A Virtue Ethics Analysis of the NSA's EternalBlue Exploit

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Bhaskar Singhvi

April 23, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____Bhaskar Singhvi_____

Introduction

In 2017, a cyberattack exploit called “EternalBlue” developed by the National Security Agency (NSA) was leaked by a group of hackers called The Shadow Brokers. This leak led to a series of serious worldwide ransomware attacks that used this tool in order to gain access to hundreds of thousands of Windows systems. At the time, this problem was deemed a security failure by leaders from the technology world, such as the president of Microsoft, to political leaders such as Russia’s prime minister.

Current literature points to how cyber espionage needs to be more secure as citizens are not only vulnerable from international actors, but also from weaknesses of their own government’s line of defense. However, the current discussion does not fully consider the morality of the NSA’s decision to not inform the appropriate actors of this vulnerability in a timely manner. By thoroughly evaluating the NSA’s decisions through ethical standards, engineers will further their understanding in what constitutes moral decision making, particularly in cases of cybersecurity.

In this paper, I will investigate whether the NSA’s decisions to develop and conceal the EternalBlue exploit for an extended period of time were socially responsible. By evaluating this case through virtue ethics, I will demonstrate how the NSA as an organization acted unethically by showing how they violated three core virtues for moral engineers: cooperativeness, competence, and seeing the “big picture.” By using news articles and principles of virtue ethics outlined by van de Poel & Royakkers, and Michael Pritchard, I intend to show how the NSA’s management of the exploit was immoral.

Background

Microsoft's Server Message Protocol is a mechanism by which computers receive and transmit information through a network. The NSA discovered a weakness in this protocol where they could send specific messages to a server running Microsoft's protocol in order to gain access to a computer remotely through the network. The NSA's intention to develop and keep EternalBlue was to conduct cyber espionage against foreign adversaries. In fact, the NSA is known to stockpile zero-day exploits — vulnerabilities that software vendor has known about for zero days. This generally means that software remains susceptible to any attacks that take advantage of that weakness. The NSA was able to keep EternalBlue a secret for five years until a data breach occurred in the organization in early 2017. Given that it was highly likely that malicious actors could use the exploit, the NSA was forced to reveal this vulnerability to Microsoft who were then able to quickly release a patch in March. However, not all systems had installed the patch which allowed hackers to release ransomware called "WannaCry" to outdated systems in May 2017. Ransomware is software that allows hackers to gain control of a computer or software and threaten the users to delete, use, or distribute the sensitive contents unless the user paid a fee, or ransom. The cost of WannaCry was estimated at $4 billion, and other attacks based on EternalBlue, such as "NotPetya," followed WannaCry also penetrated computers worldwide causing further billions of dollars of damages to both intellectual and physical property.

Literature Review

Journalists and public figures alike have condemned the NSA's practice of stockpiling exploits. Vladimir Putin, the prime minister of Russia at the time, commented that tools such as

this “one can later do damage to their authors and creators” (Geller, 2017). Scholars have also chimed in by analyzing the consequences of EternalBlue. However they do not evaluate the morality of a defense organization like the NSA in building and storing exploits in the first place. By not doing so, they overlook the opportunity to engage in a thorough discussion about the NSA’s culpability in this global incident.

The journal article by Stephen Wicker “The Ethics of Zero-Day Exploits— The NSA Meets the Trolley Car” (2020) weighs the outcomes of stockpiling vulnerabilities through the lens of consequentialism and non-consequentialism. Evaluating this case through the lens of consequentialism does not yield clear results as the author finds that the advantages and disadvantages balance each other as stockpiling can be a threat to both domestic and foreign systems. The author then analyzes this case through non-consequentialism where he finds that if one can “mitigate the risk to the general public, stockpiling becomes permissible.” While the author discusses some of the ethical nuances, by suggesting educating the public, the author fails to understand the scope of the issue and shifts the blame off of the NSA. Since computers running the flawed Microsoft software were present around the world, educating enough people quickly on cybersecurity principles would be extremely challenging. The time frame between the security patch and the hacks was only 2 months, and if Microsoft was not able to patch it quickly then the outcome could have been far more devastating.

Another article “A new role for ‘the public’? Exploring cyber security controversies in the case of WannaCry” (Christensen & Liebetrau, 2019) discusses the role of the public in the WannaCry crises. This article summarizes how incidents like this can be mitigated by not only software vendors like Microsoft and government entities like the NSA, but also by the users of technology. Their conclusion essentially states that active public participation by

both software vendors and consumers of technology is necessary in both the technological and political worlds. The little discussion the authors have on the ethical dilemma posed to the NSA ended with the statement "it can be argued that most of its potential constituents failed to qualify as participants in the affairs" (Christensen & Liebetrau, 2019, p. 402). Similar to the previous article, by placing focus on another precautionary measure, this article neglects to analyze whether the NSA itself was an ethical actor and if their actions were primarily responsible for this event.

While both articles suggest that cybersecurity issues cannot simply be solved by evaluating the actions of one rogue actor, they fail to recognize the role of the NSA as a defensive arm of the country in cyber warfare. The organization's motto is "Defending our Nation, Securing our Future," which should mean that the NSA should be engaging in practices to ensure that citizens' systems are secure from foreign threats as well (National Security Agency Central Security Service, n.d.). The following discussion will show how the NSA failure to be a virtuous actor barred them from fulfilling this goal.

Conceptual Framework

Evaluating morality of an organization can be extremely difficult, which is why in order to provide a specific, thorough analysis, one can use an ethical framework such as virtue ethics. The ethical theory was formed by Aristotle, a Greek philosopher, whose belief was that the purpose of human life was to strive for the greatest good, known as "eudaimonia." In order to do so, a person must develop and live by moral virtues which are characteristics that balance out two extreme behaviors. For example, the virtue of courage is noted as the balance between cowardice and recklessness (van de Poel & Royakkers, 2011).

When looking at a case study, the actor and virtues must be specifically defined if a reasoned determination is to be made on whether the actor is a virtuous agent. In the case of the EternalBlue exploit, one issue that arises is that no individual engineer can be held responsible. This is because a decision to keep secrets enclosed requires the approval and oversight from the many engineers and figures of authority that exist within the organization. As such, discussion shifts to analyzing whether the collective of individuals can "be held morally responsible for the outcome" (van de Poel & Royakkers, 2011, p. 253). It follows that this must be a matter of collective responsibility, where the actions of the NSA as a whole will be used to determine its morality. As van de Poel & Royakkers note, judging a responsible action requires a more specific set of virtues to evaluate the action by. In this case, the actor responsible for developing and storing the EternalBlue exploit is a group of engineers at the NSA. The appropriate set of virtues for engineers can be found in Michael Pritchard's "Virtues for Morally Responsible Engineers" (Pritchard, 2001, p.394-395), which are seen in Figure 1 below.

1. competence
2. ability to communicate clearly and informatively
3. cooperativeness (being a good "team player")
4. willingness to compromise
5. perseverance
6. habit of documenting work thoroughly and clearly
7. commitment to objectivity
8. openness to correction (admitting mistakes, acknowledging oversight)
9. commitment to quality
10. being imaginative
11. seeing the "big picture" as well as the details of smaller domains

Figure 1: Prichard's 'Virtues for Morally Responsible Engineers'

It is important to note that Pritchard states that lacking any one of these virtues is evidence enough to deem that an engineer is not practicing the profession responsibly. It follows that if a group of engineers, such as the ones at the NSA, is found to lack any of those virtues, then the actor may be deemed immoral based on the principles of virtue ethics.

The ensuing analysis will also draw on three rules from "Moral Responsibility for Computing Artifacts: "The Rules"" (2011), shown in Figure 2 below, which list five rules that determine how software developers can be held morally responsible.

Rule 1: The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is shared with other people who design, develop, deploy or knowingly use the artifact as part of a sociotechnical system.
Rule 2: The shared responsibility of computing artifacts is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying or using the artifact. Instead, a person's responsibility includes being answerable for the behaviors of the artifact and for the artifact's effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.
Rule 4: People who knowingly design, develop, deploy, or use a computing artifact can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded.

Figure 2: Rules 1,2, 4 of the "Moral Responsibility for Computing Artifacts: "The Rules""

These rules help illustrate what software developers must account for when developing these technological artifacts, and will help further the discussion on the three aforementioned virtues. Competence aligns with Rule 1, as engineers must be able to reason through ways how their product affects users. Cooperativeness aligns with Rule 2 as it means being answerable for the behaviors which requires engineers to work with other entities that can possibly be impacted by the computing artifact. Lastly, Rule 4 aligns with the virtue of seeing the "big picture" as it indicates how engineers must consider the larger sociotechnical implications of their creation.

By developing the discussion of virtue ethics with the rules mentioned earlier, one can more thoroughly judge an actor's morality in a given situation. Accordingly, the following investigation will determine whether the NSA met the ethical standards for responsible engineers. Specifically, the three virtues that will be questioned are standards for competence, cooperativeness, and seeing the "big picture."

Analysis

In this discussion, I will show how the NSA did not embody three virtues in its handling of the EternalBlue exploit: competence, cooperativeness, and seeing the "big picture." As noted earlier, the absence of even one of the professional virtues indicates an irresponsible engineer, which by the definition of virtue ethics means the acting agent is not virtuous and therefore immoral. The following sections will detail the three virtues and the decisions made by the NSA that show a lack of the virtues which form a morally sound engineering organization.

Competence

Competence is a virtue that was absent in the NSA's handling of the exploit. It is defined as "the quality or state of having sufficient knowledge, judgment, skill, or strength (as for a particular duty or in a particular respect)" ("Definition of Competence," n.d.). In order to determine if the NSA was competent, two core aspects of the agency must be analyzed with respect to this case: the duty of the NSA, and the ability of the NSA to carry out that purpose.

As indicated earlier by the NSA's motto, one of the functions of the organization is to defend the country. In simplest terms, if there is a security threat, it is the NSA's duty to take the necessary steps in order to protect American citizens from harm. At the time, 73% of the computers in the U.S. were running Windows software ("Desktop Operating System Market Share," n.d.). While it is unknown how many of them were vulnerable in May 2017, the time of the WannaCry attack, the sheer percentage of market share indicated that it was possible many systems in the U.S were running the vulnerable version of Windows. Even engineers at the NSA who were "entrusted with deploying it marveled at both its uncommon power and the widespread havoc it could wreak if it ever got loose" (Nakashima & Timberg, 2017). So, it follows that the

NSA knew of a vulnerability that could potentially impact millions of Americans yet decided to keep it disclosed for five years. This meant the NSA knowingly left a large portion of systems in the U.S. vulnerable for nearly half a decade, thus violating their mission to "Defend our Nation." This decision of inaction reflects that the NSA was reckless and therefore was not operating in a skillful manner that would belong to a responsible engineer.

Since the NSA is primarily an intelligence agency, it is also responsible for closely guarding national secrets, such as the Eternal Blue exploit, that could be disastrous for the nation if fallen into the wrong hands. It is evident that the NSA failed to do this as this exploit, amongst other highly sensitive data, were leaked to anonymous hackers in early 2017. While the exact cause of this leak is still undisclosed, the two prominent theories are that either a rogue actor stole the files from within the agency, or the files were not properly secured allowing them to be accessed remotely (Geller, 2017). In either case, it represents a failure by the NSA to properly implement and follow guidelines that would guarantee the security of dangerous tools such as EternalBlue.

As explained above, the lack of disclosure and subsequent breach demonstrated the NSA's failure to carry out its role in safeguarding its secrets and nation's citizens. A possible counter argument that could arise is that it can be impossible to totally secure information such as this exploit, and the NSA could not have predicted this possibility. Cybersecurity is a complex field, and it can be difficult to prevent every malicious actor. However, one must consider two key factors in this case. One is that the NSA is not immune to cyberattacks. This is noted by an advisory released by the U.S. Department of Defense (2020) which also underlines the need for more secure practices at defense agencies such as the NSA due to the fact that cyberattacks are attempted very frequently. In stockpiling this secret, the NSA willingly took on this risk to

themselves and consequently their citizens. Then, one must also note Rule 1 of the "Moral Responsibility for Computing Artifacts: "The Rules"" (2011) which indicates that the people who design the computing artifact must be able to judge the effects of the artifact. As such, a responsible engineer should recognize the dangerous risk of a weakness present in many computers around the world. The NSA demonstrated that they severely undervalued the impact of this exploit by keeping this information secret for five years, which is a significant amount of time for an organization that is a valuable target for many actors seeking U.S secrets and practices.

By failing to properly ensure that both citizens and the agency's sensitive data are secure, not only did the NSA not meet its central aims as a security agency, they also did not accurately judge the possible consequences of their software exploit. Thus, the organization did not fulfill the virtue of competence as it could not meet the standards of its professional goals.

Cooperativeness

Another virtue the NSA did not exemplify in this case is cooperativeness. Using the concept of each moral virtue being a moral equilibrium, cooperativeness can be seen as a balance of being independent and relying on others for one's work. The NSA as an organization centered around security must be in the middle of the two extremes. It needs to be independent so that it cannot be easily penetrated and it can function apart from malicious influences. However, considering the agency's purpose is not to drive technological innovation, it also needs to cooperate with companies and groups that influence the majority of the world's technological systems.

It is understandable that when the agency first discovered a security flaw in Windows systems, it saw an opportunity to use it to infiltrate other nations, which serves its purpose to maintain an advantage to the foreign intelligence communities. However, it failed to recognize the role of Microsoft as a company whose computers not only dominated the US market, but also composed 80% of the world's market share at the time ("Desktop Operating System Market Share," n.d.). By cooperating with Microsoft, they could have found out how large the scope could be if this vulnerability was released to the public.

A vulnerability's severity is judged by properly documenting and submitting it to the Common Vulnerability Scoring System (CVSS) which then assigns it a CVSS Score. The CVSS system is a global standard that assigns a ranking to a vulnerability from 0 to 10 based on exploit complexity, how quickly it can be exploited, and the impact the vulnerability will have on the environment if exploited. So the more dangerous a vulnerability is, the higher the score will be (Mell, P., & Romanosky, 2013). According to the National Vulnerability Database (2017), the exploit was given a 9.3 rating according to CVSS v2, the current version at the time, meaning it was a significantly dangerous vulnerability. It is important to note that the rating could only be calculated in March 2017 when Microsoft was notified and could submit it. However, this does not absolve the engineers at the NSA as responsible engineers should have been able to assess the severity of a grave issue themselves. Being able to gain remote access to any system running vulnerable Microsoft software is a very powerful cyber weapon that if obtained by malicious actors, could be used to harm many innocent people.

According to Rule 2 in "Moral Responsibility for Computing Artifacts: "The Rules"" (2011) shown in Figure 2, developers must be able to reasonably judge if their product can be misused and take responsibility for the foreseeable effects. A responsible engineer would have

identified the severity of this vulnerability and cooperated with the appropriate procedures. In this case, not only did the NSA fail to cooperate with Microsoft, they also failed to properly document and file the vulnerability quickly enough. If they had done so, they could have initiated procedures much more quickly that would have prevented this global incident. They only cooperated until after the breach happened, but this was a cooperation out of necessity rather than as precautionary measure. On the other hand, a socially responsible engineer would have recognized the severity of the vulnerability and have cooperated appropriately in time. Therefore this means they did not satisfy another virtue, cooperativeness.

Seeing the "big picture"

Lastly, the NSA did not embody the virtue of seeing the "big picture," which means asking that as the acting agent, they did not sufficiently consider the implications of their decisions. It is clear that the NSA saw immense benefits with EternalBlue; the exploit allowed them to hack and execute code on any Windows system with the specific weakness. Considering it was the NSA developed exploit, EternalBlue was a weapon that they maintained was exclusively at their disposal.

On the other hand, according to the Rule 4 in "Moral Responsibility for Computing Artifacts: "The Rules"" (2011) shown in Figure 2, in developing this exploit the NSA also had to consider the systems in the world it could impact. This meant the NSA needed to consider that if the vulnerability was found by another foreign agent, the consequences could be truly disastrous. Given that the NSA held on to this tool for five years, it was not unlikely a malicious actor could have found it. Any socially responsible engineer should have to be able to recognize that a "hard to detect and easy to use" (Shane, 2017) tool such as this one could cause not only monetary

damage, but also have consequences to physical lives. As the Internet-of-Things, the network of devices with access to the internet in the world, grows at an exponential rate, the use of computer systems increases beyond simple software to being a part of everyday systems such as healthcare. This became apparent for this incident when the United Kingdom suffered £92 million worth of damages due to the WannaCry ransomware, and their nation's healthcare system, the NHS's service was interrupted for several days (Acronis, n.d.). Though no lives were reported to have been lost due to this outage, it shows that a responsible engineer would have recognized that this tool could affect entire healthcare systems as an increasing amount of hospital devices are connected to the internet.

To expand on the previous point, the United Kingdom is one of many of U.S.'s political allies in modern times. Being responsible for the development of a powerful technological tool that can access any vulnerable systems remotely does not reflect well on the political relations the country has with the rest of the world. By stockpiling EternalBlue, engineers at the NSA inherently put themselves at risk of being exposed and consequently creating international tensions.

If the NSA truly understood the full scope of this technology, it could have been concluded that the exploit was too dangerous a tool to stockpile. A responsible engineer would see that the global implications of allowing a vulnerability in computers around the world would be far too severe in order outweigh any benefits it posed as a cyberweapon for the United States. By letting this vulnerability go unreported for five years, the NSA showed how they disregarded the "big picture," therefore did not act in line with the aforementioned virtue.

Conclusion

By analyzing this case through the virtue ethics framework, it is possible to see that the NSA was immoral in how it handled the EternalBlue exploit. The evidence suggests that the organization failed to meet the three of the virtues of professional engineers: competence, cooperativeness, and seeing the "big picture." Failing to disclose the exploit in a timely manner showed how the NSA did not appropriately judge the gravity of the tool, nor did they adhere to cybersecurity principles. Moreover, the NSA was not able to keep such a dangerous tool secure which confirmed the organization did not fulfill its duty as a national defense organization.

This analysis of the EternalBlue exploit can help an engineer understand that careful considerations are necessary when dealing with cybersecurity software that has the potential for widespread and severe impacts. Further research may be done in order to determine strict guidelines for stockpiling vulnerabilities. Doing so will help inform institutions and engineers' understanding of a virtuous agent in the world of cybersecurity.

Word Count: 3706

References

Acronis. (n.d.). *The NHS cyber attack: how and why it happened, and who did it*. Retrieved March 16, 2021, from https://www.acronis.com/en-us/articles/nhs-cyber-attack/

Burdova, C. (2020, December 8). *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* Avast. Retrieved from https://www.avast.com/c-eternalblue

Christensen, K. K., & Liebetrau, T. (2019). A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry. *Intelligence and National Security, 34*(3), 395–408. https://doi.org/10.1080/02684527.2019.1553704

Definition of Competence. (n.d.). Retrieved March 16, 2021, from https://www.merriamwebster.com/dictionary/competence

Geller, E. (2017, May 15). *Why people are blaming the global cyberattack on the NSA*. POLITICO. Retrieved from https://www.politico.com/story/2017/05/15/global-cyberattack-nsa-238412

Mago, M., & Madyira, F. F. (2018). Ransomware software: Case of wannacry. *International Research Journal of Advanced Engineering and Science (IRJAES)*, *3*(1), 258-261.

Mell, P., & Romanosky, S. (2013). *CVSS v2 Complete Documentation*. Forum of Incident Response and Security Teams. https://www.first.org/cvss/v2/guide

Miller, K. W. (2011). Moral Responsibility for Computing Artifacts: "The Rules." *IT Professional, 13*(3), 57–59. https://doi.org/10.1109/mitp.2011.46

Nakashima, E., & Timberg, C. (2017, May 16). NSA officials worried about the day its potent hacking tool would get loose. Then it did. *The Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-da

y-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

National Security Agency Central Security Service. (n.d.). *What We Do*. Retrieved March 16, 2021, from https://www.nsa.gov/what-we-do/

National Vulnerability Database. (2017, March 16). *NVD - CVE-2017-0144*. National Institute of Standards and Technology. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2017-0144

Pritchard, M. (2001). Responsible engineering: The importance of character and imagination. *Science and Engineering Ethics*, 7(3), 391–402

Shane, S. (2017, May 16). *Malware Case Is Major Blow for the N.S.A*. *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/16/us/nsa-malware-case-shadow-brokers.html

StatCounter. (n.d.). *Desktop Operating System Market Share United States Of America*. StatCounter Global Stats. Retrieved March 16, 2021, from https://gs.statcounter.com/os-market-share/desktop/united-states-of-america/#quarterly-201701-201703

U.S. Department of Defense (2020, July 23). *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems: Cybersecurity Advisory*. Retrieved from https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/1/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF

van de Poel, I., & Royakkers, L. (2011). *Ethics, technology, and engineering: An introduction*. Hoboken, NJ: Blackwell Publishing Ltd

Wicker, S. B. (2020). The ethics of zero-day exploits - The NSA Meets the Trolley Car. *Communications of the ACM, 64*(1), 97–103. https://doi.org/10.1145/3393670