Northwestern Journal of Technology and Intellectual Property

Volume 20 | Issue 3 Article 4

Spring 2023

A LOADED GOD COMPLEX: THE UNCONSTITUTIONALITY OF THE EXECUTIVE BRANCH'S UNILATERALLY WITHHOLDING ZERO-DAYS

Brendan Gilligan

Recommended Citation

Brendan Gilligan, *A LOADED GOD COMPLEX: THE UNCONSTITUTIONALITY OF THE EXECUTIVE BRANCH'S UNILATERALLY WITHHOLDING ZERO-DAYS*, 20 Nw. J. Tech. & Intell. Prop. 471 (2023).
https://scholarlycommons.law.northwestern.edu/njtip/vol20/iss3/4

NORTHWESTERN
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

A LOADED GOD COMPLEX: THE UNCONSTITUTIONALITY OF THE EXECUTIVE BRANCH'S UNILATERALLY WITHHOLDING ZERO-DAYS

Brendan Gilligan

April 2023 VOL. 20, NO. 3

Copyright 2023 by Northwestern University Pritzker School of Law
Northwestern Journal of Technology and Intellectual Property

Volume 20, Number 3 (2023)

A LOADED GOD COMPLEX: THE UNCONSTITUTIONALITY OF THE EXECUTIVE BRANCH'S UNILATERALLY WITHHOLDING ZERO-DAYS[*]

Brendan Gilligan[*]

INTRODUCTION

In 2017, National Security Agency hacking tools were leaked on the Internet.[1] One of these hacking tools relied on a vulnerability in Microsoft software.[2] Its leak caused "the most destructive and costly N.S.A. breach in history."[3] This hacking tool took out:

> [the British health care system], Russian railroads and banks, Germany's railway, French automaker Renault, Indian airlines, four thousand universities in China, Spain's largest telecom, Telefonica, Hitachi and Nissan in Japan, the

[*] Note from Editors: An earlier version of this piece was published containing editing errors that were not present in the author's submission. Those editing errors have been removed in this version.

[*] Northwestern Pritzker School of Law, J.D., 2023. I'd like to thank Professor Heidi Kitrosser for all her help and guidance throughout the writing process. I'd also like to thank Grace Stippich for her comments and feedback, as well as the JTIP staff for their help in editing.

[1] NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS 331 (2020).

[2] *Id.* at 308.

[3] Nicole Perlroth & Scott Shane, *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc*, N.Y. TIMES (May 25, 2019), https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html [https://perma.cc/J374-5X4C].

> Japanese police, a hospital in Taiwan, movie theater chains in South Korea, nearly every gas station run by PetroChina, China's state owned oil company, and, in the United States, FedEx and small electrical companies across the country.[4]

Then, this hacking tool was added to a different cyberweapon, where it caused an additional $10 billion in damage.[5] Some consider this total a "gross underestimate."[6]

The executive branch, through an internal process,[7] had withheld this vulnerability from Microsoft for seven years.[8] According to the executive branch, this Microsoft vulnerability was too valuable to disclose: the hacking tool using the Microsoft vulnerability "netted some of the very best counterterrorism intelligence" the NSA received.[9] But the executive branch lacks the authority to unilaterally decide a vulnerability's intelligence value outweighs the cost of withholding it.

Vulnerabilities like the Microsoft one that the executive branch withheld are known as zero-day vulnerabilities ("zero-days").[10] This Comment's thesis is that the executive branch can't unilaterally withhold these zero-days to conduct offensive cyber operations or surveillance. I demonstrate this thesis in three steps. First, I explain what zero-days are and why they are dangerous. Second, I show the executive branch of the U.S. government unilaterally withholds zero-days. Third, and finally, I explain why the executive branch's unilateral withholding of zero-days to conduct offensive cyber operations or national security surveillance is unconstitutional.

I. WHAT ARE ZERO-DAYS AND WHY ARE THEY DANGEROUS?

A. Defining Zero-Days

A zero-day is a software or hardware vulnerability that's unknown to the vendor of that software or hardware.[11] For example, a bug in Apple's iOS software that Apple doesn't know about would be an iOS zero-day. These vulnerabilities are called zero-days because software and hardware vendors

[4] PERLROTH, *supra* note 2, at 333.

[5] *Id.* at 341.

[6] PERLROTH, *supra* note 2, at 341.

[7] *See infra* Section II.B.

[8] PERLROTH, *supra* note 2, at 309.

[9] *Id.*

[10] ANDY GREENBERG, SANDWORM 164 (2019).

[11] PERLROTH, *supra* note 2, at 7.

have had zero days to defend against these vulnerabilities when they're first used.[12]

Zero-days are incredibly powerful.[13] Like a global skeleton key, a zero-day for software can access any machine that's connected to the internet.[14] And what someone can do with this access is astonishing: zero-days can allow invisible spying of iPhone users,[15] dismantle chemical plants' safety controls,[16] or cause spacecrafts to crash into cities.[17]

Zero-days remain powerful until the vendor of the vulnerable hardware or software discovers them.[18] As we've already seen, vendors may not discover a zero-day in their products for an extended period of time: Microsoft remained unaware that the NSA was exploiting a zero-day in its software for seven years.[19] Once a vendor discovers a zero-day, they still need to patch the vulnerability and distribute that patch to customers.[20] And even after the vendor distributes a patch, their product remains vulnerable until customers update their software.[21]

B. In the Wild: Real World Uses of Zero-Days

1. Zero-Day Attacks on Physical Infrastructure

Turn now to zero-days' uses in the real-world. The most famous zero-day is probably Stuxnet.[22] With Stuxnet, American and Israeli intelligence agencies used a computer worm containing seven zero-days to destroy centrifuges in an Iranian nuclear enrichment plant.[23] Many likely also remember Apple appealing a court order requiring the company to grant the

[12] *Id.*

[13] *See id.* at 7–8.

[14] GREENBERG, *supra* note 11, at 6.

[15] PERLROTH, *supra* note 2, at 8.

[16] *Id.*

[17] *Id.*

[18] PERLROTH, *supra* note 2, at 7. Without discovering a zero-day, a vendor might change a vulnerable product so that it no longer includes the zero-day. *See id.* Thus, in the case of product changes, securing a vulnerable product might not require discovering a zero-day. *See id.*

[19] *See supra* text accompanying note 9.

[20] PERLROTH, *supra* note 2, at 7.

[21] *Id.*

[22] *See* PERLROTH, *supra* note 2, at 117–31. *See also* GREENBERG, *supra* note 11, at 96–105; DAVID E. SANGER, THE PERFECT WEAPON 7–36 (2018).

[23] PERLROTH, *supra* note 2, at 122. And as these centrifuges raced, plant workstations didn't know what they could do. *See* Rich McCormick, *Hackers Made Iran's Nuclear Computers Blast AC/DC*, THE VERGE (Aug. 7, 2014), https://www.theverge.com/2014/8/7/5977885/hackers-made-irans-nuclear-computers-blast-ac-dc [https://perma.cc/CTH4-AQFS] (along with destroying the centrifuges, Stuxnet caused plant workstations to play AC/DC's "Thunderstruck" at maximum volume).

FBI access to a terrorist's iPhone.[24] That appeal hearing never occurred because the FBI used a zero-day to break into the iPhone.[25]

Zero-days' uses in the nuclear proliferation and terrorism contexts might lead one to believe zero-days don't affect the general public. That impression would be false. To see how, look to Ukraine, where Russia has been using zero-days to carry out destabilizing cyber operations for years.

Start with an attempted coup. Four days before Ukraine's 2014 presidential election, Russian operatives used a Microsoft PowerPoint zero-day to hack into the computer network of Ukraine's Central Election Commission.[26] These operatives wiped the commission's computers and implanted malware that would've shown a far-right presidential candidate winning the election in the commission's reporting system.[27] The operatives then spammed the commission's server with traffic to prevent Ukrainian officials from confirming the election's actual outcome.[28] Simultaneously, Russian state media reported the far-right candidate had won.[29] Ukrainians discovered and thwarted Russia's plot just before reporting the election's results to Ukraine's media.[30]

Consider next Russian operatives' use of unpatched vulnerabilities to turn off the power in Ukraine's capital. After hacking into a Ukrainian power utility's computer network, Russian operatives used unpatched vulnerabilities to move across the utility's network to its industrial control system.[31] There, these operatives implanted malware they used to both cut customers' power and prevent the utility's operators from restoring it.[32] This left thousands of homes without power in near zero-degree weather.[33]

Recall the leaked NSA hacking tool discussed in this Comment's introduction that exploited a zero-day in Microsoft software[34]—that tool is

[24] *See* Eric Lichtblau & Katie Benner, A*pple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html [https://perma.cc/DQ97-GK7V].

[25] Cyrus Farivar, *FBI Paid at Least $1.3M for Zero-Day to Get into San Bernardino iPhone*, ARS TECHNICA (Apr. 21, 2016), https://arstechnica.com/tech-policy/2016/04/fbi-paid-at-least-1-3m-for-zero-day-to-get-into-san-bernardino-iphone/ [https://perma.cc/W49Q-NRL7].

[26] GREENBERG, *supra* note 11, at 5–8, 46–47.

[27] *Id.* at 46–47.

[28] *Id.* at 47.

[29] *Id.*

[30] PERLROTH, *supra* note 2, at xvii.

[31] GREENBERG, *supra* note 11, at 131–32.

[32] *Id.* at 132, 141.

[33] *Id.* at 2.

[34] After discovering hackers stole EternalBlue, the NSA alerted Microsoft to the vulnerability EternalBlue exploited; thus, EternalBlue was technically not a zero-day. PERLROTH, *supra* note 2, at 331. Microsoft also released a security update for this vulnerability before EternalBlue was leaked on the

known as EternalBlue.[35] EternalBlue was part of two destructive cyberweapons: WannaCry and NotPetya.[36] I discussed most of the damage WannaCry caused in the introduction: it ripped around the world and paralyzed networks of hospitals, utilities, and multinational corporations,[37] ultimately infecting 200,000 companies in 150 countries in the twenty-four hours before it was neutralized.[38]

NotPetya wreaked much more sustained havoc. NotPetya began with Russia infecting accounting software used by the Ukrainian government and most of Ukraine's large companies.[39] Next, it froze the computers at Ukraine's airports, ATMs, shipping and logistics systems, gasoline payment machines, and banks.[40]

Then NotPetya spread outside Ukraine. The cyberweapon stopped production at Merck, the pharmaceutical company.[41] It shut down international law firm DLA Piper's email system.[42] It completely brought down the computer network of Maersk, the world's largest shipping operator[43]: if not for a fortuitous power outage at the company's Ghana office, Maersk would've lost all data on its servers.[44] NotPetya also locked U.S. doctors out of their patients' records and prescription systems.[45] This global spread would contribute to NotPetya's becoming the most destructive cyberweapon in history.[46]

2. *Zero-Day Surveillance*

Zero-days also gravely threaten privacy. Foreign governments have used zero-days to spy on activists, journalists, human rights defenders, and other heads of state.[47] And circumstantial evidence suggests the U.S. government has used zero-days to surveil investigative journalists as well.

internet. *Id.* However, a substantial amount of Microsoft customers hadn't installed these updates. *Id.* at 337. Thus, EternalBlue is an important example to include here: it gives some sense of the number of entities that could be affected by a zero-day exploit and the kind of destruction a genuine zero-day could cause.

[35] PERLROTH, *supra* note 2, at 331–32.

[36] *Id.* at 333–34, 340.

[37] *See supra* text accompanying notes 4–5.

[38] PERLROTH*, supra* note 2, at 334–36.

[39] *Id.* at 341.

[40] *Id.* at 339.

[41] *Id.* at 340.

[42] *Id.*

[43] *Id.*

[44] GREENBERG, *supra* note 11, at 190–95.

[45] PERLROTH, *supra* note 2, at 340.

[46] *Id.* at 341.

[47] Olivia Solon, *'I Will Not Be Silenced': Women Targeted in Hack-and-leak Attacks Speak out About Spyware*, NBC NEWS (Aug. 1, 2021), https://www.nbcnews.com/tech/social-media/i-will-not-be-

a. Foreign Governments' Zero-Day Surveillance

A 2021 investigation uncovered 50,000 phone numbers targeted by zero-day spyware known as Pegasus.[48] Someone who infects a phone with Pegasus can "turn it into a 24-hour surveillance device"[49]: Pegasus can be used to surreptitiously turn on a phone's camera or microphone or record messages, texts, emails, or calls the phone makes.[50] Pegasus can infect a phone without the phone's owner clicking on a link or attachment.[51] And, once installed, Pegasus "leaves no traces whatsoever" indicating to a victim that their phone has been hacked.[52]

Most Pegasus users in the 2021 investigation were authoritarian regimes using the spyware to surveil members of civil society.[53] Victims included a high-profile female journalist in the Middle East and a female Saudi activist.[54] Private photos of both, stored only on their respective phones, were published on Twitter.[55]

Pegasus also factored into the Saudi Arabian government's murder of dissident and Washington Post journalist Jamal Khashoggi.[56] Before killing Khashoggi, the Saudi government appears to have attempted to surveil him by targeting his wife's phone with Pegasus.[57] And after Khashoggi's murder,

silenced-women-targeted-hack-leak-attacks-n1275540 [https://perma.cc/B7UG-YPUW]; *Pegasus Project: Macron Among World Leaders Selected as Potential Targets of NSO Spyware*, AMNESTY INT'L (July 20, 2021), https://www.amnesty.org/en/latest/press-release/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware/ [https://perma.cc/R3Z6-CY6Z].

[48] *Massive Data Leak Reveals Israeli NSO Group's Spyware Used to Target Activists, Journalists, and Political Leaders Globally*, AMNESTY INT'L (JULY 19, 2021), https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/ [https://perma.cc/QQ6R-33ZZ].

[49] David Pegg & Sam Cutler, *What is Pegasus Spyware and How Does It Hack Phones?*, THE GUARDIAN (July 18, 2021), https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones [https://perma.cc/ARH4-29AK].

[50] Nicole Perlroth, *Apple Issues Emergency Security Updates to Close a Spyware Flaw*, N.Y. TIMES (Sept. 13, 2021), https://www.nytimes.com/2021/09/13/technology/apple-software-update-spyware-nso-group.html [https://perma.cc/V8Y4-KAMK].

[51] *Id.*

[52] *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, AMNESTY INT'L (July 18, 2021), https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ [https://perma.cc/C7T5-9UQA].

[53] *See* Ronen Bergman & Patrick Kingsley, *Israeli Spyware Maker Is in Spotlight Amid Reports of Wide Abuses*, N.Y. TIMES (Nov. 8, 2021), https://www.nytimes.com/2021/07/18/world/middleeast/israel-nso-pegasus-spyware.html [https://perma.cc/7NRF-UVPU].

[54] Solon, *supra* note 48.

[55] *Id.*

[56] *See The Report on Jamal Khashoggi's Killing*, N.Y. TIMES (Feb. 26, 2021), https://www.nytimes.com/interactive/2021/02/26/us/report-jamal-khashoggi-killing.html [https://perma.cc/YA7Q-HCM8].

[57] Stephanie Kirchgaessner, *Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests*, THE GUARDIAN (July 18, 2021), https://www.theguardian.com/world/2021/jul/18/nso-

Saudi Arabia targeted both Khashoggi's associates and officials conducting the murder investigation and prosecution with Pegasus.[58]

b. The U.S. Government and Zero-Day Surveillance

Circumstantial evidence suggests the U.S. government has used zero-days to surveil journalists. Barton Gellman is one of the reporters with whom Edward Snowden shared classified NSA documents.[59] While analyzing the Snowden documents, Gellman read his name in a top-secret memo for the Attorney General about "unauthorized disclosures . . . of high-level concern to U.S. policy makers."[60] This prompted Gellman to file a Freedom of Information Act request with several agencies in the U.S. Intelligence Community.[61] When these agencies failed to fulfill Gellman's request, Gellman filed a lawsuit to enforce it.[62]

An FBI affidavit filed in the ensuing court proceedings suggests it used zero-days to surveil Gellman. According to the affidavit, the FBI couldn't fulfill Gellman's request because it would expose "'non-public investigative techniques' and 'non-public details about techniques and procedures that are otherwise known to the public.'"[63] This affidavit also stated one intelligence gathering method's use was "not a publicly known fact," and the FBI wanted to "protect the nature of the information gleaned by its use."[64] A zero-day is necessarily "non-public," and its use is necessarily "not a publicly known fact."[65] Further, a plausible reading of "non-public details about techniques and procedures that are otherwise known to the public" is that the executive branch used zero-days to record audio Gellman's phone captured. Recording and wiretapping are established surveillance techniques and procedures.[66] Using zero-days to record or wiretap would be a "non-public detail" about how the executive branch conducts this surveillance.[67]

spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus [https://perma.cc/AS9U-PDHU].

[58] *Id.*

[59] BARTON GELLMAN, DARK MIRROR 22–29 (2020).

[60] GELLMAN, *supra* note 60, at 221–22.

[61] *Id.* at 276.

[62] *Id.*

[63] *Id.* at 278.

[64] *Id.*

[65] PERLROTH, *supra* note 2, at 7.

[66] *See, e.g.*, United States v. Isa, 923 F.2d 1300 (8th Cir. 1991) (recording); Olmstead v. United States, 277 U.S. 438 (1967) (wiretapping).

[67] An advanced actor also probably used a zero-day to hack Gellman's iPad. *See* GELLMAN, *supra* note 60, at 229–31. Because Gellman was a target of intelligence agencies across the world, *id.* at 241-42, I can't say with confidence that the U.S. likely hacked Gellman's iPad using a zero-day. But the iPad hack might further the circumstantial evidence that the U.S. uses zero-days to surveil journalists.

Further, recent reporting reveals the intelligence community has expressed interest in obtaining just such capabilities. In 2019, the FBI purchased and tested the aforementioned Pegasus spyware.[68] While the FBI ultimately decided against deploying it,[69] the U.S. government's interest in hacking tools like Pegasus is high: NSO even developed spyware substantially similar to Pegasus so U.S. government agencies could surveil Americans.[70]

II. THE UNITED STATES GOVERNMENT AND ZERO-DAYS

A. How the U.S. Government Comes into Possession of Zero-Days

The U.S. government, through the executive branch, comes into possession of zero-days by either finding or buying them.[71] The NSA has an elite unit known as Tailored Access Operations ("TAO").[72] TAO's raison d'être is "find[ing] every crack in every layer of the digital universe and plant[ing] [itself] there for as long as possible."[73] Finding zero-days is part of this mission.[74] The U.S. also buys zero-days from "private malware vendors."[75] For instance, Edward Snowden's disclosures revealed that the NSA had a $25.1 million budget for purchasing zero-days in 2013.[76]

[68] Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. TIMES (Jan. 31, 2022), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [https://perma.cc/Y3QE-5SWB].

[69] *Id.*

[70] *Id. See also* Joseph Cox, *NSO Group Pitched Phone Hacking Tech to American Police*, VICE (May 12, 2020), https://www.vice.com/en/article/8899nz/nso-group-pitched-phone-hacking-tech-american-police [https://perma.cc/PWA6-6LUF].

NSO has claimed that Pegasus doesn't work on smartphones with U.S. phone numbers. Craig Timberg et al., *Key Question for Americans Overseas: Can Their Phones Be Hacked?*, WASH. POST (July 19, 2021), https://www.washingtonpost.com/national-security/2021/07/19/us-phone-numbers-nso/ [https://perma.cc/EV5D-GYRP]. This is disputed. *See* Edward Snowden (@Snowden), TWITTER, (July 20, 2021, 11:53 AM), https://twitter.com/Snowden/status/1417528060245647372 [https://perma.cc/35WE-SVVB] ("NSO's claim that it is 'technologically impossible' to spy on American phone numbers is a bald-faced lie: a exploit that works against Macron's iPhone will work the same on Biden's iPhone. Any code written to prohibit targeting a country can also be unwritten. It's a fig leaf."). *See also* Edward Snowden (@Snowden), TWITTER, (July 20, 2021, 12:15 PM), https://twitter.com/Snowden/status/1417533627722829828 [https://perma.cc/G3ZM-7Q4U] (explaining how Pegasus spyware can be reverse engineered to target American phone numbers).

[71] PERLROTH, *supra* note 2, at 9, 137.

[72] *See generally id.* at 106–13.

[73] *Id.* at 106.

[74] *See id.* at 9.

[75] *Id.* at 137.

[76] *Id.* at 9, 137.

B. Executive Branch Management of Zero-Days

Executive branch officials decide whether to disclose zero-days to vendors through a process known as the Vulnerabilities Equities Process ("VEP").[77] For this Comment, there are two important takeaways about the VEP. *First*, executive branch officials unilaterally decide whether to disclose zero-days to vendors: no other branch of the federal government participates in this process.[78] *Second*, 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 . . . so that it can be used for national security and law enforcement purposes, [like] intelligence collection, military operations, and/or counterintelligence."[79]

III. ZERO-DAYS AND THE COMMANDER-IN-CHIEF AUTHORITY

A. The Constitution

We turn now to the constitutionality of the executive branch's unilateral withholding of zero-days to conduct offensive cyber operations and national security surveillance. The executive branch's authority must come from the text of either the Constitution or a congressional statute.[80] Neither grant the executive branch the authority in question here.

Start with the Constitution's text. It offers little guidance on the issue of withholding zero-days. Article II, Section 2 states only that the President is the "Commander in Chief of the Army and Navy of the United States."[81]

[77] *See* THE WHITE HOUSE, VULNERABILITIES EQUITIES POLICY AND PROCESS FOR THE UNITED STATES GOVERNMENT (Nov. 15, 2017), https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [https://perma.cc/9J74-JBCM]. *See also* Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, THE WHITE HOUSE BLOG (Apr. 28, 2014, 3:00 PM), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities [https://perma.cc/56VA-W63W].

[78] *See* THE WHITE HOUSE, *supra* note 78, at 3–4.

[79] *Id.* at 1.

[80] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585 (1952).

Some early Supreme Court cases suggested that the President has implied or emergency powers under the Constitution. *See* Cunningham v. Neagle, 135 U.S. 1, 82 (1890) (holding that presidential powers "may be found not only in the express authorities conferred by the constitution, but also in necessary and proper implications"); *In re* Debs, 158 U.S. 564 (1895), *disapproved of by* Bloom v. State of Ill., 391 U.S. 194 (1968) (suggesting in dicta that the President has broad executive power to act in the public interest); United States v. Midwest Oil Co., 236 U.S. 459 (1915) (holding the President, acting in the public interest, could withdraw land without statutory authorization when Congress did not challenge the President's actions). But *Youngstown* squarely rejects both these bases for presidential power. 343 U.S. at 585.

[81] U.S. CONST. art. II, § 2.

Consider the most expansive readings of the commander-in-chief clause, two Office of Legal Counsel ("OLC") opinions issued soon after the 9/11 attacks.[82] They prove inapposite. The two OLC opinions in question embraced broad conceptions of the President's ability to use force unilaterally.[83] But using force differs meaningfully from withholding zero-days[84]: one (using force) arguably protects Americans, while the other (withholding zero-days) necessarily leaves Americans more vulnerable. And while one might argue the executive branch's withholding zero-days ultimately protects Americans from—for example—foreign hackers, such reasoning would stretch the commander-in-chief power so far as to be unlimited.[85] Turn to the Supreme Court. Its precedent interpreting the commander-in-chief clause points in favor of requiring the executive branch disclose zero-days. First, in *Youngstown Sheet & Tube Co. v. Sawyer*, the majority opinion held the commander-in-chief authority is limited to the "theater of war."[86] This limit counsels against interpreting Article II authority to conduct unilateral military activities or operations in cyberspace expansively, to include withholding zero-days.[87]

Second, in both *Youngstown* and *The Keith Case*, the Court has made clear that the extent of the President's commander-in-chief authority is lower inside the U.S. than outside its borders. The *Youngstown* majority opinion limits the President's commander-in-chief authority to the "theater of war."[88]

[82] *See* BOB BAUER & JACK GOLDSMITH, AFTER TRUMP 299 (2020) (describing these opinions as taking "historically, and in [the authors'] view, excessively broad views of the president's authority to use force in anticipatory self-defense" and recommending these opinions be abrogated).

[83] *See* The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them, 25 Op. O.L.C. 188, 214 (2001) (concluding that the President has "plenary constitutional power" to use force "to retaliate for [the 9/11] attacks, and to prevent and deter future assaults on the Nation" against parties that either participated in the attacks or "pose a similar threat to the security of the United States and the lives of its people, whether at home or overseas") (internal citations omitted); Authority of the President Under Domestic and International Law to Use Military Force Against Iraq, 26 Op. O.L.C. 143, 152 (2002) (reasoning that, if the President "conclude[d] that Iraq's development of WMD might endanger [U.S.] national security because of the risk that such weapons either would be targeted against the United States, or would be used to destabilize the region," the President had the "independent constitutional authority" to use military force to destroy Iraq's WMD capability).

[84] This, of course, supposes these OLC opinions accurately interpret the law (which I don't grant).

[85] *See* Jack L. Goldsmith, *What Happened to the Rule of Law?*, N.Y. TIMES (Aug. 31, 2013), https://www.nytimes.com/2013/08/31/opinion/what-happened-to-the-rule-of-law.html [https://perma.cc/SRP7-8AFS] (contending that interests that are always present "place[] no limit at all on the president's ability to use significant military force unilaterally.").

[86] *Youngstown*, 343 U.S. at 586. *But see* 10 U.S.C. § 394 (stating the Secretary of Defense "shall develop, prepare, and coordinate; make ready all armed forces for purposes of; and, when appropriately authorized to do so, conduct, military cyber activities or operations in cyberspace" including conduct "short of hostilities" or in "areas in which hostilities are not occurring.").

[87] *See supra* note 86 and accompanying text.

[88] *See supra* note 87 and accompanying text.

Justice Jackson, in his *Youngstown* concurrence, similarly limited the scope of the President's commander-in-chief power inside the United States.[89] Thus, the President's Article II authority doesn't prohibit their engaging in unilateral military action within the U.S.—outside an uprising. Likewise, in *Keith*, the Court held that, while purely foreign surveillance doesn't require a warrant, the executive branch must obtain a warrant when to conduct domestic security surveillance of a U.S. citizen inside the United States.[90] Whatever the President's commander-in-chief authority might allow outside the U.S. with regard to unilaterally withholding zero-days, *Youngstown* and *Keith* stand for the proposition that this authority is sharply limited, if not barred, when it comes to zero-days in products made by American vendors and used by Americans.[91]

And third, under *Youngstown* and *Keith*, the President's commander-in-chief authority must, at the very least, be balanced against Americans' constitutional rights. *Keith* required a check on executive branch domestic security surveillance to protect Americans' Fourth Amendment rights.[92] Zero-days clearly also implicate Fourth Amendment rights.[93]

Youngstown implicated Americans' property rights: the steel industry was preparing to strike and President Truman seized the mills to keep producing for the U.S. military, then fighting the Korean War.[94] Presently, it's unclear what factual circumstances would make it such that withholding a zero-day for cyberwar implicated Americans' property rights. But it's also far too early to rule out this possibility.

B. Statutes

So, the Constitution's commander-in-chief clause doesn't authorize the executive branch's to unilaterally withhold zero-days. What about statutes? Congress has only directly addressed the executive branch's withholding of zero-days in legislation once, in the 2020 defense funding act.[95] There, Congress mandated the Director of National Intelligence make limited and classified annual disclosures concerning zero-days and the VEP basis.[96] These required disclosures are:

[89] *Youngstown*, 343 U.S. at 645–46 (Jackson, J., concurring).

[90] United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div. (*Keith*), 407 U.S. 297, 314–21 (1972).

[91] Hereafter, I use the phrase "American zero-days" to refer to zero-days in products made by American vendors and used by Americans.

[92] *Keith*, 407 U.S. at 316–18.

[93] *See supra* Section I.B.2.b.

[94] *Youngstown*, 343 U.S. at 582–83.

[95] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1632, 133 Stat. 1198, 2230-31 (2020).

[96] *See id.* at 2231; THE WHITE HOUSE, *supra* note 78.

- the number of vulnerabilities submitted for review under the VEP,
- the number of these vulnerabilities disclosed to vendors responsible for the vulnerability or to the public, and
- the aggregate number of vulnerabilities excluded from VEP review.[97]

Congress didn't authorize the executive branch to unilaterally withhold zero-days by requiring these disclosures. Under *United States v. Curtiss-Wright Exp. Corp.*, an otherwise unconstitutional delegation of congressional power to the executive branch can be constitutional when its purpose is to provide relief in a foreign conflict.[98] But the 2020 defense funding act doesn't even meet this low threshold. Delegating to the executive branch the authority to withhold zero-days can't advance relief because the executive branch uses zero-days to advance the opposite.[99] And its use of withheld zero-days isn't limited to conducting foreign cyber operations or surveillance.[100]

But, even if the 2020 defense funding act authorized the executive branch's unilateral withholding of zero-days under *Curtiss-Wright*, *Curtiss-Wright* asks the wrong question. To delegate congressional power, Congress should have to make a political commitment. Here, I draw on Professor Martin Redish's "pragmatic formalism" model for analyzing separation of powers and nondelegation issues.[101]

For Congress to delegate powers to another branch, Professor Redish's pragmatic formalism would require Congress make a political commitment, constituting a policy decision, that the executive branch must then execute.[102] Requiring this policy decision would prevent Congress from delegating freestanding legislative power, which would violate the nondelegation

[97] National Defense Authorization Act for Fiscal Year 2020, § 1632.

One might also read the 2019 funding act as authorizing the executive branch to withhold zero-days in some circumstances: it authorizes the Secretary of Defense to "take appropriate and proportional action in *foreign cyberspace* to disrupt, defeat, and deter" specific adversaries' cyberattack campaigns against the United States. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, § 1632, 132 Stat. 1636, 2123-24 (2018) (emphasis added). But, since this provision concerns foreign cyberspace, legal analysis for withholding zero-days under such circumstances exceeds this Comment's scope.

[98] United States v. Curtiss-Wright Expo. Corp., 299 U.S. 304, 329 (1936).

[99] *See supra* Section I.

[100] *See supra* pages 4–5, 10–11.

[101] *See* Martin H. Redish & Elizabeth J. Cisar, *"If Angels Were to Govern": The Need for Pragmatic Formalism in Separation of Powers Theory*, 41 DUKE L.J. 449 (1991); Martin H. Redish, *Pragmatic Formalism, Separation of Powers, and the Need to Revisit the Nondelegation Doctrine*, 51 LOY. U. CHI. L.J. 363, 398–402, 408–11 (2019).

[102] Redish, *supra* note 103, at 399–400, 408.

doctrine.[103] Further, requiring a political commitment would allow voters to evaluate their elected officials through their votes on bills proposing delegation.[104]

I would apply Professor Redish's pragmatic formalism model to the cyberwar context by requiring Congress make a political commitment authorizing a weapons capability or surveillance practice for the executive branch's use of the capability or practice to be constitutional. In this context, pragmatic formalism would only require Congress make a political commitment that the President has the power to use a certain weapon or surveillance method. Once Congress has made this political commitment, the President could constitutionally decide whether to use this weapon or method in a specific instance.[105]

Applying pragmatic formalism to weapons capabilities and surveillance practices would simultaneously strengthen separation of powers while preserving the President's ability to advance national security. The President may rightfully decide to use a weapon or surveillance method to advance national security in a particular instance. Indeed, the executive branch's very function is to allow the government to respond swiftly and decisively to urgent threats.[106] But deciding to use a weapon or surveillance method in a particular instance differs from deciding to use it generally: the distinction is one between executive and legislative action. Deciding to use a weapon or surveillance method in a particular instance fits comfortably within our understanding of "executive."[107] Unilaterally authorizing the general use of a weapon or surveillance method, however, transforms executing discretion into granting discretion and is thus unconstitutional.[108]

Were Professor Redish's pragmatic formalism applied, the executive branch couldn't unilaterally withhold, for weapons or surveillance, zero-days in products made by American vendors and used by Americans.[109] The executive branch unilaterally withholds these American zero-days for

[103] *Id.*

[104] *Id.*

[105] My model wouldn't require Congress approve tests of weapons capabilities or surveillance practices.

[106] *See* Redish, *supra* note 103, at 397–98, 408–09.

[107] *See* Redish & Cisar, *supra* note 103, at 452–55, 474–78.

[108] *See id.*

[109] My argument is limited to American zero-days because a broader argument would implicate issues that exceed this Comment's scope. For example, courts have held the President has very broad authority to advance U.S. national security interests outside U.S. borders. *See supra* Section III.B.1. Further, the executive branch may, in certain circumstances, engage in warrantless surveillance of non-U.S. persons inside the United States. *See, e.g.*, Glob. Relief Found., Inc. v. O'Neill, 207 F. Supp. 2d 779, 789–90 (N.D. Ill. 2002), *aff'd*, 315 F.3d 748 (7th Cir. 2002).

cyberweapons and surveillance.[110] Were pragmatic formalism applied, it would allow this withholding only if Congress has made a political commitment authorizing it.[111]

The 2020 defense funding act[112] doesn't constitute such a political commitment. At the minimum, a political commitment authorizing the executive branch to unilaterally withhold zero-days would require Congress determine the national security benefits of withholding zero-days could outweigh the costs.[113] The 2020 defense funding act doesn't make this minimum policy decision.

To allow the executive branch to withhold American zero-days, Congress would need to meet a higher standard. For these, Congress would need to decide—in addition to the minimum policy decision—that the national security benefits of withholding American zero-days could outweigh the costs to Americans. This added requirement would allow voters to judge their elected officials' weighing of national security, safeguarding America's critical infrastructure, and Americans' privacy.[114]

IV. CONCLUSION

Zero-days are extremely powerful hardware and software vulnerabilities.[115] They can allow for cyberattacks with substantial real-world consequences and Orwellian surveillance.[116] Currently, the executive branch, when it comes into possession of a zero-day, unilaterally decides whether to withhold or disclose it.[117] Neither the Constitution nor federal statutes permit this unilateral withholding.[118]

But the current analysis for determining Congress's ability to statutorily delegate congressional power falls short by failing to require Congress's political commitment. The threat posed by zero-days presents an opportunity to change this. Requiring Congress's political commitment to the executive branch's withholding zero-days would advance separation of powers while preserving the President's ability to advance national security.[119]

[110] *See supra* Section II.B.

[111] *See supra* text accompanying notes 98–105.

[112] *See supra* notes 97–99 and accompanying text.

[113] *See supra* notes 103–04 and accompanying text.

[114] *See supra* note 105 and accompanying text.

[115] *See supra* Section I.

[116] *See id.*

[117] *See supra* Section II.

[118] *See supra* Section III.

[119] *See supra* Sections III.B.3, III.C.