



Are U.S. government employees behaving ethically when they stockpile software vulnerabilities?

BY STEPHEN B. WICKER

The Ethics of Zero-Day Exploits—The NSA Meets the Trolley Car

THE MAY 2017 WannaCry ransomware attack caused a great deal of damage across Europe and Asia, wreaking particular havoc with Britain's National Health Service.^a The attack exploited a Microsoft Windows vulnerability that had been discovered

and exploited by the U.S. National Security Agency.⁵ The NSA informed Microsoft of the vulnerability, but only after the NSA had lost control of the assets it had developed to take advantage of the vulnerability. Shortly after the attack Microsoft President and Chief Legal Officer Brad Smith characterized the NSA and CIA's stockpiling of vulnerabilities as a growing problem:

Finally, this attack provides yet another example of why the stockpiling of

vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage.^b

Smith asserted that stockpiling of vulnerabilities, as opposed to immedi-

a <https://bit.ly/33dMn8d>


b <https://bit.ly/33dPi0L>

ately informing the software vendor, was wrong, in part because of its effects on Microsoft's customers. A national security operative might argue, however, that these same customers enjoyed a greater benefit through increased personal safety. As an example, this operative might point to the Stuxnet worm. Stuxnet took advantage of four Microsoft Windows vulnerabilities to attack a set of centrifuges that were critical to Iran's nuclear program.¹⁴ This highly sophisticated attack, created and delivered by agents of the U.S. and Israeli governments, may have saved the lives of potential targets of the Iranian nuclear program.


An ethical dilemma presents itself: Are U.S. government employees behaving ethically when they stockpile software vulnerabilities? To address this question, I begin by reviewing the nature of these vulnerabilities and the resulting "zero-day" exploits. I then consider whether participation in stockpiling is permissible from an ethical standpoint. This is a difficult problem, as the standard consequentialist arguments on which current policy is based are crippled from the outset by their need to cope with a great deal of uncertainty. Other complications include the alleged inability of decision makers to share the bases for their decisions with the general public, as well as a form of regulatory capture—those in a position to perform the ethical calculus are the same ones who will exploit the vulnerabilities. I argue these issues can be avoided by using a non-consequentialist approach. By creating detailed case studies for the ethical issues in play, computer scientists can develop a technically informed ethical intuition, and be in a better position to assist with policy moving forward.

Bugs, Vulnerabilities, and Exploits

Bugs have plagued computers and computer software since the six- and eight-legged varieties found their way into the electromechanical switches of UNIVAC. The problem continues today in the form of coding errors that lead to unexpected behavior on the part of computer software. Delivered code has been estimated to average from 15 to 50 errors per 1,000 lines across the industry.¹⁰ Through "cleanroom" techniques the number can be brought



Bugs rise to the level of vulnerabilities when they allow third parties to use the software in a manner that the scientist/engineer who wrote the code did not intend.



close to zero, but this is expensive, time-consuming, and usually limited to highly specialized and strictly compartmentalized government projects such as the space shuttle.

Bugs manifest themselves in a wide variety of forms, from the occasional crash to more subtle though potentially more dangerous behavior. Bugs rise to the level of vulnerabilities when they allow third parties to use the software in a manner that the scientist/engineer who wrote the code did not intend. For example, some vulnerabilities may allow a third-party to see information for which he or she is not authorized, while the worst allow a hacker to load and run malware on the machine on which the vulnerabilities reside.⁹ If the software vendor is unaware of a vulnerability in its product, the term "zero-day vulnerability" applies. "Zero-day" refers to the number of days the vendor has been aware of the vulnerability (zero), and thus the ongoing susceptibility of the software to ongoing attacks.⁹

A "zero-day exploit" is an attack that takes advantage of a zero-day vulnerability to compromise data on a target machine or to deliver and run malicious code on that machine. Zero-day exploits generally have two parts: the exploit code that gains access to a machine through a vulnerability, and an often-unrelated payload that is delivered to the machine once the exploit has gained access.⁹

Vulnerabilities in software are found through many means, but most techniques fall under three general headings: white box, gray box, and black box.¹⁷ The white box approach assumes complete access to source code, design specifications, and in some cases the programmers themselves. The black box approach takes the opposite extreme, assuming no knowledge of the internal structure of the software. As one might imagine, gray box attacks fall somewhere in between. In many cases, gray box attacks begin as black box attacks, but become increasingly gray as knowledge of the behavior of the target allows for refinement of the attack.

The most prominent example of a back/gray box attack is "fuzzing," a brute force approach in which the attacker provides overly large or otherwise unanticipated inputs to a program

and then monitors the response.¹⁷ This requires virtually no knowledge of the software beyond what constitutes an unanticipated input. Sutton, Greene, and Amini have likened this technique to “standing back, throwing rocks at the target, and waiting to hear a window break.”¹⁷ As we will see, the Eternal Blue vulnerability that led to the WannaCry attack appears to have fallen into this category.

For any given vulnerability and subsequent exploit, there are many possible timelines, some leading to problems and others not. Consider the following set of possible events and associated times for a given problem (acknowledging that, for some vulnerabilities, one or more of these events may never occur).

- T_B : Code with Vulnerability Produced
- T_T : Vulnerability Discovered by Third Party
- T_G : Vulnerability Discovered by Government Employees
- T_S : Vulnerability Discovered by the Software Vendor
- T_P : Patch Developed and Deployed by Software Vendor
- T_{CP} : All Vulnerable Computers Patched

A zero-day exploit is possible whenever the government or a third party discovers a vulnerability that the vendor of the software has yet to detect. This occurs whenever the following holds:

$$\max [(T_S - T_T), (T_S - T_G)] > 0$$

Given that the development of a patch takes a non-zero amount of time, the minimum window of vulnerability to hacking by a third party is $(T_P - T_T)$. This attack window can be shortened if T_S and thus T_P are moved up in time. It follows that there is room for the government to have a positive impact on software security if it informs the vendor of a vulnerability before the vendor discovers it on its own.^c

One can imagine a host of hypothetical situations based on who discovers what when, supporting a wide variety of arguments and assertions along the

» key insights

- Policies that try to balance the benefits of stockpiling zero-day exploits against the threat to the general public will generally fail, as they attempt to balance objectives that are probabilistic, or even incommensurable.
- Non-consequentialist ethics offer a better guide to policy making, as it captures our ethical intuition regarding the public risk that many think is inherent in zero-day exploits and, more generally, cyberwarfare.
- Public policy that educates the public about stockpiling while reducing general risk will find more favor with the public, and will be more ethically appealing to the practitioner.

way. Fortunately, there is data that lends credence to some of these hypothetical situations, providing us with points of focus. In a recently released RAND Corporation study, Ablon and Bogart provide a statistical analysis of several hundred actual zero-day vulnerabilities and exploits.¹ There were many interesting conclusions; but for our purposes, the following are particularly on point:

- In the RAND dataset, exploits and their underlying vulnerabilities had an average life expectancy of 6.9 years after initial discovery. Some 25% of exploits did not survive for more than a year and a half, and another 25% survived for more than 9.5 years.
- Once an exploitable vulnerability had been found, the median time required to develop a fully functioning exploit was 22 days.
- For a given stockpile of zero-day vulnerabilities, approximately 5.7% had been discovered by an outside entity after one year.

In an unrelated study, Bilge and Dumitras examined data from 11 million active hosts to identify files that exploited known vulnerabilities.⁴ They found that after zero-day vulnerabilities became public knowledge, the number of malware variants exploiting them increased between 183 to 85,000 times, while the number of attacks increased between 2 and 100,000 times.

In summary, vulnerabilities can last for a very long time, and the likelihood of two or more parties finding the same vulnerability is small, but **non-zero**. Further, once a vulnerability becomes known, it will be rapidly exploited by a large number of hackers.

To see how these tendencies played out in a specific case, consider the WannaCry attack in further detail. The delivery vehicle in this instance was a vulnerability that had been known and potentially exploited by the NSA but was published to the world at large by the Shadow Brokers in April 2017, and apparently from there made its way into the hands of the North Korean government.⁴ The particular vulnerability at the heart of the attack was found in a Windows transport protocol called Server Message Block (SMB). SMB operates over the Transmission Control Protocol (TCP), supporting read and write transactions between an SMB client and a server. Codenamed “EternalBlue” by the NSA, the vulnerability was probably found through fuzzing; when an SMB message request exceeds the maximum buffer size, the SMB server moves to a state in which the vulnerability can be exploited.⁷

Having learned of (or discovered) EternalBlue, the WannaCry perpetrators used the vulnerability to put target machines in the desired vulnerable state, and then issued a “request data” command that caused an encrypted viral payload to be loaded onto the target machines. The payload included ransomware as well as software that searched for other machines that had the same vulnerability. The ransomware rapidly propagated across the Internet, infecting machines that shared the EternalBlue vulnerability.

The WannaCry ransomware portion of the payload encrypted hard drives, making them inaccessible to their owners, then presented a request for a few hundred dollars in Bitcoins for reversing the operation. It has been estimated that 230,000 computers in over 150 countries were infected in the first day of the attack.² As the attack spread across Europe and Asia, it damaged Britain’s National Health Service, in part because the NHS employees were not in a position to immediately provide the requested Bitcoins. In many cases doctors were blocked from gaining access to patient files, and emergency rooms were forced to divert patients to other facilities.^d In the Essex town of Colchester, the hospital closed

c The problem remains that T_{CP} may always be in the future. One may wish to refine the definition to cover only a suitable number of patched computers, along the lines of herd immunity in epidemiology.

d <https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html>

down a significant part of its facilities, only accepting patients in “critical or life-threatening situations.”^e

If the attackers learned of the EternalBlue vulnerability from the Shadow Brokers, it is noteworthy that the EternalBlue vulnerability was weaponized in a matter of weeks. Though this seems fast, the timeline is in keeping with the results of the RAND Corporation study. On the other hand, if the attackers knew of the vulnerability beforehand (having discovered it themselves), then this was an example of a “collision,” which the RAND analyses have also shown to happen with a small, but non-zero probability.

Whatever its origin, the attack highlighted a widespread failure on the part of individuals and corporations to patch their computers. Microsoft posted a security patch as part of Microsoft Security Bulletin MS17-010 (critical)^f on Mar. 14, 2017, a full two months before the first WannaCry attack. The inability of some to patch their computers in a timely manner reduces the impact of government disclosure of vulnerabilities to software vendors. We will bear this in mind when considering the balancing tests in the following section.

Is Stockpiling Ethical?

The Consequentialist Approach

Consequentialism is a school of ethics that holds that the morality of an act follows exclusively from its consequences.^g The utilitarianism of John Stuart Mill and Jeremy Bentham, usually summarized as holding that an ethical act is one that provides the greatest happiness for the greatest number, is probably the best-known example of consequentialist ethics.³ In determining the greatest good, one must, of course have a happiness metric of some sort by which to select from among a range of actions. Bentham developed a “felicific calculus” that he claimed would determine the

amount of happiness that a given act would bring.³

The computer scientists and philosophers who have weighed in on the question of whether government stockpiling of zero-day vulnerabilities is ethical have, for the most part, adopted a consequentialist approach, and have attempted to craft zero-day policies with the goal of providing the best possible outcome (however defined).^h For example, in “Zero Days, Thousands of Nights,” Ablon and Bogart frame the debate in terms of longevity and collision rate, asserting that these factors determine whether stockpiling is desirable:

*Government agencies, security vendors, and independent researchers have each been trying to determine which zero-days to hold on to and for how long. This generally involves understanding (1) the survival probability and expected lifetime of zero-day vulnerabilities and their exploits (longevity) and (2) the likelihood that a zero-day found by one entity will also be found independently by another (collision rate). While longevity of a vulnerability may be an obvious choice of desired metric, collision rate is also important, as the overlap might indicate what percentage of one's stockpile has been found by someone else, and possibly the types of vulnerabilities that may be more or less desirable to stockpile.*¹ (emphasis added.)

Ablon and Bogart are using longevity and collision rate as inputs to a calculus that provides a greatest good: an optimal balance between maintaining a set of offensive capabilities and preventing attacks against one's own people. They refine the calculus by arguing that if there are multiple vulnerabilities, then the rationale for disclosing a known vulnerability to the software vendor diminishes. They further argue that disclosure makes little sense if vulnerabilities are very hard to find.

If another vulnerability usually exists, then the level of protection consumers gain from a researcher disclosing a vulnerability may be seen as modest, and some may conclude that stockpiling

*zerodays may be a reasonable option. If zero-day vulnerabilities are very hard to find, then the small probability that others will find the same vulnerability may also support the argument to retain a stockpile.*¹

We have already noted that some users do not patch their computers in a timely manner; in the above analysis, the consequent reduced impact of disclosure would also weigh against disclosure, increasing the ethical attraction of stockpiling from a balancing perspective.

Other attempts to find the right balance have led to similar analyses. For example, in “Would a ‘Cyber Warrior’ Protect Us: Exploring Trade-Offs Between Attack and Defense of Information Systems,” Moore, Friedman, and Procaccia adopt a game-theoretic approach that yields a decision process that, they argue, would best protect the public while maintaining a satisfactory offensive capability.¹¹

The U.S. government made an effort to implement a balancing doctrine in the form of the “Vulnerability Equities Process” (VEP). Former White House Cybersecurity Coordinator Michael Daniel described VEP as follows:

*Each such agency then is responsible for designating one or more Subject Matter Experts (“SMEs”) to participate in a discussion convened by the Executive Secretary to arrive at a consensus on whether the vulnerability should be retained by the government or disclosed for patching.*⁶

Daniel asserted that the process was strongly biased toward disclosure of vulnerabilities.

In a Belfer Center discussion paper, Ari Schwartz and Rob Knake criticized the process, noting the process has apparently lapsed at least once.

*While the Obama Administration deserves credit for re-invigorating the process and for demonstrating a clear bias toward disclosure, the fact that the process fell into disuse from when it went into effect in 2010 until the Intelligence Review Group made its recommendations in 2014 is troubling.*¹⁶

Schwartz and Knake went on to recommend that the government “[m]ake public the high-level criteria that will be used to determine whether to disclose to a vendor a zero-day vulnerability in their product, or to retain the vul-

e <https://bit.ly/30hMA8n>

f <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

g This definition is sufficient for assessing balancing considerations, and as a contrast to the non-consequentialist discussion to follow. For more details on consequentialism, see Samuel Scheffler (Ed.), *Consequentialism and Its Critics*, Oxford University Press, 1988.


h This is a separate question from that of the ethics of using the vulnerabilities. We will save the question of whether zero-day exploits are ethical for another day, noting that this involves the Pandora's box of cyber warfare and questions of just war.

nerability for government use.” It is notable that the documents that provide an overview of the VEP were only made public through a FOIA request by the Electronic Frontier Foundation.


In summary, consequentialist arguments assert that U.S. citizens are best served by zero-day exploit policies that balance a current threat (that of identity theft, loss of data, suffering from the hacking of our critical infrastructure, among others) against the mitigation of a future threat (loss of economic dominance or an attack by a foreign power using advanced weaponry).

There are problems with this approach. For example, consider whether there is an *ethical* obligation for the state to provide aid by immediately informing software vendors of vulnerabilities. Consequentialist ethics has an “Equivalence Thesis” that holds that there is no distinction between the failure to aid and actively doing harm.⁸ This follows from the fact that consequentialists focus on outcomes, rather than intent. North Korea may have been the efficient cause of the WannaCry attack, but as Brad Smith noted, the NSA played a role. If one is to invoke balancing arguments, one must accept responsibility when the balance fails. To avoid being complicit with WannaCry-type attacks, government agencies must *immediately* inform software vendors of flaws discovered in their software. This is not necessarily a weakness in the balancing argument, but it does suggest that the practitioner should be willing to take responsibility and explain what happened when preventable attacks occur.

There is another underlying assumption of balancing arguments that is problematic; namely, that a good balance exists at all. In other words, it is assumed that some risk to the public is worthwhile given the corresponding offensive capability obtained through stockpiling vulnerabilities. It may be that no risk is acceptable—the damage done by a single WannaCry-type attack may be far greater than the potential gains from an offensive cyberattack by the U.S.. In the RAND study discussed earlier, Ablon and Bogart acknowledge that “some” may conclude that if there is *any* chance that a vulnerability may



Even if an accurate assessment of longevity and collision rate were possible, it would require a detailed knowledge of the software available only to the programmers themselves.



be found by another party, then that vulnerability should be disclosed to the vendor.

On the other hand, our analysis shows that the collision rates for zero-day vulnerabilities are non-zero. Some may argue that, if there is any probability that someone else (especially an adversary) will find the same zero-day vulnerability, then the potentially severe consequences of keeping the zero-day private and leaving a population vulnerable warrant immediate vulnerability disclosure and patch. In this line of thought, the best decision may be to stockpile only if one is confident that no one else will find the zero-day; disclose otherwise.¹

Given that we are considering vulnerabilities in software that is in general public use, there is *always* a non-zero probability that an adversary will find a given vulnerability.

There is a further potential problem of incommensurability—there may be no acceptable basis for comparing the potential damage of a WannaCry-type attack to the added safety derived from stockpiling vulnerabilities for later use as offensive weapons. What sort of metrics can be used? Ablon and Bogart proposed the use of longevity and collision rates, but several problems arise immediately. How do we translate longevity into a utility metric? What likelihood of collision is too high? All of this assumes, of course, that longevity and likelihood of collision can actually be determined for a specific vulnerability.

Even if an accurate assessment of longevity and collision rate were possible, it would require a detailed knowledge of the software available only to the programmers themselves. It would further require a knowledge of the resources and skillset of likely attackers that would be known only to certain individuals in security agencies. There may be very little overlap between these two groups, but even if there were, the task of assigning probability metrics to longevity and collision rates for a given vulnerability would involve a great deal of guesswork.

Which brings me to a final problem with the balancing approach, namely the potential for inherent bias: those who are making the balancing decisions are generally the same people who will develop and launch the ex-


plots. The apparent lack of enthusiasm for the Vulnerability Equities Process is a case in point.

In the face of these problems, it is difficult to see how a governmental decision maker can arrive at a demonstrably ethical, well-balanced and objective stockpiling decision.


Is Stockpiling Ethical? The Non-Consequentialist Approach

There is another approach to ethical questions that may, in this instance, provide more clarity. Non-consequentialist ethics assume the rightness or wrongness of a given act cannot be based solely on the consequences of that act.⁸ Sometimes it is not ethical to choose the act that provides the greatest good for the greatest number; we must also look to prerogatives and constraints that appeal to our ethical intuition to get a more complete picture of an ethical obligation. In non-consequentialist studies, ethical intuition is developed through the study of hypothetical cases. The basic idea here is that such situations help to isolate the individual from personal details that may create a bias, providing a less cluttered focus on the ethical issues involved.

As an example, consider the famous case of the runaway trolley car.ⁱ Assume the driver of a trolley car has lost control, and that the car is now hurtling toward five people who are tied to the tracks. (In these scenarios we must stick to the facts at hand and not start wondering how we arrived at this situation.) A bystander finds herself next to a switch which, if thrown in time, will divert the trolley and save the five people. Unfortunately, the diversion will cause the trolley to run down a sidetrack and kill a single person who happens to be on that track. What is the bystander to do? To do nothing would entail the certain death of five people, while turning the switch



In determining the greatest good, one must have a happiness metric of some sort by which to select from among a range of actions.



would lead to the certain death of a single, otherwise safe individual.

Having given this some thought, most people agree that it would be ethical for the bystander to throw the switch and save the five at the cost of the one.¹⁵ In exploring the nature of this intuition, ethicists have developed the Doctrine of Double Effect: a foreseen, but unintended harm in pursuit of a greater good is ethically permissible, while an intended harm is not. The Doctrine of Double Effect thus acts as a constraint on intended harm, even when the harm may lead to a greater good.⁸

In order to sharpen the contrast between the foreseen and the intended, consider “the transplant case.” A noted surgeon has five patients, all of whom need transplants of various kinds if they are to survive. We may assume the surgeries will be successful and that the patients will thrive if they receive the various organs. Early one morning a strong healthy individual who has the needed organs walks into the surgeon’s office, asking for directions to the nearest fitness center. The surgeon has the skill to harvest the organs and save his five patients. Unfortunately, the harvesting of the organs will kill the strong healthy individual. Should the surgeon take the organs anyway, saving five lives at the cost of the one? Though on its surface, the ethical arithmetic appears identical to that of the trolley car case, in the transplant case most people would say that harvesting the organs is not ethically permitted. The intuition in this case rests on the fact that the death of the one was not only foreseen but was also intended.

In developing hypothetical cases to study the ethics of stockpiling, I adopt two guidelines.

- The cases must engage with the facts, while bringing those facts closer to home for those less versed in the details of computer hacking. This guideline broadens the discussion, making the issues more accessible.

- The cases should elide facts that are not ethically dispositive, but may promote bias; for example, facts that appeal to political passions.

With these guidelines in mind, I offer the following, which I call “the electrical generator case.” A manufacturer of electric generators, let’s call it Mac-

i See Philippa Foot, The Problem of Abortion and the Doctrine of the Double Effect in *Virtues and Vices*, *Oxford Review* 5, 1967. Foot was a noted British philosopher and the granddaughter of the former U. S. President Grover Cleveland. What she referred to as the “tram problem” is now a cottage industry. See, for example, F.M. Kamm, *The Trolley Problem Mysteries* (The Berkeley Tanner Lectures), Oxford University Press, 2015.

roVolt, has come up with an electric generator that is so efficient and so inexpensive that it has become the world standard for generating electricity. The MacroVolt generator is used in laboratories, test facilities, hospitals and schools throughout the world. Unfortunately, the MacroVolt generator relies on a great deal of software, and that software has bugs. A government employee has discovered a vulnerability through which any given generator can be disabled. The laboratories of a particular foreign government, for example, can be disrupted and perhaps destroyed with a few lines of code, greatly postponing the development of weapons by that government. On the other hand, if an enemy agent finds this vulnerability, he or she can cut the electric power to hospitals and other critical infrastructure in our country with equal ease. The ethical dilemma is as follows: should the government employee keep the vulnerability a secret in the hope of using it as a weapon? Or should she tell MacroVolt as soon as possible to prevent an attack by a third party? I think that the potential threat to life and limb through the failure of medical, air traffic control, and other systems that depend on electricity clearly point to the latter.

The Doctrine of Double Effect can clarify this intuition. The potential threat to life and limb caused by the MacroVolt exploit is both foreseeable *and* intended. Any exploit designed to take advantage of the vulnerability is designed to disrupt *any* generator, not just those of a foreign power.

Note the similarity to the WannaCry attack. The damage caused was foreseeable *and* intended. It is certainly true that the NSA developed the EternalBlue exploit for use against a foreign adversary, and not, presumably, the British health care service. But it is also the case that the EternalBlue exploit was intended for use against a vulnerability that the NSA knew to be shared by *all* instantiations of the target Microsoft software, whether used by adversaries, allies, or U.S. citizens. The EternalBlue exploit was intended to cripple *any* user of Microsoft software, as the attack apparently did not distinguish, say, Farsi versions of the software from that used in the U.K.

Now change the scenario slightly

and consider the “research generator case.” Suppose that MacroVolt’s generators are extremely expensive, and only used in government research environments that require a precise and stable power source. For this reason, MacroVolt’s generators are often used in nuclear weapons research, but generally not in commercial or medical environments. Once again, a government employee has discovered a vulnerability through which any given generator can be disabled. Should the government employee keep the vulnerability a secret in the hope of using it as a weapon? Now the decision to stockpile and later exploit the vulnerability seems more ethically permissible. What changed? It seems less ethically problematic that our own government research facilities are taking the risk of stockpiling upon themselves as opposed to allocating the risk to the public at large. This is an example of a core intuition in non-consequentialist ethics; namely, that individuals should not be used as a means to an end.


Non-consequentialist ethics can thus be used to hone our understanding of ethically permissible and non-permissible risk. By creating narratives that put us at a distance from the facts of a situation, we are better placed to engage our ethical intuition. One may conclude from the above that, in the case of vulnerabilities to software in general use, stockpiling is not ethically permissible. But with some efforts to mitigate the risk to the general public, stockpiling becomes permissible.

Conclusion and Further Thoughts

In this article we have taken two basic approaches to evaluating the ethics of stockpiling zero-day exploits. I have argued that the consequentialist approach has significant difficulties, primarily due to problematic underlying assumptions and a need to balance objectives that are probabilistic, or even incommensurable.

The non-consequentialist approach, on the other hand, offers more traction, capturing our ethical intuition regarding the public risk that many think is inherent in zero-day exploits in particular and cyberwarfare in general. Public policy that attempts to educate the public about stockpiling while reducing general risk will find

more favor with the public. Perhaps of equal importance, those who are involved with the stockpiling and the development of exploits will have greater cause to feel they are both defending their country and engaging in demonstrably ethical activity.

Acknowledgments. I thank the Cornell Einaudi Center for the opportunity to present these ideas at the 2018 Workshop on Privacy, Surveillance, and Civil Society. Thanks to Rebecca Slayton, Fred Schneider, and Linda Lader for their insightful comments and to Sarah Wicker for her encouragement, editorial skills, and ethical equilibrium. 

References

1. Ablon, L. and Bogart, A. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. The RAND Corporation, 2017, Santa Monica, CA, USA.
2. BBC News. Cyber-Attack: Europol says it was unprecedented in scale. May 13, 2017; <http://www.bbc.com/news/world-europe-39907965>.
3. Bentham, J. *An Introduction to the Principles of Morals and Legislation*. London, 1789. Also in *Collected Works*. J.H. Burns and H. L. A. Hart, Eds. Clarendon Press, Oxford, U.K., 1970.
4. Bilge, L. and Dumitras, Y. Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM Conf. Computer and Communications Security*, 833–844.
5. Brewster, T. An NSA Cyber weapon might be behind a massive global ransomware outbreak. *Forbes*, May 12, 2017; <https://bit.ly/3l3qwGu>
6. Daniel, M. Heartbleed: Understanding When We Disclose Cyber Vulnerabilities. Whitehouse.gov blog, (April 28, 2014).
7. Islam, A., Oppenheim, N., Thomas, W. SMB exploited: WannaCry use of ‘EternalBlue’. *FireEye*, May 26, 2017; <https://bit.ly/3n3Z2m7>
8. Kamm, F.M. *Intricate Ethics: Rights, Responsibilities, and Permissible Harm*. Oxford University Press, 2007.
9. Libicki, M.C., Ablon, L., Webb, T. The Defender’s Dilemma: Charting a Course Toward Cybersecurity. The RAND Corporation, 2015, Santa Monica, CA, USA.
10. McConnell, S. *Code Complete: A Practical Handbook of Software Construction*. Microsoft Press, Redmond, WA, USA, 2004.
11. Moore, T., Friedman, A., and Procaccia, A.D. Would a ‘cyber warrior’ protect us: Exploring trade-offs between attack and defense of information systems. In *Proceedings of the 2010 Workshop on New Security Paradigms*. ACM, New York, NY, 2010, 85–94.
12. Nakashima, E. The NSA has linked the WannaCry computer worm to North Korea. *Washington Post*, (June 14, 2017); <https://wapo.st/2SpSPmB>
13. Nakashima, E. and Gregg, A. NSA’s top talent is leaving because of low pay, slumping morale and unpopular reorganization. *Washington Post* (Jan. 2, 2018); <https://wapo.st/30m9Xh9>
14. Ryan, N. Stuxnet attackers used 4 Windows zero-day exploits. *ZDNet*, (Sept. 14, 2010); <http://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/>
15. Sandel, M. *Justice: What’s the Right Thing to Do?* Farrar, Straus, and Giroux, New York, NY, 2009, 21.
16. Schwartz, A. and Knake, R. Government’s Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process. Discussion Paper 2016–04. Harvard University, Belfer Center, Cambridge, MA, USA, June 2016.
17. Sutton, M., Greene, A. and Amini, P. *Fuzzing: Brute Force Vulnerability Discovery*. Addison-Wesley, Boston, MA, 2007.

Stephen B. Wicker is a professor of electrical and computer engineering at Cornell University, Ithaca, NY, USA.