

Cyber Exploits: A Cyber Wild West for National Security Law

Victoria Walter

POSC 390: National Security Law

April 30, 2019

Cyber Exploits: A Cyber Wild West for National Security Law

“Heartbleed bug puts the chaotic nature of the Internet under the magnifying glass,” read the headline of the Technology section of the Washington Post just over 5 years ago, on April 9th 2014 (Timberg, 2014). It continues, “While the extent of the damage caused by the bug may never be known, the possibilities for data theft are enormous.” When Social Security numbers, credit card numbers, passwords, Internet-linked surveillance camera videos, healthcare information, and a plethora of other data from private companies—as high profile as Yahoo, eBay, and Amazon—and government agencies, some of which has not been accessed in years, is stolen, it is clear that there is a problem. The United States branches of government should know this as well, but at the time, only a small pocket of individuals knew. The NSA knew about the Heartbleed bug—and the damage it was causing to United States consumers and businesses—for two years, until a Google programmer discovered the vulnerability in an open source code that almost every user on the Internet uses. Outrage sparked immediately: How could the NSA hide this for so long and knowingly allow American consumers and businesses to be extremely vulnerable to hacks? Because there is no policy directly regulating whether the NSA and other US Intelligence agencies share their knowledge of 0day vulnerabilities and exploits or take advantage of those vulnerabilities as an offensive tool to other foreign states.

In this analysis I will discuss how the current guidelines, the Vulnerabilities Equities Process, for the United States Government are deeply flawed and insufficient in regulating the NSA’s treatment of exploits. Several ethical and legal issues arise because of this. Ethically concerning is that the NSA leaves the privacy of American citizens, companies, and organizations vulnerable for long periods of time to zero-day attacks by not disclosing

vulnerabilities and exploits they discover. Most importantly, controversial legal concerns have arose in the last decade for the use of exploits for federal law enforcement purposes. The amendment made to Rule 41 of the Federal Criminal Procedure now opens up risks of tense cross-border cyberoperations in foreign states because the FBI can now obtain information from any device anywhere in the world if a district magistrate court judge permits a warrant. The increased scope of intelligence collection could result in international tensions and even retribution, because this type of infringement on foreign sovereignty can be perceived as “a use of force” under international norms. Finally, I argue my support for PATCH, a bill in consideration in Congress that would normalize and formalize the VEP, as well as add additional requirements to foster greater transparency between the NSA and U.S. consumers and businesses when it comes to vulnerabilities and exploits.

So, what are zero-day vulnerabilities and exploits? Norton, a trusted software leader in the cyber security and anti-virus space, defines a 0day vulnerability as, “a software security flaw that is known to the software vendor but doesn’t have a patch in place to fix the flaw... that left unaddressed... can create security holes that cybercriminals can exploit” (Norton). These vulnerabilities can occur in any code or operating system and can occur in private businesses big and small, government agencies, and private individuals’ computers worldwide. Every day, constantly, hackers target major information systems in order to collect as much data as possible, whether it is for political means or to steal money from people through using their credit cards and social security numbers. Because the software space is so meritocratic, hackers are sometimes able to discover these vulnerabilities before software vendors, even as sharp and large as Amazon, Google, and Yahoo, realize they exist and then hackers exploit them. Norton

describes the process of these exploits: “Hackers write code to target a specific security weakness. They package it into malware called a zero-day exploit. The malicious software takes advantage of a vulnerability to compromise a computer system or cause an unintended behavior” which is almost always to steal some kind of data (Norton). Other times, software vendors discover the vulnerability and then have to act quickly to patch it. Norton explains,

The term ‘zero-day’ refers to a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn’t been released. So, ‘zero-day’ refers to the fact that the developers have ‘zero days’ to fix the problem that has just been exposed — and perhaps already exploited by hackers. Once the vulnerability becomes publicly known, the vendor has to work quickly to fix the issue to protect its users. But the software vendor may fail to release a patch before hackers manage to exploit the security hole. That’s known as a zero-day attack.

A short analogy can be used understand these terms and how they work together in the cybersecurity space. A zero-day vulnerability is like a crack in the wall of a house from the outside. A zero-day exploit is when you hit the crack hard enough and create a hole, but then hide the hole. A zero-day attack is when a robber reaches into the hole and steals possessions from the house. These vulnerabilities, exploits, and attacks can cause extremely serious—and sometimes even unknown—damage. Additionally, there are other types of exploits that are intentional, and therefore not zero-day, such as network investigative techniques.

What does a vulnerability, exploit, and attack look like in action? Taking a closer look at Heartbleed is a perfect case study to illustrate the technology, the damage, and the inaction from government. Discovered in November of 2014, the Heartbleed bug developed as a vulnerability

in OpenSSL, a major cryptographic software library (US-CISA, 2014). It is used to encrypt almost all of the information from individuals, businesses, and governments online. When opening a browser and going to a website, the web address should begin with “https://” if that particular site is using encryption (DigiCert). When a site uses encryption, it means that as the information passes through several intermediary nodes before reaching the required server on which your desired website lies, the information cannot be viewed by those intermediaries. Heartbleed’s specific vulnerability lied in the accessibility to memory, and thus information on a server. Normally, hackers are only able to view a small amount of memory on a server. With Heartbleed, hackers were able to access more memory than previously and were able to access a cryptographic key that was usually protected. With the cryptographic key, hackers were then able to view all memory/information going in and out of a server (US-CISA, 2014).

To put this into perspective, every single website must have at least one server to function in order to store the copious amounts of data that build up. Websites that experience significant traffic on a regular basis, such as Amazon, Netflix, Facebook, but even lesser known sites such as popular blogs, gaming websites, etc, have multiple servers to accommodate the large amounts of data and memory that accumulate (Sullivan, 2018). This data that builds up includes everything from usernames, passwords, emails, phone numbers, credit card numbers, social security numbers, and depending on the website can even include photos, private messages, and search histories. For example, if someone was applying for financial aid for college from the FAFSA before Heartbleed was discovered, and therefore had to enter copious amounts of private information such as tax returns, social security numbers, etc, all of that information was vulnerable on one of FAFSA’s servers. On social media websites—Facebook, for

example—private messages, posts, photos, videos, and any other type of media was vulnerable. There have been proof of concept demonstrations showing the hack (Westpoint, 2018). A cartoon strip explaining the exploit is in the appendix (xkcd).

Heartbleed and other zero-day attacks have obscene and still not fully known consequences financially and on confidential and sensitive user data. Because of how large a scale the vulnerability existed on the Internet, the Heartbleed attack was able to infiltrate the entire Internet worldwide, and hit popular websites such as Amazon, Yahoo, and Tumblr especially hard. Any app, website or service on those servers are vulnerable. According to Fortune, “Heartbleed has been blamed for the breach of 4.5 million patient records at the hospital group Community Health Systems by the alleged Chinese hacker group” (BBC, 2014). Though a patch to fix the vulnerability was developed within 48 hours once it became public knowledge, the damage is still ongoing. Even after a year, according to a security scan by a trusted cyber security firm Venafi, 74% of organizations of the public-facing systems of Global 2000 companies were vulnerable to Heartbleed (1,642 companies) even after a year of the exploit and patch being released (Fortune, 2015). To this day, about 5% of all servers and machines worldwide are still affected by the 0day attack called Heartbleed, and most of these servers and machines will never be patched.

It is clear why zero-day exploits are a national security issue—but why are they a national security *law* issue? Zero-day vulnerabilities and exploits are valuable for hackers trying to obtain confidential information, steal large sums of money, or make political statements, but they are also useful for governments. Governments have their own hackers that are constantly searching the Internet for vulnerabilities with the goal of exploiting those vulnerabilities on

against adversaries. For example, the NSA in the United States searches for these vulnerabilities and upon discovering them, uses them to collect as much sensitive data as possible from adversaries such as China and Russia. From the perspective of foreign intelligence collection, zero-day exploits provide a gold mine of information at a much cheaper cost (both in dollars and in human lives) than traditional information collection in the past. The use of zero-day exploits as an offensive cyber tactic is an excellent national security strategy but has its own set of consequences.

Important legal and ethical issues arise when the government uses these exploits offensively. In this section of the analysis, I focus briefly on the ethical issues. Later in the analysis, there will be an in-depth consideration of the legal issues. Important strategic national security objectives can be met when the NSA stockpiles and uses these exploits offensively on U.S. foreign adversaries. But in these instances, the federal government cannot release this information to American citizens so that they can protect themselves. For example, in the Heartbleed exploit, the NSA knew for two years that the vulnerability existed—and *had a patch for it*—and knew the extent of the damage it was causing. For two years, American citizens input their credit card numbers, social security numbers, health data, pictures, geolocations, private messages, and other very sensitive data into a computer system that suffered from a drastic security vulnerability. Meanwhile the United States government knew about the vulnerability, did not disclose it to the American public, had the patch to fix the vulnerability, and disclosed that to no one either, all because they thought it was more important to strategic national security goals to keep those vulnerabilities a secret and exploit them against other foreign powers. Additionally, the NSA knew that other hackers around the globe had discovered the vulnerability

and that they were exploiting American citizens' sensitive data, and even then the federal government did not disclose the vulnerability or inform U.S. citizens to protect themselves. There are ethical concerns for this type of national security cyber operations that have real implications on American citizens. For example, if the public was informed when the NSA initially discovered it, OpenSSL, the software system that contained the vulnerability in Heartbleed, could have taken steps to patch the vulnerability quickly and prevent two years of American citizens' sensitive data—and money—from being hacked and stolen.

When Heartbleed occurred, there was a policy in place to guide—not regulate—how the NSA collected, used, and disclosed zero-day exploits. Even today, over five years after Heartbleed, there is still no policy directly regulating the use and disclosure of zero-day vulnerabilities and exploits. According to the Electronic Privacy Information Center (Electronic Privacy Information Center), in 2008 and 2009 several working groups in the executive branch were tasked with creating “a Joint Plan for improving the government’s ability to use offensive capabilities against U.S. adversaries and to protect both government and public information systems.” What was formed is the Vulnerabilities Equities Process (VEP). The White House website describes the VEP in more detail:

[The VEP] balances whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the U.S. government, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence.

In the appendix of the White House de-classified document on the VEP, they outline several questions that the NSA is suggested to consider (US Govt. 2017). There are four parts: “Defensive Equity Considerations”; “Intelligence, Law Enforcement, and Operational Equity Considerations”; “Commercial Equity Considerations”; and “International Partnership Equity Considerations.” The first two parts—those concerned with whether knowledge of an exploit should be used defensively or offensively—are broken down into several categories. For example, “Defensive Equity Considerations” is separated into threat, vulnerability, impact, and mitigation considerations.

But with these questions, there is no information provided as to what kinds of answers would sway a decision of whether to disclose. One would assume that if the threat is high and that there would be a large impact on the American people, the NSA would choose to disclose. But these exploits are very complicated and highly classified, so assumptions are not enough when it comes to the vulnerability of highly sensitive data. Legal scholars also note how quickly answers to these questions can become highly subjective (Aitel and Tait, 2016). For example, “How dangerous is too dangerous?” or “How great does a risk that a given adversary finds a vulnerability need to be before the balance tips to disclosure?” (Aitel and Tait, 2016).

Upon reading the White House’s official, declassified document on the VEP, the NSA is mostly vague, but there are a few areas that can rise immediate attention. In the section labeled “Determination to Disseminate or Restrict” the exploit (US Govt. 2017), the NSA says:

Decisions whether to disclose or restrict a vulnerability will be made quickly, in full consultation with all concerned agencies, and in the overall best interest of USG [U.S.

government] missions of cybersecurity, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection.

Nowhere in the entire document is there mention of ethical concerns about disclosure for the American people, legal concerns, or privacy concerns. As a policy analyst, I am very concerned that in the above paragraph and other two paragraphs of the section there is not even a single mention of the best interest for American citizens. Regardless of this, legal scholars note that the VEP boils down to answering two specific questions: (1) Will the vulnerability be used? (2) is the vulnerability too dangerous? (Aitel and Tait, 2016).

While the VEP is a step in the right direction of legislating and making policy regarding the use and disclosure of these exploits, it has several issues, some of which I began describing above. Other issues include (1) that the VEP does not provide a frame of time between discovery and disclosure, (2) that the VEP was created without the consultation of technology experts in the private sector, and (3) that the scoring and responses to the questions posed by the VEP (for determination) are subjective and inconsistent. Dave Aitel and Matt Tait of Lawfare say that the VEP is “broken” and that “the US has confused a public relations strategy with a security strategy to the detriment of a nation” (Aitel and Tait, 2016).

One of the biggest points of concern in relation to the VEP is that it does not express *when* the exploit can be disclosed and therefore patched, nor the amount of time between discovery and disclosure. In November of 2015, the NSA released a statement saying, “Historically, NSA has released more than 91 percent of vulnerabilities discovered in products that have gone through our internal review process and that are made or used in the U.S,” (Reuters). A former White House official said that although the NSA discloses 91% of the

exploits they find, they do not note the amount of time between discovering a vulnerability, turning into an exploit, and disclosing it to vendors or the American people. He specifically says that it would be “a reasonable assumption” to conclude that most of those 91% disclosed were only disclosed after the NSA had used the exploits offensively to gather intelligence (Menn, 2015).

The Vulnerabilities Equities Process was also designed without consulting with relevant stakeholders: technology companies, consumers, etc (Romanosky, 2019). Therefore, the process was designed with only one perspective in mind-- that of executive branch policymakers and not experts in the field from the private sector. Because of this, the VEP does not take into consideration several other factors, including the business and social impact to consumers, businesses and national infrastructure and the probabilities that the vendor would produce a patch and that users would apply (Romanosky, 2019).

Another flaw in the Vulnerabilities Equities Process is that the responses to the questions used for determination in the guidelines are not standardized (Romanosky, 2019). The answers to the questions receive no quantitative or standardized value according to the VEP guidelines released by the White House (Romanosky, 2019). Not only does this breed heavy subjectivity in the determination process, but also glaring inconsistencies in how different exploits are treated. Exploits, especially those that are specifically zero-day, are very different and extremely complicated so consistency is key in their evaluation.

It is worthwhile in this analysis to consider the NSA’s argument for not disclosing exploits and stockpiling them for offensive use. There are many things that the NSA can do by using exploits offensively, including foreign information collection, law enforcement purposes,

and cyberattacks (Crocker, 2015). Hacking and the offensive use of exploits broadens the scope of the magnitude of information the NSA can collect throughout the entire Internet. One of the earliest and most known offensive uses of an exploit is Stuxnet. The NSA was able to alter the code and eventually destroy the centrifuges in Iran's nuclear facilities program because they discovered a vulnerability in Microsoft's and Siemens AG's software that was used for Iran's cybersecurity. After discovering the vulnerability, the NSA figured out how to fully penetrate their cybersecurity, and thus alter the code used in the nuclear facility. The exploit was also used in a way so that the control panel was unable to show changes in how fast the centrifuges were spinning. If the control panel had showed how fast the centrifuges were spinning, the scientists at Iran's nuclear facility would have just shut it down. But because the exploit was used in that specific way, the scientists had no idea that the centrifuges were spinning that fast and eventually led to their destruction. Though some today debate the ethics of Stuxnet, it was nonetheless a breakthrough in the exploit space as well as a breakthrough in the American national security and foreign policy space. Prior to Stuxnet's development, the only other options to stop Iran's nuclear program at the time would have been very costly, both in terms of dollars and in human lives.

Cost reduction is another major reason why the NSA argues for stockpiling and opposing disclosing these exploits. "For foreign intelligence, hacking is both safer and more effective than previous forms of intelligence," experts note (Aitel and Tait, 2016). Instead of having to physically be present in a dangerous country and risk lives to wiretap or intercept local messages between targets, American intelligence officials can sit behind a supercomputer in a safe environment in the U.S. The NSA and other federal intelligence agencies are not going to stop

collecting foreign intelligence anytime soon, so reducing the number of exploits that can be used offensively will encourage less safe forms of collection and possibly endanger human lives. Even if intelligence collecting does not occur in person and endanger human lives, collection will occur but in undifferentiated forms—such as bulk collections—“which are more threatening to the privacy of innocent citizens on a larger scale ” (Romanosky, 2019). However, the NSA’s justifications opposing disclosure do not produce benefits greater than the harm that nondisclosure causes to the privacy rights of Americans and technology users worldwide and the ensuing consequences of violating those rights.

There are several aspects of how the NSA treats exploits that are both legally and ethically concerning. The vague, relaxed guidelines and lack of transparency have large impacts on privacy rights of Americans and people around the world. The lack of disclosure of exploits on the part of the NSA is unacceptable, but other parts of the executive branch in the United States are using exploits in a different and much more legally controversial way.

This analysis focuses on the legal implications of the use of exploits for federal law enforcement investigations because it is particularly concerning from a national security law perspective. It is important to note that the use of cyber exploits for federal law enforcement criminal investigations is technically legal, but only because no cases have been settled by the Supreme Court to pass judgement on the issue. The Congressional Research Service describes this use, “Law enforcement has explored various avenues to discover and exploit vulnerabilities in technology so it may attempt to uncover information relevant to a case that might be otherwise inaccessible.” In the 1990s, the U.S. Naval Research Lab developed “TOR,” a means to protect government communication. TOR works by using:

A group of volunteer-operated servers to create a network of “virtual tunnels,” allowing users to connect to a website anonymously. Rather than making a direct connection between a computer and a website, TOR routes a connection through different “nodes” in the TOR network, thereby obscuring aspects of how and where its users are accessing the Internet.¹⁸ This allows users to circumvent software designed to censor content, to avoid tracking of their browsing behaviors, and to facilitate other forms of anonymous communication. (Widenhouse, 2017)

TOR eventually acquired independent sponsors and was no longer used only for government purposes, but rather anyone who wanted better privacy on the Internet for a legitimate reason could use it. Since TOR became more popular and provided the capability to conceal physical locations and anonymize a user’s online activity, it has become more difficult for law enforcement to locate bad actors and attribute malicious activity to specific persons. Because of the development of better privacy technology, law enforcement officials have started using exploits to hack into phones, computers, and other devices to gain the information they need for a case. Law enforcement also use zero-day exploits to hack into devices they do not or cannot have in person to view their information remotely. This is done in two ways. The first is that law enforcement can leverage previously known exploits, discovered by the NSA, that have not yet been patched. The second method is that law enforcement can develop their own tools, outside of the NSA, to take advantage of previously unknown vulnerabilities and manifest them into useful exploits. The use of zero-day exploits for law enforcement purposes has important legal implications both in the United States and around the world.

One of the most recent and high-profile cases of the NSA using zero-day exploits for law enforcement purposes is *Apple v. FBI* in December 2015. Following the December 2, 2015 shooting by Syed Rizwan Farook and Tashfeen Malik that killed 14 people in San Bernardino, law enforcement officials found an iPhone 5C belonging to Farook. Like most iPhones, the phone was locked with a passcode that the government did not possess. On February 16, 2016, Magistrate Judge Sheri Pym of the Federal District Court of the Central District of California issued an order mandating Apple to help the government unlock the iPhone for the purpose of helping the investigation. They wanted Apple to “create software that would help it override a security system on the phone designed to erase its contents after 10 unsuccessful tries to enter its password” (NYT). Additionally, the government wanted Apple to create a backdoor, intentionally modifying their operating system to enable federal agencies to unlock any iPhone they wanted without having to know the password. Backdoors are intentional vulnerabilities left by vendors to gain special and unauthorized and unauthenticated access into systems, often with administrative privileges (SearchSecurity). Therefore, backdoors are intentional exploits left by the vendors. The problem with backdoors as history will support is that, they are often found by hackers. Vendors can make it hard for backdoors to be found but with enough research, hackers have found and used them time and again. The reasons for Apple not wanting to create the backdoor is:

1. The federal government is trying to force Apple to create software that does not exist
2. Creating that software would result in the hacking of its own technology

According to Apple, there were nine other cases of multiple government agencies in the DOJ that have them asked for help unlocking iPhones-- each time Apple refusing. Shortly after, Apple filed their own motion against the FBI. The main argument of the motion is that:

Compelling Apple to create software in this case will set a dangerous precedent for conspiring Apple and other technology companies to develop technology to do the government's bidding in untold future criminal investigations... Broadly, the order would inflict significant harm — to civil liberties, society and national security — and would pre-empt decisions that should be left to the will of the people through laws passed by Congress and signed by the president.

Apple justified their motion legally arguing that the government's motion oversteps the First and Fifth Amendments, as well as the All Writs Act of 1789. Their motion was overturned in part because the government claimed that compelling Apple to open this particular iPhone would not create an "undue burden" on them and therefore the All Writs Act of 1789. (nyt) A long legal battle ensued between the federal government and big technology companies, including Microsoft, Facebook, Twitter, and Google all submitting their own briefs to stop the government from compelling Apple to create software to unlock the iPhone.

The legal struggle on Apple's part was ultimately useless because on May 2017, the FBI announced that they were withdrawing the case as they had found an external group of hackers who helped them unlock the phone (Nakashimat, 2016). Because the NSA claimed they used an external group, they could not disclose the vulnerability in Apple's operating system.

Ahmed Ghappour, an author for the Stanford Law Review, says, "The use of hacking tools by law enforcement to pursue criminal suspects who have anonymized their

communications on the dark web presents a looming flashpoint between criminal procedure and international law.”

The nondisclosure and law enforcement use of exploits has had a profound effect on the Federal Rule of Criminal Procedure 41. Ghappour explains what it is:

The legal process for the use of network investigative techniques is governed by Federal Rule of Criminal Procedure 41, which articulates procedures for obtaining a search warrant in federal magistrate court. The former version of Rule 41(b) restricted authority to issue search warrants to the district of the magistrate making the decision. This had caused courts to deny search warrants for computers whose locations were unknown because they may have been outside the magistrate’s district.

An amendment (Rule 41(b)(6)) has been adopted that would give magistrate judges the authority in any district to issue a warrant to remotely access information on a device whether the device is located within or outside the district if “the district where the media or information is located has been concealed through technological means.” With the “largest expansion of extraterritorial enforcement jurisdiction in FBI history” of the current version, legal issues arise in that any given law enforcement target is likely to be located outside of the U.S.

For example, federal law enforcement in the Eastern District of Virginia received a tip and were able to find and take control of a child pornography site called “Playpen” in December 2014 (Zalkind Duncan & Bernstein LLP, 2017). The website was on the “Dark Web” and therefore used TOR to protect the privacy of the operator and users from sharing or learning one another’s IP addresses. Instead of shutting the website down immediately, FBI officials operated the website for two weeks, attempting to identify users of the website and those likely to download

child pornography. While this occurred, the U.S. Magistrate Judge for that district obtained a warrant use a network investigative technique (NIT), a type of exploit that the NSA already had in its arsenal. The goal of the NIT was to plant malware on any computer that visited the Playpen website and then use that malware to collect data from the infected computers. The warrant application incorrectly stated that the scope of the NIT would only be computers in Virginia, when really, the full scope was unknown because this site was available globally on the Dark Web (Zalkind Duncan & Bernstein LLP, 2017).

It took several weeks for the malware to be downloaded on every single computer, until thousands of computers around the world were infected. Then the FBI was able to gather the IP addresses directly from the infected computers and prosecuted hundreds of people for violating child pornography laws in the U.S.(Zalkind Duncan & Bernstein LLP, 2017). Even though viewing and downloading child pornography is objectively wrong and illegal in almost every country, the U.S. still technically violated the privacy rights of thousands of people worldwide. For the severity of this case, the use of exploits for law enforcement is well justified. But applying this same logic-- exploits and Rule 41(b)-- to much less severe types of criminal activity, some that are not illegal in every country, becomes a very slippery slope and can result in international tension.

Among all the concerns relating to the treatment and disclosure of exploits, why is this specific issue so important? The resulting effect of the amendment to Rule 41(b) violates one of the basic principles of international law—that one state may not unilaterally exercise its law enforcement functions in the territory of another state. According to Ghappour, this issue “has not been adequately addressed by courts or scholarship in the context of cyberspace.” Ghappour

notes that these kinds of cross-border cyberoperations can follow under the three categories of cyber conflict under international law: “an intentionally wrongful act,” “a use of force,” and “armed attack” (Ghappour 2017). There is relative consensus among the cybersecurity community that this use of exploits for law enforcement extending into foreign states does not reach the threshold of “an armed attack.” However, some scholars think that these types of cyberoperations would qualify as “uses of force” because they infringe on a state’s sovereignty. A cyberoperation considered as a “use of force” permits the attacked state to authorize retaliatory force and cyberoperations for self-defense that would otherwise be prohibited. Even if the use of exploits is interpreted as meeting a lower standard—“an intentionally wrongful act”—this could result not only in greater tension and complications in international affairs but also tangible problems that could affect average Americans. For example, a state could place economic sanctions on the U.S. in retribution or attempt to alter trade. If the exploit is considered a “use of force” by a foreign power, the effects would be much more drastic, including more aggressive and severe cyberattacks.

This analysis argues that, at the end of the day, exploits discovered by the NSA should be disclosed to vendors and consumers as soon as possible and maintain greater transparency about the determination process. Additionally, I conclude that the amendment made to Rule 41 was a mistake with unintended consequences that have the potential to open Pandora’s Box when it comes to cyberoperations globally and foreign affairs. Catching criminals and obtaining necessary information for criminal cases is still extremely important, but the risk of severe, unintended consequences to the United States and its citizens are not worth it.

Following the zero-day exploits of Heartbleed, Playpen, Apple v. FBI, and public and Congressional outrage, potential solutions to replace or at least improve the Vulnerabilities Equities Process began to form. For several months a bipartisan bill called the PATCH Act of 2017 was taking shape. Congress describes the goals of the bill:

“This bill establishes the Vulnerability Equities Review Board to establish and make available to the public policies on matters relating to whether, when, how, to whom, and to what degree information about a vulnerability in a technology, product, system, service, or application that is not publicly known should be shared or released by the government to a non-federal entity” (Ted, 2017).

PATCH would streamline the decision making process on determining which vulnerabilities should be released to the public and which need to be kept secret. The process takes into consideration the importance of the system with the vulnerability, the potential risks if left unaddressed, the potential harm that the U.S. could face if left unaddressed, how valuable the vulnerability is for intelligence agencies, and several other important considerations. The biggest difference that this analysis notes is that there is a greater emphasis on PATCH to search for other means of obtaining the same information without using a vulnerability. There is no mention of this type of consideration in the Vulnerabilities Equities Process.

The board can make recommendations to Department of Homeland Security to share or release exploits to vendors and DHS needs to act on the recommendation and share or release the information. “The board must submit to Congress and the President a draft of such policies, along with a description of challenges or impediments requiring legislative or administrative action” (Ted, 2017).

Additionally, the act formalizes the process of vulnerability disclosure and helps streamline the process. Agencies that discover the vulnerabilities have an interest in keeping them secret. A review board is much less biased and thus can weigh the benefits of secrecy and the need for transparency better. The board members can also be held accountable for their actions which brings accountability to the process.

There are numerous benefits to having a more formalized, standardized, and transparent process for the treatment of exploits (Herpig, 2019). These include oversight of government hacking and decreases in leaked government information.. Better oversight, even while maintaining most of these exploits as confidential until they are disclosed, helps the government, businesses, and consumers. It especially builds trust from technology companies and strengthens cooperation between the two entities. The federal government has been struggling in the last decade to get big tech companies such as Google and Apple to work with them because the companies are so skeptical. With better oversight of the use of exploits, this issue can slowly be eroded. With a stronger, more transparent process for the treatment of exploits, the government is likely to see a decrease in leaked government information. When the NSA discovers vulnerabilities and zero-day exploits in the government's own cybersecurity, they are very unlikely to patch it for fear of adversaries learning how the NSA discovers vulnerabilities. Because of this, it has allowed for an increase in leaked information from the government because of these vulnerabilities that got turned into zero-day exploits.

Exploits, especially zero-day exploits, are becoming an increasingly used tool by United States intelligence agencies and federal law enforcement officials. Exploits are developed from unknown vulnerabilities in the code of information systems or devices as hackers seek to use the

weakness to their advantage. These exploits turn into attacks when the hacker decides they want to use the exploit on a particular system. Zero-day exploits are especially dangerous because they are exploits that are discovered immediately, before there is a patch to fix the vulnerability. The damage that has been caused both financially and on the loss of personal and sensitive data of American citizens has been severe and still not fully known due to the scope of these exploits.

However, there is still a lot of mystery that still surrounds their treatment, use, and even their full scope and capabilities. Exploits can be treated defensively or offensively. Defensive treatment entails disclosing the vulnerability to the vendor or consumers so that it can be patched, or fixed. Offensive treatment entails not disclosing the vulnerability and turning it into an exploit to use on American foreign adversaries for cyberattacks or intelligence gathering. Additionally, offensive treatment can be used for gathering additional information for federal criminal investigations. The different treatments of exploits have serious ethical and legal implications, much of which are still being processed in courts and policy. Particularly ethically dubious is that the NSA will know that vulnerabilities and exploits exist and choose not to tell the American people that their sensitive data-- such as Social Security numbers, credit card numbers, health data, private conversations, and more-- are being stolen.

The conception of the Vulnerabilities Equities Process was an adequate first step in the process of creating a more transparent and formalized approach for the NSA to determine whether or not to disclose an exploit. Several topics and questions are considered, but in summary, the VEP asks two central questions: (1) Will the vulnerability be used? (2) Is the vulnerability too dangerous? The VEP is highly flawed, however. It is simply a set of guidelines that the NSA is not bound to follow and answers to the questions during the process of


determination are inconsistent and very subjective. Additionally, the VEP was created without the consultation of technology companies or experts and rather by policymakers in the executive branch.

Legal concerns about the treatment and use of exploits are particularly relevant when it comes to federal law enforcement use in criminal investigations. The passing of the amendment to Rule 41 of Federal Criminal Procedure now allows district magistrates to approve warrants for remote access view of information on computers, phones, and anything online. Therefore the scope of intelligence collection for federal law enforcement purposes is now the entire world as long as a warrant is obtained. This is technically legal, but only because no case has risen to the Supreme Court yet for judgement to be passed. This information collection on foreign devices constitutes as infringement on state sovereignty and can therefore be perceived as “a use of force” under international norms. A perceived of force under international norms permits the attacked state to use cyber measures for self-defense that are typically not permitted, and therefore are very damaging.


Something needs to be done to better regulate the treatment and use of cyber exploits, because intelligence agencies around the world are highly unlikely to stop using them any time soon. Possible solutions are in the works in Congress with bipartisan support, such as PATCH, but none have been passed. If this issue of regulating cyber exploits is not properly addressed in the coming years, American citizens will continue to face impediments to their privacy rights. Additionally, the U.S. could face international scrutiny for its invasion of privacy on citizens around the globe, potentially resulting in cyberattacks and other damage.

HOW THE HEARTBLEED BUG WORKS:


SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).




...pages about "boats". User Eric wants secure connection using key "4538538374224". User Meg wants these 6 letters: **POTATO**. User Ida wants pages about "irl games". Unlocking secure records with master key 513098573343. (content: 034b9c2e7c8b9ff90b1315f8)



...pages about "boats". User Eric wants secure connection using key "4538538374224". User Meg wants these 6 letters: **POTATO**. User Ida wants pages about "irl games". Unlocking secure records with master key 513098573343. (content: 034b9c2e7c8b9ff90b1315f8)



POTATO



SERVER, ARE YOU STILL THERE?
IF SO, REPLY "BIRD" (4 LETTERS).



...pages about "boats". User Eric wants secure connection using key "4538538374224". User Meg wants these 4 letters: **BIRD**. There are currently 340 connections open. User Brendan uploaded the file 034b9c2e7c8b9ff90b1315f8



HMM...




BIRD




...pages about "boats". User Eric wants secure connection using key "4538538374224". User Meg wants these 4 letters: **BIRD**. There are currently 340 connections open. User Brendan uploaded the file 034b9c2e7c8b9ff90b1315f8

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).



...pages about "boats". User Eric wants secure connection using key "4538538374224". User Meg wants these 500 letters: **HAT**. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoHoBaRt". User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoHoBaRt". User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoHoBaRt". User



...pages about "boats". User Eric wants secure connection using key "4538538374224". User Meg wants these 500 letters: **HAT**. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoHoBaRt". User

Bibliography

"Alert (TA14-098A)." OpenSSL 'Heartbleed' Vulnerability (CVE-2014-0160).

<https://www.us-cert.gov/ncas/alerts/TA14-098A>.

Center, Electronic Privacy Information. "EPIC - Vulnerabilities Equities Process." Electronic

Privacy Information Center. <https://epic.org/privacy/cybersecurity/vep/>.

"Community Health Systems Data Hack Hits 4.5 Million." BBC News. August 18, 2014.

<https://www.bbc.com/news/technology-28838661>.

Crocker, Andrew. "It's No Secret That the Government Uses Zero Days for 'Offense'."

Electronic Frontier Foundation. November 09, 2015.

<https://www.eff.org/deeplinks/2015/11/its-no-secret-government-uses-zero-days-offense>.

"Developing an Objective, Repeatable Scoring System for a Vulnerability Equities Process."

Lawfare. February 08, 2019.

<https://www.lawfareblog.com/developing-objective-repeatable-scoring-system-vulnerability-equities-process>.

"Everything You Know About the Vulnerability Equities Process Is Wrong." Lawfare. August 26, 2016.

<https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong>.

"Heartbleed Explanation." Xkcd. <https://xkcd.com/1354/>.

Finklea, Kristin. "Law Enforcement Using and Disclosing Technology Vulnerabilities"

<https://fas.org/sgp/crs/misc/R44827.pdf>

Ghappour, Ahmed. 2017. Searching Places Unknown: Law Enforcement Jurisdiction on the

Dark Web.

Hern, Alex. "Heartbleed: Hundreds of Thousands of Servers at Risk from Catastrophic Bug."

The Guardian. April 09, 2014.

<https://www.theguardian.com/technology/2014/apr/08/heartbleed-bug-puts-encryption-at-risk-for-hundreds-of-thousands-of-servers>.

Menn, Joseph. "NSA Says How Often, Not When, It Discloses Software Flaws." Reuters.

November 07, 2015.

<https://www.reuters.com/article/us-cybersecurity-nsa-flaws-insight/nsa-says-how-often-not-when-it-discloses-software-flaws-idUSKCN0SV2XQ20151107>.

Nakashima, Ellen. "FBI paid professional hackers one-time fee to crack San Bernardino iPhone".

https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.7947e0cca420. April 12, 2016

"On Heartbleed's Anniversary, 3 of 4 Big Companies Are Still Vulnerable." Fortune.

<http://fortune.com/2015/04/07/heartbleed-anniversary-vulnerable/>.

Sullivan, Nick. "Staying Ahead of OpenSSL Vulnerabilities." The Cloudflare Blog. August 27,

2018. <https://blog.cloudflare.com/staying-ahead-of-openssl-vulnerabilities/>.

Ted. "H.R.2481 - 115th Congress (2017-2018): PATCH Act of 2017." Congress.gov. May 17,

2017. <https://www.congress.gov/bill/115th-congress/house-bill/2481>.

"The Future of Vulnerabilities Equities Processes Around the World." Lawfare. January 10, 2019.

<https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world>.

Timberg, Craig. "Heartbleed Bug Puts the Chaotic Nature of the Internet under the Magnifying Glass." The Washington Post. April 09, 2014.

https://www.washingtonpost.com/business/technology/heartbleed-bug-puts-the-chaotic-nature-of-the-internet-under-the-magnifying-glass/2014/04/09/00f7064c-c00b-11e3-bcec-b71ee10e9bc3_story.html?noredirect=on&utm_term=.fd4e1f75e4e0.

"Understanding the Heartbleed Proof of Concept." Westpoint.

<https://www.westpoint.ltd.uk/blog/2014/04/14/understanding-the-heartbleed-proof-of-concept/>.

"Vulnerabilities Equities Policy and Process for the United States Government" US Government.

<https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>. November 15, 2017.

Widenhouse, Kurt C. "Playpen, the NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to be Found."

<https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1285&context=jbtl>

"What Is SSL (Secure Sockets Layer)?" DigiCert. <https://www.digicert.com/ssl/>.

"What Is Backdoor (computing)? - Definition from WhatIs.com." SearchSecurity.

<https://searchsecurity.techtarget.com/definition/back-door>.

Zalkind Duncan & Bernstein LLP, and Zalkind Duncan & Bernstein LLP. "Big Changes to a Little-Known Rule: Rule 41(b) and the Unlawful Search That Paved Its Way." Boston Lawyer Blog. August 30, 2017.

<https://www.bostonlawyerblog.com/big-changes-little-known-rule-rule-41b-unlawful-search-paved-way/>.

"Zero-day Vulnerability: What It Is, and How It Works." Official Site.

<https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html>.