# Harboring Malware for Good: Government Purchase of Zero-days

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Roman Bohuk
April 3, 2020

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: _____ Date: _____
Roman Bohuk

Approved: _____ Date: _____
Peter Norton, Department of Engineering and Society

**Harboring Malware for Good: Government Purchase of Zero-days**

The development of internet made the world connected as never before, but it also opened a venue for a new style of combat. Cyberwarfare allows states to remotely and discretely collect intelligence, disrupt enemy infrastructure, and even influence politics. In an attempt to grow their influence and augment national security, many countries have secretly invested into development of cyberwarfare capabilities (Halpern, 2019). The U.S. cyber arsenal is secret, but emerging evidence of its methods have attracted criticism.

Cyberweapons rely on *zero-day exploits*: vulnerabilities in popular software that are unknown to the public and to the authors of the code. Through such vulnerabilities, attackers can penetrate secure and up-to-date code. Stuxnet, a 2009 worm developed by United States to damage Iran's nuclear power plant, exploited four such zero-days at once (Naraine, 2010). Since value can be gained from the knowledge of these flaws, they can also be referred to as *vulnerability equity*.

As vulnerabilities accumulate in publicly used software, knowledge of them may leak or adversaries may discover and exploit them directly. Governments therefore face a dilemma: do they disclose exploits or do they hide them for a later use? (Weaver, 2017). Retaining a zero-day compromises national cybersecurity, yet disclosing it to vendors for patching may impair criminal investigations, intelligence gathering, or offensive military cyber operations (Schwartz & Knake, 2016). Because of these side effects and lack of faith in the government, secret stockpiling of vulnerabilities is controversial.

Since the turn of the 21$^{st}$ century, government agencies across the world have been developing vulnerability equity processes to govern their collection of zero-days and procedures

for their release. Iterations of these policies have been described as opaque and ambiguous (Lieu, 2017; Geiger, 2017) despite agencies' claims to err on the side of disclosure (Healey, 2016). Public distrust makes matters worse. Privacy advocacies, such as the Electronic Frontier Foundation, contend that retaining vulnerabilities degrades security and privacy. Only through transparency can government intelligence and security agencies rebuild public trust. Governments must balance internet security against other goods, amid public pressures. In addition, the need for these cyberweapons by governments and criminals has led to a creation of unregulated black and grey markets with additional stakeholders and agendas that need to be considered (Gallagher, 2013).

**Review of Research**

An optimal vulnerability equity process would account for the age of the exploit, the security of vulnerability storage, effects on unregulated markets, and the extent of authority that governs it. Researchers have studied individual components of such a process.

Ablon & Bogart of the RAND Corporation (2017) argue that the merits of a zero-day release to the vendor depend on adversaries' awareness of it, which is difficult to gauge. Within a year, about 5.7 percent of any given set of vulnerabilities have been discovered by others. Emery (2017) suggests that by purchasing zero-days, governments encourage responsible disclosure by private researchers, keeping the vulnerabilities off the black market. They also propose that companies cannot rely on responsible disclosure and should instead invest in novel anomaly intrusion detection mechanisms that would make these newly exploits obsolete.

Stockton and Golabek-Goldman (2013) report a "booming" black market for zero-day exploits and offer explanations of its growth. They find that researchers can make more money

from weaponizing the vulnerability than responsibly disclosing it because affected vendors of vulnerable software do not pay enough in comparison to the black market.

Security researchers Aitel and Tait believe that the current vulnerability equities process proposed by the US intelligence community is hasty and a poorly though-out public relations cover developed in response to growing criticism from the public (2016). They suggest a lack of evidence that zero days used by the U.S. actually overlap with those of adversaries. Disclosing the vulnerability to the vendor makes the application more secure against the specific vulnerability, but it does not guarantee any protection from Russians, Chinese, or Iranians. Such disclosures waste the state's financial resources without any proven benefits. It is even worse when the company then sends the information about the vulnerability to a foreign contractor for remediation, which can be easily exfiltrated by the government of that country.

In 1979 Axelrod proposed an approach to address similar geopolitical threats. A zero-day can be generalized as a state's resource of surprise. To exploit surprise, a state must risk losing it. To expend surprise at the first opportunity is to lose the opportunity to use it later when it is more suitable. But because maintaining a surprise is expensive, Axelrod generally recommends that it is better to get a given payoff sooner rather than later.

**To Protect and Defend**

Cyber weapons have become indispensable to the military arsenals of many nation states. Like conventional weapons, exploits in cyberspace can advance national agendas, for example by obtaining intelligence or damaging adversary infrastructure (Zetter, 2014). It is recognized that the United States is not prepared to defend against similar attacks (Thomson, 2019), and its cybersecurity capabilities are growing to counteract this threat. The U.S. Army created a new

branch for cyber and the Pentagon has expanded its cybersecurity forces across all service branches. It is unclear, however, what these forces actually are and how the Department of Defense would use them (Vinik, 2015).

Governments must both protect the public from exploits online and also gather intelligence, enforce law, and conduct military operations that may require the use of such vulnerabilities (Herpig & Schwartz, 2019). Obama's Cybersecurity Coordinator Michael Daniel contended that "building up a huge stockpile of undisclosed vulnerabilities while leaving … the American people unprotected would not be in our national security interest. But that is not the same as arguing that we should completely forgo this tool as a way to conduct intelligence collection, and better protect our country in the long-run." Despite the claim of commitment to national security, the lack of guarantee has raised concerns and made his position controversial. Daniel described his difficulty: "too little transparency and citizens can lose faith in their government and institutions, while exposing too much can make it impossible to collect the intelligence we need to protect the nation" (2014).

Amid public pressures, government officials have changed their rhetoric. In 2013, former NSA chief Michael Hayden said the agency is not always "ethically or legally compelled" to help fix flaws it knows (Peterson, 2013). Former commander of the U.S. cyber command, General Keith Alexander, argues: "to ask NSA not to look for weaknesses in the technology that we use, and to not seek to break the codes our adversaries employ to encrypt their messages is … misguided. I would love to have all the terrorists just use that one little sandbox over there so that we could focus on them. But they don't" (2014). Releasing vulnerabilities would put the U.S. at a major security disadvantage and limit their ability to deal with threats.

In a 2013 report to President Obama, the National Security Agency proposed 46 recommendations designed to protect national security and advance foreign policy "while also respecting [the] longstanding commitment to privacy and civil liberties and recognizing [the] need to maintain the public trust" (Clarke et al., 2013). According to one recommendation, zero-day vulnerabilities should be stored only in rare circumstances and only for short times. The report recommended eliminating software vulnerabilities rather than using them for intelligence collection.

But the Obama administration's response retained a major loophole: zero-day vulnerabilities could be exploited if they have a "clear national security or law enforcement" use (Clarke et al., 2013). In 2013 NSA spent $25.1 million from the black budget on covert purchases of software vulnerabilities from private European malware vendors, according to top-secret documents obtained by *The Washington Post* (Gellman & Nakashima, 2013). Michael Daniel had asserted that government intelligence agencies do not aggressively seek and stockpile vulnerabilities (Zetter, 2014), but in 2013, Edward Snowden's leaks revealed countless examples of U.S. efforts to develop offensive capabilities. In 2014, the discovery of the devastating "Heartbleed" bug caused even more concerns. Bloomberg reported that NSA retained the vulnerability for over two years before it was discovered publicly instead of patching it. This series of events further undermined public trust (EFF, 2014). A similar incident happened in the UK. When Privacy International filed a lawsuit against GCHQ's illegal hacking operations in the Investigatory Powers Tribunal, the government quietly ushered through legislation amending the anti-hacking laws to exempt GCHQ from prosecution, notifying the plaintiff just hours prior to a hearing (Privacy International, 2015). Gripping tightly to their need for secrecy, agencies forgot about the citizens.

In the aftermath of these events, the Electronic Frontier Foundation filed a lawsuit under the Freedom of Information Act to access the federal Vulnerability Equities Process, which was subsequently released in 2016. It outlined a process with a pipeline of reviews and approvals for every new exploit. In a follow-up blog post, the White House summarized these criteria: presence and the extent of the vulnerability in actively used systems, its magnitude and potential damage if misused, and the likelihood of discovery by others.

More recently, the discussion has been more productive. In a 2018 report, Rasmussen revealed that 34 percent of likely U.S. voters believed that FBI was more likely to have meddled in the 2016 elections than Russia (42 percent). Acting more carefully, the former White House cybersecurity coordinator Rob Joyce acknowledged the "tension between the government's need to pursue rogue actors in cyberspace through the use of cyber exploits, and its obligation to share its knowledge of flaws" to "ensure digital infrastructure is upgraded and made stronger in the face of growing cyber threats" (2017). Jeanette Manfra, U.S. Cybersecurity and Infrastructure Security Agency assistant director for cybersecurity, declared fiscal year 2020 the agency's "year of vulnerability management" (Heckman, 2019). In 2018, GCHQ published the "Equities Process" guiding retention or publication of a vulnerability by three criteria: possible remediation, operational necessity, and defensive risk (GHCQ, 2018).

**Subversion of Global Security**

The Electronic Frontier Foundation suggests that when a government creates, acquires, stockpiles, or exploits weaknesses in digital security, it risks making everyone less safe by failing to bolster that security (Crocker, 2016). Likewise, Kevin Bankston, the director of the Open Technology Institute at New America, argues that when government agencies stockpile

vulnerability information about widely used software products, they leave the users of that software open to attack (Whittaker, 2017). Such exploits include ransomware known as WannaCrypt, which was developed by NSA, leaked by Shadow Brokers, and used to wreak havoc on 74 countries (Thomson, 2017).

When an adversary learns of the vulnerability, everyone is at risk. The success of public policies governing retention or disclosure depend on the likelihood of someone else discovering the flaw. Research from Harvard suggests that zero-day vulnerabilities are independently rediscovered much faster than previously thought (Herr, Schneier, & Morris, 2017), and are therefore more likely to be used against Americans before manufacturers can fix them (Waterman, 2017). This reveals that the policies currently in use by the government may be operating on wrong assumptions.

This problem has privacy implications as well. With a secret backdoor to a company's data, government intelligence agencies can obtain the personal information of their citizens. When FBI asked Apple to unlock an iPhone to help in its investigation of a terrorist case, the company refused (Nakashima, 2016). Apple's CEO Tim Cook (2016) argued that a secret key to a phone would only be "as secure as the protections around it" and it would be equivalent to a master key "capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes." That key could be leaked, or the attackers could reverse engineer it for themselves. Since the time a group leaked a portion of NSA cyberweapon code known as EternalBlue on the internet in 2017, it has been the standard offensive tool for exploiting Windows SMB service (Newman, 2018). Evidently, a decryption key can be leaked, despite of what some government agencies may claim. Even if that key existed, its uses would also not have been known. A possible contributor to this dilemma comes from the fact that modern

adversaries tend to use same tools, software, and protocols as regular citizens, making it nearly impossible to distinguish friend from foe when observing communications and deciding what to crack. “It used to be that only, say, German forces used a crypto-device like Enigma to encipher their messages. But in today’s environment, encryption technology is embedded into all our communications” (Alexander, 2014).

To its critics, the Vulnerabilities Equities Process is opaque and unclear. Government agencies such as NSA claim to err in favor of disclosure (Rogers, 2014), but they are still not required to report security flaws to manufacturers. According to EFF (2017), government cyberwarfare tools are “disproportionate to the threat” and “as a society, we have an interest in protecting innocent users from the collateral effects of intrusive surveillance.” The rules governing public disclosure to manufacturers remain mostly under wraps (Whittaker, 2017). V.E.P. is not law.

The National Security Agency has been hacked before. Whistleblowers like Snowden leaked vast information, and groups of hackers are now selling U.S. government cyber-spying tools in online auctions. Despite its own recommendations in a 2013 report to the Obama administration about preferring disclosure (Clarke et al., 2013), the agency was caught red-handed and further lost the public trust it sought to maintain. The volume and severity of the exploits suggests that the agency may have violated White House policy governing secrecy and disclosure (Condliffe, 2016). “The agency regarded as the world’s leader in breaking into adversaries’ computer networks failed to protect its own” (Shane, Perlroth, & Sanger, 2017). Because of these risks, California Representative Ted Lieu claimed that the current process is “unaccountable to the American people” especially “when our medical records, bank accounts and communications are on the line” (2017). The world’s militaries may be investing more

money in finding vulnerabilities than the commercial world is investing in fixing them. “No matter what cybercriminals do, no matter what other countries do, we in the U.S. need to err on the side of security and fix almost all the vulnerabilities we find” says Bruce Schneier, an American cryptographer and a fellow at Harvard Law School (2014).

**Practical Considerations**

Government purchase of zero-days turns exploits into a valuable commodity. Contractors profit from such work, and there is no incentive to slow down. But some social groups seek to reduce governments’ access to spying tools by identifying flaws before others do (Greenberg, 2014). Google Project Zero pays researchers to find and report vulnerabilities in popular software and tools, whether they are owned by Alphabet Inc. or not (Google, 2019). Companies offer bug-bounty programs (HackerOne, 2017; Ahmed, 2015) to deter developers from selling their findings to governments. For cyber criminals, crime can pay, and some researchers who identify flaws for a living may not care how their work is used (Barth, 2019).

If a government were to stop stockpiling zero-days and release them all instead, the profitability of government procurement and research would vanish. Researchers would then find it more profitable to sell vulnerabilities to criminals, promoting a black market. Independent marketplaces such as a Washington, D.C. based startup Zerodium provide malware to multiple nation states (Zerodium, n.d.). These services are largely unregulated, but are also government sponsored. If government contracts cease, such groups may switch sides.

One of the recommendations proposed in the aforementioned report from NSA to the Obama administration suggested that the “US Government may be authorized to use temporarily a Zero Day instead of immediately fixing the underlying vulnerability” (Clarke et al., 2013).

Researchers like Aitel and Tait believe this to be a “terrible idea.” Due to the lack of talent needed to turn a vulnerability into a deployable exploit, every attempt would require monumental investment of time and resources. Patching vulnerabilities after they have been used also leaks which vulnerabilities the U.S. found and exploited (Aitel & Tait, 2016).

Like unilateral nuclear disarmament, unilateral forfeiture of vulnerability equity is risky (Hardin, 1983), as it also puts a nation at a military disadvantage. A global agreement may therefore be necessary to deter zero-day exploits. Yet some researches contend that without a treaty, if the United States were to unilaterally adopt a norm by which zero-days would be disclosed after a limited period, the U.S. would destroy their value as weapons and simultaneously disarm the U.S., other countries and criminals without having to negotiate a treaty (Nye, 2015). Schwartz and Knake (2016) suggest that with sufficient funding, agencies could afford substitute techniques and therefore would not need to retain vulnerabilities for an extended period merely because they do not have the funding necessary to obtain replacements on demand (2016).

## Conclusion

At first, the dilemma of zero-day retainment seems to be unprecedented. It may feel that way because even tactics wrapped in secrecy, such as covert military raids, are governed by some standards about when and how the military uses them (Vinik, 2015). Vulnerability disclosure is almost never legally mandatory and processes do not consistently determine when a disclosure is necessary. Nevertheless, in its essentials the problem of zero days is not unique and its examination affords insight into analogous problems in other fields and vice versa.

Government agencies across the world have begun developing and releasing some internal processes that govern their vulnerability equity. They outline the entities involved in the decision-making process, the criteria used to determine whether or not to retain the vulnerability, and the methods of release. The Government Communications Headquarters, describes their mechanism: “Expert analysis, based on objective criteria, is undertaken to decide whether such vulnerabilities should be released to allow them to be mitigated or retained so that they can be used for intelligence purposes in the interests of the UK. The starting position is always that disclosing a vulnerability will be in the national interest” (GCHQ, 2018).

But stronger oversight is necessary to ensure that each participating agency favors disclosure when disclosure is warranted. Because threats to the national security from states and terrorist groups persist, conditional retention must be permitted, allowing security agencies to protect infrastructure against threats (Schwartz & Knake, 2016). Yet government agencies must also earn public trust. A government that has lost the confidence of its citizens cannot effectively protect them.

## References

Ablon, L., & Bogart, A. (2017). *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Santa Monica, CA: Rand Corporation.

Ahmed, M. (2015, Apr 10). Internet companies pay out to those who spot bugs. *Financial Times*, https://www.ft.com/content/fcd027b4-c0d7-11e4-876d-00144feab7de

Aitel, D., & Tait, M. (2016, Aug 18). Everything you know about the vulnerability equities process is wrong. *Lawfare.* https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong

Alexander, K. (2014, May 7). Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander. Interview by C. Joye. *Australian Financial Review*. https://www.afr.com/technology/interview-transcript-former-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140508-itzhw

Axelrod, R. (1979). The Rational Timing of Surprise. *World Politics*, 31(2), 228-246. www.jstor.org/stable/2009943

Barth, B. (2019, Aug 8). Selling zero-days to governments takes some business savvy, says former bug broker. *SC Magazine*. https://www.scmagazine.com/home/security-news/vulnerabilities/selling-zero-days-to-governments-takes-some-business-savvy-says-former-bug-broker/

Clarke, R. A., Morell, M. J., Stone, G. R., Sunstein, C. R., & Swire, P. (2013). *Liberty and security in a changing world*. The President's Review Group on Intelligence and Communications Technologies. https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Condliffe, J. (2016, Aug 18). The NSA hack shows it was sitting on a trove of severe computer vulnerabilities, experts say. *MIT Technology Review.* https://www.technologyreview.com/s/602201/security-experts-agree-the-nsa-was-hacked/

Crocker, A. (2016, Aug 1). What to do about lawless government hacking and the weakening of digital security. https://www.eff.org/deeplinks/2016/08/what-do-about-lawless-government-hacking-and-weakening-digital-security

Daniel, M. (2014, Apr 28). Heartbleed: understanding when we disclose cyber vulnerabilities. *The White House*. https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

EFF. (2014, Jul 1). EFF v. NSA, ODNI - vulnerabilities FOIA. Electronic Frontier Foundation. https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia

EFF. (n.d.). Government hacking and subversion of digital security. Electronic Frontier Foundation. https://www.eff.org/issues/government-hacking-digital-security

Emery, A. C. (2017). Zero-day responsibility: the benefits of a safe harbor for cybersecurity research. *Jurimetrics, 57*(4), 483-503. https://search.proquest.com/docview/1965541181

Gallagher, R. (2013, Jan 16). Cyberwar's gray market. *Slate.* https://slate.com/technology/2013/01/zero-day-exploits-should-the-hacker-gray-market-be-regulated.html

Geiger, H. (2017, Nov 16). Welcome transparency on government's vulnerability disclosure process. *Rapid7 Blog*. https://blog.rapid7.com/2017/11/16/welcome-transparency-on-governments-process-for-disclosing-vulnerabilities/

Gellman, B., & Nakashima, E. (2013, Aug 31). US spy agencies mounted 231 offensive cyber-operations in 2011, documents show. *Atlantic Council.* https://www.atlanticcouncil.org/blogs/natosource/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/

GCHQ. (2018). The equities process. Retrieved from Government Communications Headquarters website: https://www.gchq.gov.uk/information/equities-process

Google (2019, Jul 31). Vulnerability Disclosure FAQ. *Project Zero*. https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html.

Greenberg, A. (2014, Jul 15). Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers. *Wired*. https://www.wired.com/2014/07/google-project-zero/.

HackerOne (2017, Jan 3). Together We Hit Harder: HackerOne Company Values. *HackerOne Blog*, https://www.hackerone.com/blog/Together-We-Hit-Harder-HackerOne-Company-Values.

Halpern, S. (2019, Jul 18). The How cyber weapons are changing the landscape of modern warfare. *The New Yorker,* https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare

Hardin, R. (1983). Unilateral Versus Mutual Disarmament. *Philosophy & Public Affairs,* 12(3), 236-254.

Healey, J. (2016). The U.S. government and zero-day vulnerabilities. *Journal of International Affairs.* https://jia.sipa.columbia.edu/sites/default/files/attachments/Healey%20VEP.pdf

Heckman, J. (2019, Oct 24). CISA to kick off 'year of vulnerability management' with updated threat disclosure policy. *Federal News Network.*

https://federalnewsnetwork.com/cybersecurity/2019/10/cisa-to-kick-off-year-of-vulnerability-management-with-updated-threat-disclosure-policy/

Herpig, S., & Schwartz, A. (2019, Jan 4). The future of vulnerabilities equities processes around the world. *Lawfare.* https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world

Herr, T., Schneier, B., & Morris, C. (2017, Jul). Taking stock: estimating vulnerability rediscovery. *Belfer Center for Science and International Affairs, Harvard Kennedy School*. https://www.belfercenter.org/publication/taking-stock-estimating-vulnerability-rediscovery

Internet Society. (2019). 2018 cyber incident & breach trends report. *Internet Society's Online Trust Alliance*. https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf

Joyce, R. (2017, Dec 10). Improving and making the vulnerability equities process transparent is the right thing to do. https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/

Lieu, T. (2017, Jun 27). Bipartisan, bicameral lawmakers introduce bill to enhance cybersecurity, promote transparency. https://lieu.house.gov/media-center/press-releases/bipartisan-bicameral-lawmakers-introduce-bill-enhance-cybersecurity

Naraine, R. (2010, Sep 14). Stuxnet attackers used 4 Windows zero-day exploits. *ZDNet*. https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/

Nye, J. S. (2015, Oct 1). The world needs new norms on cyberwarfare. *The Washington Post.* https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html

Peterson, A. (2013, Oct 4). Why everyone is left less secure when the NSA doesn't help fix security flaws. *The Washington Post.* https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/

Privacy International. (2015, May 15). After legal claim filed against GCHQ hacking, UK government rewrite law to permit GCHQ hacking. https://privacyinternational.org/press-release/1158/after-legal-claim-filed-against-gchq-hacking-uk-government-rewrite-law-permit

Rasmussen Reports. (2018, Feb 7). *Just 42% think Russia meddled more in 2016 election than FBI.* https://www.rasmussenreports.com/public_content/politics/general_politics/february_2018/just_42_think_russia_meddled_more_in_2016_election_than_fbi

Rogers, M. S. (2014, Mar 11). Advance questions for vice admiral Michael S. Rogers, USN. Interview by U.S. Senate Committee on Armed Services. https://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf

Schwartz, A., & Knake, R. (2016, Jun). *Government's role in vulnerability disclosure*. Paper presented at Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf

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

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

Stockton, P. N., & Golabek-Goldman, M. (2013). Curbing the Market for Cyber Weapons. *Yale Law & Policy Review*, *32*(1), 239–266. https://digitalcommons.law.yale.edu/ylpr/vol32/iss1/11/

Thomson, I. (2017, May 13). 74 countries hit by NSA-powered WannaCrypt ransomware backdoor: Eeergency fixes emitted by Microsoft for WinXP+. *The Register.* https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/

Thomson, I. (2019, Aug 12). US still 'not prepared' in event of a serious cyber attack and Congress can't help if it happens. *The Register.* https://www.theregister.co.uk/2019/08/12/defcon_politicians_hackers/

Vinik, D. (2015, Dec 9). America's secret arsenal. *Politico.* https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331/

Waterman, S. (2017, Jul 21). Study: Zero-days rediscovered much faster. *Cyberscoop.* https://www.cyberscoop.com/zero-days-rediscovery-rate-herr-schneier-belfer-nsa/

Weaver, N. (2017, Sep 25). Is the NSA doing more harm than good in not disclosing exploits? *FP*. https://foreignpolicy.com/2017/09/25/is-the-nsa-doing-more-harm-than-good-in-not-disclosing-exploits-zero-days/

Whittaker, Z. (2017, May 17). Congress introduces bill to stop US from stockpiling cyber-weapons. *ZDNet.* https://www.zdnet.com/article/congress-introduces-bill-to-prevent-us-from-stockpiling-cyber-weapons/

Zerodium. (n.d.). Zerodium Solutions - zero-day research feed. https://zerodium.com/solutions.html

Zetter, K. (2014, November 17). U.S. Gov insists it doesn't stockpile zero-day exploits to hack enemies. *Wired.* https://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/