Mill's morality indicates where improvements can be made. VEP17, in composition and language, does not do enough to ensure institutional equity is not at the expense of public interest.

THIS PAGE IS INTENTIONALLY LEFT BLANK

IV. IF NOT ZERO DAYS, HOW MANY?

A. OVERVIEW

This thesis set out to apply the moral principle of utilitarianism to the policy problem associated with zero-day vulnerabilities, which can be understood as errors in coding that are potentially exploitable and unknown to either the creators or users of the software. If attack vectors related to zero-day vulnerabilities are completely dependent upon correctable coding errors, what should policy require when the U.S. government detects a zero-day vulnerability: disclose it publicly so it can be patched, or restrict knowledge of it so it can be weaponized? To inform this larger question, this thesis has focused on a more specific question: what does utilitarianism say the USG should do and how would this moral principle evaluate and inform the Federal Government's zero-day policy?

In the aftermath of Heartbleed and WannaCry, the USG's handling of zero-day vulnerabilities was subject to increased criticism (Holland, 2017; Ng, 2017). A major portion of the public's suspicions stemmed from a lack of transparency (Smith, 2017; Spring, 2017). Democratic representative governments derive much of their legitimacy from transparency, but cyberspace has complicated the long-standing practice of public disclosure. Many of the operations in cyberspace are classified, as they rely on sources and methods that cannot be immediately publicly known. Consequently, the information is not released for years, sometimes decades, after the fact. The aggregate aftermath of Edward Snowden, WikiLeaks, HeartBleed, and WannaCry severely damaged Americans' trust in their government.

In an effort to assuage misgivings and rebuild trust, the Trump administration publicly released its zero-day policy, a move generally considered as remarkable as it was unprecedented. The Federal Government provided clear, legalese-free policy detailing the USG's process for making the zero-day determination.

This thesis has been concerned with moral evaluation of the policy, first to establish the utilitarian moral obligation of a nation-state, then to apply the terms of that obligation to the USG's zero-day policy and determine if the obligation was met.

Utilitarianism is traditionally understood as a single principle moral theory concerned with improving happiness, either by increasing pleasure or decreasing pain. John Stuart Mill's version is not traditional, it requires more. Through an analysis of Mill's work, this thesis has developed a multi-faceted moral obligation, and determined a nation-state's primary moral duty. A nation's utilitarian obligation is to the public good. In practice, the USG zero-day policy has a single focus on national interest with multi-faceted considerations. Prima facie, the Vulnerabilities and Equities Policy, as designed, seems aligned with utilitarian principle. The focus of the policy was essentially the same as the utilitarian obligation conferred upon the government. However, further scrutiny did not entirely favor the face value assessment.

While the policy's focus was effectively identical to the moral obligation's terms, there were aspects that diverged from or were incongruent with the moral obligation. There was undeniable potential for the policy's implementation to run contrary to its focus. Additionally, it created major loopholes by offering exemptions to vulnerabilities involved with sensitive operations or protected by NDAs. VEP17 utilized an Executive Review Board to make the best possible disclosure versus restriction determination, with half of the board having questionable institutional motivations and behavior related to the very topic they were expected to prudently preside over. Furthermore, VEP17 kept the agency many considered least capable of transparency and objectivity, an assessment tacitly endorsed by the PATCH Act, in the role of Executive Secretariat. The NSA was put in a position that is expected to be, above all else, objective and impartial, while remaining an agency that is also frequently a vulnerability equity stakeholder, with institutional motivations to favor retention over disclosure.

Finally, there are the issues posed by Annex B. Annex B of VEP17 provides a list of considerations to inform ERB member's decisions regarding zero-day vulnerabilities. The list was neither exhaustive nor exclusionary, but all considerations are intended to be applied to every zero-day decision. Rule utilitarianism holds that all regulations, ranging

from those codified in law to agreements unspoken, be made with the express purpose of increasing overall utility, meaning for the public good or in the public interest. Some considerations prescribed in Annex B kept the public's interest in focus and increased the overall good. Therefore, some fulfilled the utilitarian moral obligation. Some did not. Some considerations advocated for interests not self-evidently convergent with the broader public good, while others presented a potential for a conflict of interest. The preponderance of VEP17's considerations was in the public interest, but according to rule utilitarianism, the majority is not enough. Every rule must be written to improve overall welfare. While the policy does not fully comply with rule utilitarianism, with structural and procedural improvements, it could still serve as mechanism for the USG to fulfill the moral obligation.

B. POLICY RECOMMENDATIONS

The first policy recommendation is an existential one; the VEP should no longer be an agreement between agencies but rather an Executive Order or a law passed by Congress. If codified as law it gains not only legitimacy and permanence, but Congressional oversight as well. Kevin Bankston, the director of the New America Foundation's Open Technology Institute, in an interview with *FCW,* said the PATCH Act "would codify what the White House claims it has had all along: a rigorous process, with all the key government stakeholders involved, that carefully considers the pros and cons of withholding the information and is strongly weighted in favor of disclosing it" (Carberry, 2017). The same holds true for VEP17.

Both laws and E.O.s have their strengths and weaknesses, relating to with whom the authority resides and how long the policy lasts. An E.O. derives its authority from the President and does not have the permanence of a law. What an Executive Order lacks in longevity, it makes up for in ease of implementation. Laws require consensus approval from two legislative bodies. Executive Orders require a signature. But Executive Orders are subject to legal limitations. Presidents understandably tend to prefer sacrificing durability if more control is conferred and execution is all but guaranteed. The current political climate has caused some to question the effectiveness of regulation through Presidential fiat.

It seems many of the unspoken rules of partisan politics have changed. The Obama Administration was famously unwilling to deal with Congress, largely because Congress, on more than one occasion, expressed their unwillingness to cooperate (Barr, 2010). In situations where compromise is unlikely or impossible, the President's recourse is an Executive Order. Issues arise if the subsequent administration is intent on undoing the work of its predecessor. Despite the fervor of the new administration's conviction, the process for undoing the previous administration's legacy is significantly more difficult if their predecessor's efforts are manifest through legislation. Ultimately, only a Presidential signature is required to undo an Executive Order. The Vulnerabilities and Equities Policy has the greatest likelihood of affecting lasting change as a set of regulations codified by Congress. Unfortunately, since zero-day policy through legislation takes power and flexibility away from the President, minus a perceived emergent need, the Vulnerabilities and Equities Process is very likely to remain an agreement between agencies.

A policy change that does not require an act of Congress and would immediately improve public trust concerns VEP17's exemption section. A vulnerability should not be excluded from the jurisdiction of the VEP and the consideration of the ERB due to a non-disclosure agreement. If the USG purchases only usage, but not exclusive rights to a vulnerability, and if the private entity has no restrictions on resale, it could then resell the same exploit, with no requirement to notify the USG of the sale or who purchased the malware. Situations like these have the potential to not only put the American public at risk, but compromise national security (Knake & Schwartz, 2016). If the VEP is truly in the public's interest and the USG is actually biased towards disclosure, then more vulnerabilities, not fewer, should be subject to the process. The exclusionary provision related to NDAs means fewer vulnerabilities are eligible; that needs to change.

The easiest policy correction with the most obvious solution is in regard to the VEP's Executive Secretariat. Of all ten permanent members of the ERB, the one that seems consistently embroiled in some cyber-related controversy is the NSA. Incidents like WannaCry and HeartBleed, regardless of the degree of NSA culpability, impugn the NSA's reputation nonetheless. An Executive Secretariat is a neutral facilitator, yet no agency consistently has more vulnerability-related equities than the NSA. Even if the NSA could

be consistently impartial, it seems unreasonable to expect it to do so, as it is frequently an equity stakeholder – just as it is unreasonable to put a fox in charge of a henhouse and then expect it to keep its paws off the hens. The NSC would be wise to heed the advice of Schwartz and Knake (2016). If the Executive Secretariat is supposed to be an objective facilitator, and the USG is legitimately interested in increased transparency, then the Department of Homeland Security should serve in that capacity.

Other opportunities to improve transparency and accountability in the vulnerability equities process design might be considered. Some ideas include increased Congressional oversight; an advisory group comprised of information technology firms and experts; judicial oversight (similar to the FISA process); and a watchdog entity composed of private citizens able to obtain requisite clearances.

C. FUTURE RESEARCH

This thesis was concerned with moral obligation in utilitarian terms. Other normative moral theories exist that can also provide valuable insight. The first one that comes to mind is utility's foil, deontology. As noted in the previous chapter, deontology is generally concerned with magnitude of rightness. While utilitarianism has been adopted by politicians on both sides of the aisle, deontology has not received as warm a political welcome. While utilitarianism can be criticized as cold, it is also more pliable. Resourceful politicians can use the "for the greater good" sentiment to transform the expedient into the morally justified. The same cannot be said for deontology. Deontic morality is largely intractable. Right is right and wrong is wrong, with little to no leeway afforded. Value based judgements are not made with regard to quantity or quality. They are made with regard to right or wrong. Although it would likely be a purely academic pursuit, it would still be interesting to see how deontology informs and evaluates the Vulnerabilities and Equities Policy.

John Stuart Mill is considered a primary exponent of utilitarianism, but he lived in Victorian England. Even utilitarianism's next great herald, Henry Sidgwick, who wrote *The Methods of Ethics*, regarded by many as the definitive treatise on moral theory, barely lived to see the 20th century ("Henry Sidgwick," 2015). While moral theory should remain

true irrespective to time, there is additional value in applying a more contemporary understanding. Further research should be done using modern moral and political philosophers to gain more insight into the best possible answer to the zero-day decision. Excellent candidates would be John Rawls, Bertrand Russell, or Alasdair MacIntyre.

Another research topic, less interested with morality and more directly related to policy, concerns VEP17's public reporting provision. VEP17 states an annual report will be provided to the ERB's permanent members' representatives and to the NSC staff at the lowest classification possible, with an unclassified executive summary at a minimum (WH, 2017b). It then states, "as part of a commitment to transparency, annual reporting may be provided to the Congress" (2017, p. 5). Notice "will" or "shall" are not used, instead the policy opts for "may." This is an important distinction. The annual public reporting requirement was heralded as proof of a commitment to transparency. Yet, no such requirement exists, which forces one to question the commitment as well. There are a number of future research concerns to address: does the VEP willingly provide an unsolicited public report, do they decide to wait and only produce if Congress asks, if Congress asks do they comply, and finally if no USG entity requests a report, will a third-party watchdog like EFF submit a FOIA request to generate a report?

The Trump administration continues to advance cyber causes on policy and doctrinal grounds. While not watershed like the public disclosure of VEP17, the administration's release of the *National Cyber Strategy* was still a landmark (White House, 2018). While not always mutually exclusive, moral and strategic imperatives are often at odds. Consequently, any analysis of strategic policy in terms of Mill's utilitarianism would likely raise concerns. Future research would be well served to evaluate the *National Cyber Strategy* in terms of Mill's utilitarianism in an effort to identify places where policymakers let overzealous pursuit of national interest get the best of them, places where Mill's moral framework could temper zeal into prudence and rectitude.

Finally, conducting research at the classified level would provide the most accurate assessment of conformity to rule utilitarianism and fulfillment of moral obligation.

LIST OF REFERENCES

Ablon, L., & Bogart, A. (2017). *Zero days, thousands of nights.* Santa Monica, CA: RAND Corporation.

Ablon, L., Libicki, Martin C., & Webb, T. (2015). *The defender's dilemma: Charting a course toward cybersecurity*. Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=2075897&query=

Actual Ransom [@actual_ransom]. (2017, July 31). Status of WannaCry wallets [Twitter]. Retrieved from https://twitter.com/actual_ransom

Ahmed, S. (2015, December 4). Who were Syed Rizwan Farook and Tashfeen Malik. Retrieved from https://www.cnn.com/2015/12/03/us/syed-farook-tashfeen-malik-mass-shooting-profile/index.html

Ballhausen, T. Friesinger, G., & Grenzfurthner, J. (2010). *Urban hacking: Cultural jamming strategies in the risky spaces of modernity.* Verlag, Bielefeld: Transcript.

Barr, A. (2010, October 28). The GOP's no compromise pledge. Retrieved from Phttps://www.politico.com/story/2010/10/the-gops-no-compromise-pledge-044311

Bentham, J. (2017). *An introduction to the principles of morals and legislation.* Retrieved from https://www.earlymoderntexts.com/assets/pdfs/bentham1780.pdf

Boyle, J. (1997). *Foucault in cyberspace: Surveillance, sovereignty and hardwired censors.* Retrieved from https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1552&context=faculty_scholarship

Brandom, R. (2016, April 27). The FBI bought an iPhone hack, but not the right to tell anyone how it works. Retrieved from https://www.theverge.com/2016/4/27/11518754/fbi-apple-iphone-hack-vulnerability-disclosure-vep

Committee for Economic Development. (2017, September 27). Regulation & the economy: The relationship & how to improve it. Retrieved from https://www.ced.org/reports/regulation-and-the-economy

Cox, J. (2016, April 13). The FBI may sitting on a Firefox vulnerability. Retrieved from https://motherboard.vice.com/en_us/article/aekeq4/the-fbi-may-be-sitting-on-a-firefox-vulnerability

Crisp, R., (2002). *Routledge philosophy guidebook to Mill on utilitarianism.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=170060&query=

Crocker, A. (2017, November 16). Time will tell if the new vulnerabilities equities process is a step forward for transparency. Retrieved from https://www.eff.org/deeplinks/2017/11/time-will-tell-if-new-vulnerabilities-equities-process-step-forward-transparency

CSI (2017, August 14). Who are the Shadow Brokers? [Cyber Security Intelligence Blog]. Retrieved from https://www.cybersecurityintelligence.com/blog/who-are-the-shadow-brokers-2684.html

Daniel, M. (2014, April 28). Heartbleed: Understanding when we disclose cyber vulnerabilities. [the WHITE HOUSE Blog]. Retrieved from https://obamawhitehouse.archives.gov

de Vuyst, B. & Fairchild, A. (2005). Intellectual property rights, resource allocation and ethical usefulness. *Information ethics: privacy and intellectual property.* Retrieved from https://www.igi-global.com/gateway/chapter/full-text-pdf/22940

Deontology. (2018). In *Stanford encyclopedia of philosophy.* Retrieved October 21, 2018, from https://plato.stanford.edu/entries/ethics-deontological/

France. (2017). *Defence and national security strategic review.* Retrieved from https://www.defense.gouv.fr/layout/set/popup/content/download/520198/8733095/version/2/file/DEFENCE+AND+NATIONAL+SECURITY+STRATEGIC+REVIEW+2017.pdf

Fruhlinger, J. (2017, September 13). What is the Heartbleed bug, how does it work and how is it fixed. Retrieved from https://www.csoonline.com/article/3223203/vulnerabilities/what-is-the-heartbleed-bug-how-does-it-work-and-how-was-it-fixed.html

Fruhlinger, J. (2018, August 30). What is Wannacry ransomware, how does it infect and who was responsible. Retrieved from https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Fung, B. (2013, August 31). The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/?noredirect=on&utm_term=.0ad22f4abe85

Goldsmith, J. (2003). Against cyberanarchy. *Who rules the net?: Internet governance and jurisdiction.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=231619&query=

Goodin, D. (2015, February 16). How "omnipotent" hackers tied to NSA hid for 14 years-and were found at last. *Ars Technica.* Retrieved from https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/

Gray, J. (2003). *Mill on liberty: A defence.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=166838&query=

Guha, M. & Chatterjee, A. (2010). Morality and cyberspace: Intellectual property and the right to information. *Applied ethics and human rights: Conceptual analysis and contextual applications.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=840419&query=&ppg=295

Hamelink, C. (2000). *The ethics of cyberspace.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=420931&query=

HM Government. (2018). *National security capability review.* London, Cabinet Office. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf

Holland, P. (2017, April 15). Hacked NSA tools could put some Windows users at risk. Retrieved from https://www.cnet.com/news/hacked-nsa-tools-put-windows-users-at-possible-risk/

Hosenball, M & Menn, J. (2016, April 13). Apple iPhone unlocking maneuver likely to remain secret. *Reuters.* Retrieved from https://www.reuters.com/article/us-apple-encryption-whitehouse-idUSKCN0XB05D

Jacobson, D. (2008). *Utilitarianism without consequentialism: The case of John Stuart Mill.* Retrieved from https://www.jstor.org/stable/40606016?seq=1#metadata_info_tab_contents

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review,* 50(1193). Retrieved from https://www.ntia.doc.gov/legacy/ntiahome/privacy/files/CPRIVACY.PDF

Kay, Charles. (1997). Note on utilitarianism. [Wofford Department of Philosophy]. Retrieved from http://sites.wofford.edu/kaycd/utilitarianism/

Kimppa, K. (2005). Intellectual property rights - or rights to the immaterial-in digitally distributable media gone wrong. *Information ethics: Privacy and entellectual property.* Retrieved from https://www.igi-global.com/gateway/chapter/full-text-pdf/168385

Kirwan, G. & Power, A. (2012). *Investigating cyber law and cyber ethics: Issues, impacts and practices*. Retrieved from https://www.igi-global.com/gateway/chapter/full-text-pdf/59940

Knake, R. & Schwartz, A. (2016). Government's role in vulnerability disclosure: Creating a permanent and accountable vulnerability equities process. *Harvard Kennedy School.* Retrieved from https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf

Knake, R. (2017, November 16). Grading the new Vulnerabilities and Equities Policy: Pass. [the Council on Foreign Relations blog]. Retrieved from https://www.cfr.org/blog/grading-new-vulnerabilities-equities-policy-pass

Langde, R. (2017, September 26). WannaCry Ransomware: A detailed analysis of the attack. Retrieved from https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack/

Le Guin, U. (1973). *Those who walked away from omelas.* Retrieved from http://www.mccc.edu/pdf/eng102/Week%209/Text_LeGuin%20Ursula_Ones%20Who%20Walk%20Away%20From%20Omelas.pdf

Lee, T. (2014, April 11). The NSA may have known about Heartbleed for years – why didn't they warn us? *Vox.* Retrieved from https://www.vox.com/2014/4/11/5605496/the-nsa-may-have-known-about-heartbleed-for-years-why-didnt-they-warn

Lessig, L. (2001). The laws of cyberspace. In R. Spinello and H. Tavani (Eds.), *Readings in cyberethics* (pp. 124–134). Sudbury, MA: Jones & Bartlett.

Lessig, L. (2006). *Code: And other laws of cyberspace.* Retrieved from http://codev2.cc/download+remix/Lessig-Co0dev2.pdf

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution.* New York, NY: Dell Publishing.

Lyons, D. (1994). *Rights, welfare, and Mill's moral theory.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=272624&query=&ppg=88

Michelfelder, D. (2001). The moral value of information privacy in cyberspace. *Ethics and information technology.* Retrieved from https://search.proquest.com/docview/222252773?OpenUrlRefId=info:xri/sid:primo&accountid=12702

Mill J. (2011). *On liberty.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=770561&query=&ppg=34#

Mill, J. (2009a). *Considerations on representative government.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=435878&query=&ppg=234

Mill, J. (2009b). *A system of logic.* Retrieved from https://www.gutenberg.org/files/27942/27942-pdf.pdf

Mill, J. (2009c). *Utilitarianism.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=435879&query=&ppg=33

Mill's moral and political philosophy. (2018). In *Stanford Encyclopedia of Philosophy.* Retrieved September 17, 2018, from https://plato.stanford.edu/entries/mill-moral-political/#UtiStaCon

Moore, J. & Tavani, H. (2000). Privacy protection, control of information, and privacy enhancing technologies. In R. Spinello and H. Tavani (Eds.), *Readings in cyberethics* (p. 451–462). Sudbury, MA: Jones & Bartlett.

Moore, J. (1997). Toward a theory of privacy for the information age. In R. Spinello and H. Tavani (Eds.), *Readings in cyberethics* (p. 349–359). Sudbury, MA: Jones & Bartlett.

Ng, A. (2017, May 16). Hackers behind stolen NSA tool for WannaCry: More leaks coming. Retrieved from https://www.cnet.com/news/hackers-behind-stolen-nsa-tool-for-wannacry-more-leaks-coming/

Nissenbaum, H. (1997). Toward an approach to privacy in public: Challenges of information technology. . In R. Spinello and H. Tavani (Eds.), *Readings in cyberethics* (p. 487–492). Sudbury, MA: Jones & Bartlett.

ODNI. (2014, April 11). Statement on Bloomberg News story that NSA knew about the "Heartbleed bug" flaw and regularly used it to gather critical intelligence [Blog post]. Retrieved from http://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew

Perlroth, N. & Sanger, D. (2014, April 11). U.S. denies it knew of Heartbleed bug on the web. *The New York Times.* Retrieved from https://www.nytimes.com/2014/04/12/us/us-denies-knowledge-of-heartbleed-bug-on-the-web.html

Perlroth, N. & Sanger, D. (2018, May 15). White House eliminates cybersecurity coordinator role. *The New York Times.* Retrieved from https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html

Perlroth, N. & Sanger, D., & Shane, S. (2017, November 12). Security breach and spilled secrets have shaken the N.S.A. to its core. *The New York Times.* Retrieved from https://www.nytimes.com00/2017/11/12/us/nsa-shadow-brokers.html

Post, D. (2003). Against "Against Cyberanarchy." *Who rules the net?: Internet governance and jurisdiction.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=231619&query=

Powell, A. (2016). Hacking in the public interests: Authority, legitimacy, means, and ends. *New Media in Society.* Retrieved from http://journals.sagepub.com/doi/pdf/10.1177/1461444816629470

Pynnoniemi, K. (2018). Russia's national security strategy: Analysis of conceptual evolution. *The Journal of Slavic Military Studies,* 31(2). Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/13518046.2018.1451091?needAccess=true

Rawls, J. (1999). A theory of justice. Retrieved from http://www.univpgri-palembang.ac.id/perpus-fkip/Perpustakaan/American%20Phylosophy/John%20Rawls%20-%20A%20Theory%20of%20Justice~%20Revised%20Edition.pdf

Reed, C. (2010). How to make bad law: Lessons from cyberspace. *The Modern Law Review.* Retrieved from: https://www.jstor.org/stable/40926555

Riley, M. (2014, April 11). NSA said to have used Heartbleed bug, exposing consumers. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers

Russian Federation. (2016). Doctrine of information security of the Russian federation. Retrieved from http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Saini, R. & Vaisla, K. (2014, March 5). Analyzing of zero day attacks and identification techniques. Retrieved from file://comfort/aakil$/Desktop/02-AnalyzingofZeroDayAttackanditsIdentificationTechniques.pdf

Schneier, B. (2014, May 19). Should U.S. hackers fix cybersecurity holes or exploit them? *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/

Schneier, B. (2017, May 23). Who are the Shadow Brokers? *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/

Schrock, A. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media in Society.* Retrieved from http://journals.sagepub.com/doi/pdf/10.1177/1461444816629469

Senate Armed Services Commit0tee. (2014). Advance questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command. Retrieved from https://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf?utm_content=buffer878a9&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Smith, B. (2017, May 14). The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. [the Official Microsoft Blog]. Retrieved from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/?utm_medium=email&utm_campaign=news-alert&utm_source=app&irgwc=1&OCID=AID681541_aff_7593_1243925&tduid=(ir_cd9b41e2Ne88d4b651dd10784ac0be9f7)(7593)(1243925)(je6NUbpObpQ-kh5j8N9LCyceWW_UADG3PQ)()&irclickid=cd9b41e2Ne88d4b651dd10784ac0be9f7#sm.0001wquey01dm2dtaxetp6jihcs80&ranMID=24542&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-kh5j8N9LCyceWW_UADG3PQ&epi=je6NUbpObpQ-kh5j8N9LCyceWW_UADG3PQ

Solon, O. (2016, August 16). Hacking group auctions 'cyber weapons' stolen from NSA. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group

Spinello, R. (2000). *CyberEthics: Morality and law in cyberspace.* Sudbury, MA: Jones & Bartlett.

Spinello, R. (2007). *Intellectual property rights. Information ethics.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=291574&query=

Spring, T. (2017, November 16). White House releases VEP disclosure rules. Retrieved from https://threatpost.com/white-house-releases-vep-disclosure-rules/128917/

Szoldra, P. (2016, September 16). This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. *Business Insider*. Retrieved from https://www.businessinsider.com/snowden-leaks-timeline-2016-9

United Nations. (2018, Aug 24). Uphold international law. Retrieved from http://www.un.org/en/sections/what-we-do/uphold-international-law/

Warwick, S. (2001). Is copyright ethical? An examination of the theories, laws, and practices regarding the private ownership of intellectual work in the United States. In R. Spinello and H. Tavani (Eds.), *Readings in cyberethics* (p. 263–279). Sudbury, MA: Jones & Bartlett.

White House. (2003). *Liberty and security in a changing world.* Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

White House. (2017a). *National security strategy*. Washington, DC: White House.

White House. (2017b). Vulnerabilities and Equities Policy and process for the United States government. Retrieved from https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

White House. (2018). *National cyber strategy.* Washington, DC: White House.

Whittaker, J. (2004). *The cyberspace handbook.* Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=182170&query=

Whittaker, Z. (2014, April 12). How the NSA shot itself in the foot by denying prior knowledge of Heartbleed vulnerability. [ZDNet]. Retrieved from https://www.zdnet.com/article/how-the-nsa-shot-itself-in-the-foot-by-denying-prior-knowledge-of-heartbleed-vulnerability/

Whittaker, Z. (2017, November 15). Trump administration releases rules on disclosing security flaws. [ZDNet]. Retrieved from https://www.zdnet.com/article/trump-administration-releas00es-secret-rules-on-disclosing-security-flaws/

Wright, D. (2014). *John Stuart0 Mill's sanction utilitarianism: A philosophical and historical interpretation.* Retrieved from http://oaktrust.library.tamu.edu/bitstream/handle/1969.1/152774/WRIGHT-DISSERTATION-2014.pdf?sequence=1

Zapotsky, M. (2016, March 28). FBI has accessed San Bernardino shooter's phone without Apple's help. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html?utm_term=.623afc943a2f

Zetter, K. (2014, April 11). Report: NSA exploited He0artbleed to siphon passwords for two years. *Wired.* Retrieved from https://www.wired.com/2014/04/nsa-exploited-heartbleed-two-years/

Zetter, K. (2015, June 26). Turns out the U.S. launched its zero-day policy in Feb 2010. *Wired.* Retrieved from https://www.wired.com/2015/06/turns-us-launched-zero-day-policy-feb-2010/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California