REGULATING THE ZERO-DAY VULNERABILITY TRADE: A PRELIMINARY ANALYSIS

MAILYN FIDLER*

I. INTRODUCTION

In April 2014, computer security experts revealed "Heartbleed," a vulnerability in software encrypting information transmitted over the Internet.[1] The bug existed in OpenSSL, which up to two-thirds of websites use to encrypt Internet traffic.[2] Heartbleed exposed large swaths of data to interception and exploitation. Initially, news stories speculated the U.S. government knew about Heartbleed, and, rather than disclosing it, had been using it or keeping it for intelligence or other purposes, leaving Internet users at risk.[3]

Although the Heartbleed speculation seems to have been unfounded, public concerns about Heartbleed, combined with distrust created by Edward Snowden's disclosures about the National Security Agency (NSA), forced the U.S. government to detail[4] how it deals with software vulnerabilities it knows about but that remain unknown to software vendors or users – "zero-day" vulnerabilities or "zero-days."[5] The Obama administration's response to Heartbleed raised further questions about U.S. policy on zero-day vulnerabilities, including the U.S. government's role in purchasing vulnerabilities from the zero-day market.

---

* Marshall Scholar, Department of Politics and International Relations, University of Oxford. I would like to thank the following people for their advice, input, and support during my work on this research: Lily Ablon, Richard Bejtlich, Fred Cate, Scott Charney, Jack Goldsmith, Jennifer Granick, Herb Lin, Jonathan Mayer, Chris Soghoian, Michael Sulmeyer, and Peter Swire.

[1] Nicole Perlroth, *Experts Find a Door Ajar in an Internet Security Method Thought Safe,* N.Y. TIMES (Apr. 8, 2014), http://bits.blogs.nytimes.com/2014/04/08/flaw-found-in-key-method-for-protecting-data-on-the-internet/.

[2] *Id.; The Heartbleed Bug,* CODENOMICON (April 2014), http://heartbleed.com/.

[3] Michael Riley, *NSA Said to Exploit Heartbleed Bug for Intelligence for Years,* BLOOMBERG (Apr. 11, 2014), http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html.

[4] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities,* WHITE HOUSE BLOG (Apr. 28, 2014), http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[5] See Part II.A *infra* for a detailed description of zero-days.

The legal and illicit trade in zero-days is lucrative and global. The U.S. government is a buyer, with the NSA devoting $25.1 million to "covert purchases of software vulnerabilities" from private vendors during fiscal year 2013, corresponding to an estimated minimum of 100 to 625 vulnerabilities annually.[6] Israel, Britain, Russia, India, Brazil, Malaysia, Singapore, North Korea, and Iran purchase zero-days.[7] Countries can use zero-day vulnerabilities for law enforcement investigations, improving cyber defenses, conducting cyber espionage, and conducting offensive military cyber operations.

The U.S. government's participation in this market raises concerns because keeping zero-days secret to preserve military, intelligence, or law enforcement capabilities can negatively affect U.S. and global cybersecurity. In purchasing vulnerabilities to use or stockpile rather than disclose, governments prioritize national security, law enforcement, and intelligence objectives over general Internet security. The U.S. government denied prior knowledge of Heartbleed, but the policy issued in response to this vulnerability did not rule out that, had the government known about Heartbleed, it would have kept this bug secret and exploited it.[8] This possibility worries those concerned with this policy's effect on U.S. national security, Internet security, and the future of cyberspace. Stockpiling and not disclosing vulnerabilities could leave global computer users, companies, and other countries at risk. The global nature of the zero-day market also means this trade could enable unfriendly governments, non-state actors, and criminals to gain capabilities damaging to U.S. interests and abuse human rights and civil liberties.[9]

The negative security implications, lucrative nature, and global scope of the zero-day vulnerability trade have sparked debate about whether to regulate it. Some civil liberties advocates have

---

[6] Stefan Frei, *The Known Unknowns: Empirical Analysis of Publicly Known Security Vulnerabilities,* NSS LABS (Dec. 2013), https://www.nsslabs.com/reports/known-unknowns-0, at 15; Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show,* WASH. POST (Sept. 3, 2013), http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

[7] Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code,* N.Y. TIMES (July 13, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

[8] Riley, *supra* note 3.

[9] Eric Rosenbach, Keynote Address at the Armed Forces Communications and Electronics Cyber Con 2013 (Mar. 18, 2013), http://www.c-span.org/video/?c4390789/keynote-address-eric-rosenbach, at 3:24.

suggested regulation,[10] and parts of the government have called for greater analysis.[11] However, many zero-day sellers oppose regulation.[12] The debate exhibits disagreements about whether a problem exists, let alone how to address it. Further, as discussed below, despite the market's global reach, no international institution seems prepared to address this issue.

The debate's divisiveness indicates that serious policy questions exist about the zero-day trade and its implications for U.S. national security, cybersecurity, and international relations more broadly. Recognizing that the debate has reached no consensus, this article analyzes potential domestic and international strategies for regulating the zero-day trade, exploring their substantive content, feasibility, and possible consequences. Regulation need not necessarily mean banning sale and/or use of zero-days. The strategies range across the spectrum of regulatory approaches, including consideration of how existing laws already have regulatory effects on the zero-day trade. A number of the strategies examined connect to established governance frameworks used with other dual-use technologies. In examining potential strategies, this article scrutinizes how well each option addresses the security problems associated with the zero-day trade and its feasibility, given the foreseeable course of national and international politics.

First, the article examines the scale and security implications of the zero-day trade. Little academic work has been completed on the zero-day issue, so I conducted on-and off-the-record interviews with government, academic, civil society, and private sector experts to obtain perspectives on this issue. Next, the article investigates domestic regulatory approaches, including criminalization, export controls, and increased oversight of U.S. government actions. It concludes that increased executive branch oversight is the best domestic strategy. The article then analyzes international strategies:

---

[10] Electronic Frontier Found. v. Nat'l Sec. Agency, Office of the Dir. of Nat'l Intelligence, No. 3:14-cv-03010 (N. D. Cal. 2014); *Expert Warns of the Growing Trade in Software Security Exploits*, HARVARD LAW TODAY (Oct. 30, 2012), http://today.law.harvard.edu/expert-warns-of-the-growing-trade-in-software-security-exploits/?redirect=1.
[11] National Defense Authorization Act for Fiscal Year 2014, Pub. L. No. 113-66, § 924; Rosenbach, *supra* note 9.
[12] *See, e.g.*, Andy Greenberg, *Shopping for Zero-Days: A Price List for Hacker's Secret Software Exploits,* FORBES (Mar. 23, 2012), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ ("That'll work just as well at eliminating exploits as the war on drugs has worked at eliminating drugs.").

international legal approaches, voluntary collective action through coordinated export controls, and cooperation through collective defense organizations. It concludes that voluntary collective action to harmonize export controls on zero-days through the Wassenaar Arrangement is the most feasible international option.

II. WHAT IS THE ZERO-DAY PROBLEM?

A. *Zero-Day Vulnerabilities*

A zero-day vulnerability is a previously unknown flaw in a computer program that exposes the program to external manipulation. Zero-day vulnerabilities have been found in many programs, including Microsoft, Internet Explorer, Adobe, and Apple products.[13] Zero-day vulnerabilities also appear in software running critical infrastructure, such as power plants. What differentiates a zero-day from other computer vulnerabilities, and what makes it valuable, is that it is unknown to the software's makers and users. Whoever has knowledge of a zero-day can exploit it from the "zero-th" day of its discovery, until the software maker or users learn of it and fix the vulnerability.

What makes a zero-day vulnerability different from other cyber tools is that it is simply information. A zero-day encapsulates the knowledge that X could happen if you do Y. As Auriemma and Ferrante of ReVuln, a zero-day seller, argue, "we don't sell weapons, we sell information."[14] Other companies, however, do sell weaponized vulnerabilities – zero-day "exploits" – that contain new software code taking advantage of a zero-day vulnerability. Desautels, of vulnerability-seller Netragard, states Netragard sells exploits.[15] Zero-day exploits range in complexity and functionality, from enabling access to, monitoring, extracting information from, or damaging a software program. For instance, the Stuxnet

[13] Frei, *supra* note 6, at 10.
[14] Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, REUTERS (May 10, 2013), http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510.
[15] *The Digital Arms Trade*, ECONOMIST, Mar. 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade.

program allegedly used by the United States to damage uranium-enrichment Iranian centrifuges made use of four zero-day vulnerabilities.[16]

In this article, the term zero-day "vulnerability" describes the software flaw itself. When a zero-day vulnerability is sold, knowledge of the flaw is sold. The press often uses the term zero-day "exploit" interchangeably to describe knowledge of a flaw or new software code exploiting a flaw. In this article, the term "exploit" refers only to new code written to take advantage of a zero-day vulnerability. Although turning a vulnerability into an exploit can be relatively easy, motivations for finding and exploiting vulnerabilities often differ. For instance, cybersecurity researchers have less motivation to turn vulnerabilities into exploits than someone selling or buying zero-days. This distinction between a zero-day vulnerability and exploit, and the different groups interacting with them, is important to make when analyzing regulatory options for the zero-day vulnerability trade.[17]

Vulnerabilities are most exploitable if kept secret. Zero-days are discovered and not made, so there is no guarantee someone in possession of a vulnerability is the only person who knows about it. The value of secrecy complicates efforts to control the zero-day trade because it contributes to market opacity and lack of transparency about buyer and seller behavior.

B. *Overview of Vulnerability Markets*

Zero-days are traded in three markets. As defined in this article, the "white market" encompasses sales of vulnerabilities between zero-day vulnerability hunters and software vendors or third-party clearinghouses. The "black market" describes interactions where the buyer or the seller has criminal intent. The "gray market" involves interactions between vulnerability sellers and government agencies,

---

[16] David Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran,* N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. The Symantec report details three zero-days in Stuxnet, while news reports have indicated four were used.

[17] The press does not always distinguish between zero-day vulnerabilities and exploits. After assessing context for each use, I refer to all zero-days as vulnerabilities – knowledge of a software flaw – rather than exploits, unless I could verify otherwise. This assumption may introduce error: prices, actors, and policy recommendations may vary between vulnerabilities and exploits. Where possible, I point out how dealing with a vulnerability or exploit may differ.

conducted as legal business deals. It also encompasses sales between vulnerability sellers and legal users of zero-day vulnerabilities, including high-end cybersecurity firms. This article distinguishes between "legal" and "legitimate" zero-day vulnerability markets. White-market and gray-market transactions are legal, and black market transactions illegal. The negative security ramifications of the gray market mean this article designates only white-market options legitimate.

Gray-market firms, rather than freelance hackers, now sell more than half of zero-day vulnerabilities.[18] NSS Labs included many of the firms I identify in Table 1 in its market analysis, and concluded that "half a dozen boutique exploit providers have the capacity to offer more than 100 exploits per year, resulting in 85 privately known exploits being available on any given day," at minimum.[19] One seller identified the decreased risk of getting ripped off, the possibility of job offers, and stable contracts with government or industry clients as reasons vulnerability hunters choose to operate on the gray market.[20] The scale and function of each market is discussed in detail later in the paper.

C. *Security Implications of the Global Gray-Market Trade in Zero-Day Vulnerabilities*

The gray market for zero-days causes concern beyond its size and global reach. The gray market also raises national and international security worries. The zero-day issue, particularly U.S. government participation in the trade and its policies towards disclosure, is an instance where national security and broader cybersecurity needs may conflict. According to the Obama administration, if the U.S. government discovers a zero-day vulnerability, it has a "bias" towards disclosure.[21] What "bias" means is unclear. U.S. policy makes exceptions to this bias, providing opportunities for the government to keep vulnerabilities without notifying software vendors.[22] Keeping vulnerabilities secret means other governments or cyber criminals may independently discover and use the vulnerability to the detriment of

[18] *Digital Arms Trade, supra* note 15.
[19] Frei, *supra* note 6, at 2.
[20] Lily Ablon, Martin Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, RAND CORPORATION (March 2014), http://www.rand.org/pubs/research_reports/RR610.html, at 25.
[21] Daniel, *supra* note 5.
[22] For full details, see discussion of the Michael Daniel blog post in part III.D.2.E *infra*.

general cybersecurity.[23] These concerns were evident with Heartbleed: computer users would have been at risk if the U.S. government had known about the vulnerability and chosen to keep it secret for exploitation. U.S. non-disclosure of zero-days also leaves global users at risk, because undisclosed vulnerabilities affect anyone using globally disseminated software.

Government participation helps catalyze gray-market expansion, which has potentially harmful ramifications. Vulnerability sellers may offer information to multiple sources. The U.S. government's willingness to purchase vulnerabilities has spurred growth of vulnerability-selling firms, encouraging gray-market expansion and increasing availability and mobility of gray-market products, which actors unfriendly to the U.S. may be able to access. Soghoian, a cybersecurity expert at the American Civil Liberties Union (ACLU), states that, "as soon as one of these weaponized zero-days sold to governments is obtained by a 'bad guy' and used to attack U.S. infrastructure" bad things will happen; gray-market sellers "will drag the entire security industry into a world of pain."[24]

Even without duplicitous vulnerability sellers, the very nature of zero-days means they could independently find their way into the hands of both the U.S. government and bad actors. Howard Schmidt, former White House cybersecurity coordinator, explained that, "it's pretty naïve to believe that with a newly discovered zero-day, you are the only one ... that's discovered it."[25]

Government participation in the gray market could affect the black market. U.S. involvement in the gray market "bankroll[s] dangerous R&D" and "build[s] the black market," a U.S. military-intelligence official stated.[26] Michael Hayden, former Central Intelligence Agency (CIA) and NSA Director, argues that tax dollars used to purchase vulnerabilities on the gray market may benefit the black market – for instance, if spent with a company that also supplies bad actors.[27] Or, a buyer participates in

[23] Menn, *supra* note 14; *In Cyberwar, Software Flaws Are a Hot Commodity*, NPR (FEB. 12, 2013), http://www.npr.org/2013/02/12/171737191/in-cyberwar-software-flaws-are-a-hot-commodity.
[24] Greenberg, *supra* note 12.
[25] Menn, *supra* note 14.
[26] *Digital Arms Trade*, *supra* note 15.
[27] Menn, *supra* note 14.

the gray market using a front company, but is actually a criminal organization. This crossover effect exists in the traditional arms trade, where legitimate arms transfers end up with renegade groups.[28]

A robust gray market expands access to advanced cyber tools to states that would otherwise not be able to independently develop them. Before the gray market, the ability to discover zero-days in-house was largely a boutique capability, the privilege of a few capable governments or those with access to skilled hackers.[29] Colonel John Adams, head of the Marine Corps' Intelligence Integration Division, states that gray-market sellers "provide cyber-power to hostile governments that would otherwise lack the expertise to attack an advanced country's computer systems."[30]

Easier access to zero-days by non-state actors is also a security concern. Eric Rosenbach, Deputy Assistant Secretary of Defense for Cyber Policy, said that the prospect of non-state actors accessing zero-days on the market "keeps me awake at night."[31] In acquiring zero-days, the United States may inadvertently enable a market that also allows less cyber-capable nations and non-state actors unfriendly to U.S. interests to improve their cyber capabilities.

Concerns that zero-days can contribute to human rights abuses have also emerged. As established, the gray market may enable bad actors, including oppressive governments, to acquire cyber capabilities they can use to violate human rights. For instance, since September 2013, a vulnerability in Adobe Flash, publicly disclosed in April 2014, was used to target Syrians who visited a government "complaints" website.[32] This bug appears to have been professionally planned and executed.[33] This situation demonstrates that concerns about connections between human rights abuses and zero-days are

---

[28] Nicholas Marsh, *Two Sides of the Same Coin? The Legal and Illegal Trade in Small Arms*, 4 J. WORLD AFF. 217 (2002).
[29] Morgan Marquis-Boire, *For Their Eyes Only: The Commercialization of Digital Spying*, Citizen Lab (May 1, 2013), https://citizenlab.org/2013/04/for-their-eyes-only-2/, at 2.
[30] *Digital Arms Trade, supra* note 15.
[31] Rosenbach, *supra* note 9.
[32] Dennis Fisher, *Flash Zero-Day Used to Target Victims in Syria*, THREATPOST – KASPERSKY LABS (April 28, 2014), http://threatpost.com/flash-zero-day-used-to-target-victims-in-syria.
[33] Recent security analyses have tied this April 2014 vulnerability to a wider surveillance operation also targeting other countries, likely originating from a Francophone country; some have implicated France. This finding complicates linking the incident directly to the Syrian government. Still, *someone* was conducting surveillance of Syrian "complainers" using a zero-day vulnerability. See Franceschi-Biccherai, Lorenzo, *Meet Casper: Yet Another Malware Likely Created by France for Surveillance.* MOTHERBOARD *(Mar. 5, 2015),* http://motherboard.vice.com/read/meet-casper-yet-another-malware-likely-created-by-france-for-surveillance.

real. European Union politician Marietje Schaake has advocated regulating trade in such cyber technologies that could be used to abuse human rights.[34]

D. *Detailed Look at Vulnerability Markets*

1. *White-Market Programs*

In early bug-hunting days, hackers who discovered bugs could either alert the vendor in return for recognition and free company gear or turn to the black market. White-market purchasing programs emerged as a third option in the mid-2000s, when companies and independent organizations began offering bounties for bugs. For example, in 2005, a group of "white hat" hackers started the TippingPoint Zero Day Initiative (ZDI). This initiative compensated researchers for reporting bugs to ZDI. ZDI would then notify affected vendors. The typical ZDI award was $1,000-5,000, with most below $2,000. Another similar initiative was the VeriSign iDefense Vulnerability Contributor Program (VCP), started in 2002.[35] The VCP also compensates researchers for reporting vulnerabilities and then coordinates with vendors to patch them. A new player is HackerOne, which operates as a middleman between software companies and flaw-finders, orchestrating paid deals.[36]

Even though compensation by vulnerability purchasing programs is lower than black market prices, these programs constitute a substantial source of bug reports. One study reports 14 percent of all Microsoft, 10 percent of Apple, and 17 percent of Adobe vulnerabilities in the past decade came through white-market programs.[37] Many software companies also offer their own bug bounties, including:

---

[34] Ryan Gallagher, *The Secretive Hacker Market for Software Flaws,* SLATE MAG. (Jan. 16, 2013), http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html.

[35] *Defense Vulnerability Contributor Program,* VERISIGN IDEFENSE VENDOR-COORDINATED PUBLIC VULNERABILITY REPORTS (2013), http://www.verisigninc.com/en_GB/cyber-security/security-intelligence/vulnerability-reports/index.xhtml.

[36] Joseph Menn, *HackerOne Gets $9 Million in Funding to Reward Spotters of Software Flaws,* REUTERS (May 28, 2014), http://www.reuters.com/article/2014/05/28/cybersecurity-bounties-idUSL1N0OE2CI20140528?irpc=932.

[37] Frei, *supra* note 6, at 10.

- Facebook, offering rewards from $500 up, spending $1 million in the first two years of the program; [38]
- Google, offering $100 to $20,000 in rewards, with most rewards around $1000; [39]
- Microsoft, which has a newly expanded bounty up to $150,000 for certain bugs, potentially in response to gray-market pricing; [40] and
- Mozilla, averaging about $3000 per bug.[41]

Google, frustrated by reliance on insecure code from other companies, has launched Project Zero, its own in-house team of vulnerability hunters searching for bugs in Google and other software.[42] No money appears to be exchanged through Project Zero, but Google gives other companies 60 to 90 days before publicly releasing details of discovered vulnerabilities.

2. *Black-Market Programs*

The black market is a long-standing option for profiting from zero-day vulnerabilities. In the black market, zero-days and other tools are available for purchase on widely accessible sites and restricted-access marketplaces.[43] Sellers include freelance hackers and organizations.[44] Black-market buyers include individual criminals and criminal organizations.[45] Some governments may turn to the black market if legitimate sellers refuse to service them.

---

[38] *Facebook.com/whitehat*, FACEBOOK (2013), https://www.facebook.com/whitehat; *An Update on Our Bug Bounty Program*, FACEBOOK (Aug. 2, 2013), https://www.facebook.com/notes/facebook-security/an-update-on-our-bug-bounty-program/10151508163265766.
[39] *Vulnerability Reward Program*, GOOGLE (2013), https://www.google.com/about/appsecurity/reward-program/.
[40] *Microsoft Bounty Programs*, MICROSOFT SEC. TECH CTR. (June 26, 2013), http://technet.microsoft.com/en-us/security/dn425036.
[41] Frei, *supra* note 6, at 13.
[42] Andy Greenberg, *Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers*, WIRED (June 15, 2014), http://www.wired.com/2014/07/google-project-zero/.
[43] Ablon, Libicki, and Golay, *supra* note 20, at 8; Charles Miller, *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*, WORKSHOP ON THE ECON. OF INFO. SEC. (2007), http://weis2007.econinfosec.org/papers/29.pdf.
[44] Ablon, Libicki, and Golay, *supra* note 20, at 4.
[45] *Id.* at 5-6.

Black-market trade is largely conducted online, including bulletin-board style forums, email, and chat rooms.[46] Recently, Amazon-type stores have developed, allowing buyers to shop without direct interaction with the vulnerability provider.[47] Radianti identified at least twelve publicly accessible black-market forums.[48] Radianti's interviews with black-market participants reveal that prices are higher on black markets than the white market.[49] One subject described a sale where a bug would go for $2500 on the white but $30,000 on the black market.[50] Other interview subjects described an Adobe Acrobat bug sold for $75,000, a Windows Meta File vulnerability purchased for $4,000, and an Internet Explorer 7 bug acquired for $15,000.[51] Clearly, prices vary according to bug type and potential. Radianti documented at least one case of a seller criticizing a black-market offer by comparing it to a higher white market offer.[52] Radianti concluded that the legitimate market provides bargaining power to black-market sellers.[53] It also demonstrates that black-market sellers are aware of, or operate simultaneously on, illegal and legal markets.

3. *Gray-Market Programs*

The gray market refers to trade between vulnerability sellers and government agencies or other non-criminal clients. Potential buyers of gray-market zero days include private-sector clients, brokers who resell vulnerabilities, and governments.[54] Private-sector clients typically include high-end penetration testing firms, but this customer base is considered much smaller than the government base.[55]

---

[46] *Id.* at 7.
[47] *Id.* at 7.
[48] Jaziar Radianti, Eliot Rich, & Jose Gonzalez, *Vulnerability Black Markets: Empirical Evidence and Scenario Simulation,* 42ND HAWAII INT'L CONFERENCE ON SYS. SCI. (2009).
[49] Jaziar Radianti, *Eliciting Information on the Vulnerability Black Market from Interviews,* IEEE FOURTH INT'L CONFERENCE ON EMERGING SEC. INFO., SYS., AND TECH. (2010).
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] Radianti, Rich, & Gonzalez, *supra* note 48.
[54] Ablon, Libicki, & Golay, *supra* note 20, at 25-26.
[55] Telephone Interview with Richard Bejtlich, Chief Security Strategist, FireEye, (May 7, 2014).

Governmental buyers are the most typical final customers for zero-days in the gray market, but zero-days often first pass through brokers.

The U.S. government is a reported buyer of zero-day vulnerabilities. According to the intelligence budget leaked by Snowden, the NSA devoted $25.1 million in fiscal year 2013 to purchase software vulnerabilities from private vendors, despite relying on in-house staff for most vulnerabilities.[56] The NSA is the only publicly identified U.S. government purchaser. *Reuters* reported that the Department of Defense (DoD) and other intelligence agencies participate in the gray market but provided no specifics.[57] In the absence of other information, the following suggestions represent informed guesses about government agency participants. Possible candidates include the Central Intelligence Agency (CIA), based on zero-day usefulness to intelligence and the recent creation of a CIA digital directorate, and non-NSA parts of the DoD, given its intelligence-gathering responsibilities and role in coordinating military cyber operations through U.S. Cyber Command (CYBERCOM).[58] The Federal Bureau of Investigations (FBI) and Department of Homeland Security (DHS) are also possible purchasers, given their roles in law enforcement, intelligence gathering, and cybersecurity policy. The FBI appears to stockpile and use zero-day vulnerabilities, but no information currently establishes the FBI as a buyer.[59]

Private-sector companies purchasing vulnerabilities on the gray market fall into two categories: companies reselling vulnerabilities, usually to governments, and companies using vulnerabilities for purposes such as cyber defense research or penetration testing.[60] Contractors such as Northrop Grumman, Lockheed Martin, Harris Corporation, and Raytheon are likely buyers/resellers.[61] These contractors may also have their own vulnerability discovery teams selling directly to the government.

---

[56] Gellman & Nakashima, *supra* note 6.
[57] Menn, *supra* note 14.
[58] DAVID SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 200-01 (2012).
[59] Michael Riley & Chris Strohm, *FBI Keeps Internet Flaws Secret to Defend Against Hackers*, BLOOMBERG (Apr. 29, 2014), http://www.bloomberg.com/news/2014-04-30/fbi-keeps-internet-flaws-secret-to-defend-against-hackers.html.
[60] Ablon, Libicki, & Golay, *supra* note 20, at 25.
[61] Thomas Brewster, *Words of War and Weakness: The Zero-Day Exploit Market*, TECHWEEKEUROPE (Sept. 10, 2012), http://www.techweekeurope.co.uk/news/zero-day-exploit-vulnerabilties-cyber-war-91964.

Miller predicted commercial cyber tool suppliers, large penetration testing and consulting firms, intrusion detection companies, and security subscription services also buy vulnerabilities on the gray market.[62] Besides actions like penetration testing, the legality of industry use of vulnerabilities is contested, and some vulnerability sellers refuse to offer their most sensitive products to the private sector.

Brokers source vulnerabilities from vulnerability finders and offer them to potential customers for a 10-15 percent cut of the final sale.[63] For example, Miller agreed to give a broker 10 percent in return for access to multiple potential government clients and subsequently received offers of $10,000 and $80,000.[64]

In addition, the gray market is global, with the governments of Israel, Britain, Russia, India, and Brazil identified as purchasers.[65] North Korea and Middle Eastern intelligence services are on the market, including Malaysia, Singapore, and the Revolutionary Guards of Iran.[66] Most well-financed intelligence agencies probably purchase vulnerabilities.[67]

Excluding contractors and brokers, this research identified ten independent gray market zero-day vulnerability sellers, listed in Table 1 below, along with their known business practices. This table only includes entities whose participation could be verified using at least two sources: two news articles or a news article and the company's website. This table is not exhaustive or definitive. It represents companies willing to speak to the press or otherwise indicate their activities and which operate primarily in English. Errata Security took issue with sources indicating it is a seller.[68] However, the company has not publicly denied participation, so until public sources indicate otherwise, Errata will remain listed in Table 1.

---

[62] Miller, *supra* note 43.
[63] Perlroth & Sanger, *supra* note 7; Brewster, *supra* note 61.
[64] Miller, *supra* note 43.
[65] Perlroth & Sanger, *supra* note 7.
[66] *Id*.
[67] *Digital Arms Trade*, *supra* note 15.
[68] Robert Graham, *0day Market Conspiracy Theories*, ERRATA SECURITY (JUN. 25, 2014), http://blog.erratasec.com/2014/06/0day-market-conspiracy-theories.html.

Table 1: Zero-Day Sellers

Entity	Location	Self-Imposed Selling Restrictions	Pricing	Notes	Broker
Headquarters Outside United States					
VUPEN[69]	-Montpelier, France - Fort Meade, MD	- Does not sell to countries under European Union, United States or United Nations restrictions. - Only sells to government clients.	- $100,000 subscription fee - Per flaw charge - 1.2 million revenue in 2011	- Confirmed contract for some form of vulnerability service with United States Government. -86% of sales outside France.	Maybe
ReVuln[70]	Malta			- Vulnerabilities not disclosed to companies. - Offers SCADA vulnerabilities.	Maybe
Arc4dia[71]	Quebec	- Sells to "national governments, foreign intelligence services, and other lawful agencies." - Only sells to government agencies.			
Headquarters Inside United States					

[69] Perlroth & Sanger, *supra* note 7; Brian Fung, *The NSA Hacks Other Countries By Buying Millions of Dollars' Worth of Computer Vulnerabilities,* WASH. POST (Aug. 31, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/; *NSA-Vupen Contract,* NAT'L SEC. AGENCY, Sept. 9, 2013; Gallagher, *supra note 34*.
[70] Perlroth & Sanger, *supra* note 7; *ReVuln,* REVULN (2013), http://revuln.com/.
[71] *Digital Arms Trade, supra* note 15; *Arc4dia*, ARC4DIA (2013), http://arc4dia.com/company.html.

Exodus Intelligence [72]	Austin, TX	All vulnerabilities are responsibly reported to companies.	-Top 4 contributors receive $20,000 bonus - In its first six weeks, it purchased 12 vulnerabilities (20% of submissions)	-Sells a feed of information relating to vulnerabilities. - Network of 150 contributing researchers.	Yes
Endgame[73]	Arlington, VA	In March 2014, Endgame announced it would no longer sell exploits, but would continue selling vulnerabilities to governments.	- $100,000 - 200,000 for best products - Package of 25 zero-days for 2.5 million	- Links to In-Q-Tel. - Former NSA director as investor. - Recently raised $23 million in second-round funding.	Maybe
Netragard[74]	Acton, MA	- Strictly U.S.-based customers. - Screening procedures for contractors.	- $16,000-250,000 - 50 zero-days sold in 2012	Contracts with 3-dozen independent suppliers.	Yes
Errata Security[75]	Atlanta, GA				
Government Contractors[76]	U.S. based		$100,000 and up based on review of an anonymous product catalogue		Likely

[72] Perlroth & Sanger, *supra* note 7; *EIP August Incentives*, EXODUS INTELLIGENCE (Aug. 7, 2012), http://blog.exodusintel.com/page/2; Brewster, *supra* note 61.
[73] Andy Greenberg, *A Second Act for the Blackwater of Hacking*, FORBES (Mar. 3, 2014), http://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/; Perlroth & Sanger, *supra* note 7; Menn, *supra* note 14; *Digital Arms Trade*, *supra* note 15; Gallagher, *supra* note 69; *Endgame*, ENDGAME (2013), https://www.endgame.com/.
[74] Perlroth & Sanger, *supra* note 7; *Digital Arms Trade*, *supra* note 15; Greenberg, *supra* note 12; Gallagher, *supra* note 69.
[75] *Errata Security*, ERRATA SECURITY (2013), http://www.erratasec.com/; Brewster, *supra* note 61.
[76] Menn, *supra* note 14; Brewster, *supra* note 61.

Individual Sellers					
The Grugq[77]	Bangkok, native of South Africa	Only sells to American and European agencies for moral and profit reasons.	- 1 bug for $250,000 - $1 million projected revenue for 2012	80% of revenue from the United States.	Yes
Charlie Miller[78]	U.S. based		$50,000	Currently inactive.	
Cesar Cerrudo[79]	Argentina/ Seattle, WA	Selectively decided which requests to supply.		Currently inactive.	

[77] Perlroth & Sanger, *supra* note 7,Greenberg, *supra* note 12; Marcia Hoffman & Trevor Timm, *Zero-Day Exploit Sales Should Be Key Point in Cybersecurity Debate*, ELECTRONIC FRONTIER FOUNDATION (Mar. 29, 2012), https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate.

[78] Perlroth & Sanger, *supra* note 7; Miller, *supra* note 43.

[79] Menn, *supra* note 14; Robert Lemos, *Bug Brokers Offering Higher Bounties*, SECURITYFOCUS (Jan. 23, 2007), http://www.securityfocus.com/news/11437/3.

Estimating zero-day market volume with so little data is difficult. Figures for total U.S. government spending on zero-day vulnerabilities are not available. The NSA, presumably the largest purchaser of vulnerabilities, budgeted at least $25.1 million, as noted above.[80] Other agencies may spend more, less, or nothing.

Despite lack of data, rough estimates provide some insight; the following estimates represent original calculations. Yearly estimates of revenue or sales volume were available only for some sellers. The Grugq projected $1 million in revenue for 2012, with 80 percent from the United States,[81] which would indicate a maximum of $800,000 U.S. revenue. VUPEN reported $1.2 million revenue in 2011, with 86 percent outside France.[82] VUPEN's maximum U.S. revenue would be about $1 million. Netragard reports yearly sales of 50 bugs[83] from $16,000[84] to $250,000.[85] Netragard's lowest possible maximum U.S. revenue from zero-days would be $800,000, assuming all bugs are sold in the United States for $16,000. Assuming Netragard sells two zero-days yearly for its top price, its largest estimated maximum U.S. revenue would be $1.3 million. Exodus Intelligence reported purchasing 12 bugs in its first 6 weeks.[86] Assuming this trend continues, Exodus would purchase roughly 100 bugs annually. Given no public price information for Exodus, assume Exodus purchases bugs at the lowest price listed by Forbes, $5,000, and sells them for $10,000 each.[87] Exodus would earn $500,000. For a higher estimate, assume Exodus sells each bug for the lowest listed price in Table 1, $16,000, generating revenue of $1.1 million.

[80] Gellman & Nakashima, *supra* note 6.
[81] Greenberg, *supra* note 12.
[82] Gallagher, *supra* note 69.
[83] *Digital Arms Trade*, *supra* note 15.
[84] Gallagher, *supra* note 69.
[85] *Digital Arms Trade*, *supra* note 15.
[86] *EIP August Incentives*, *supra* note 72.
[87] Greenberg, *supra* note 12.

Table 2: Estimated Maximum Yearly U.S. Revenue from Vulnerability Sales (2012-13)

Seller	**Revenue**
The Grugq	$800,000
VUPEN	$1,000,000
Netragard	$800,000-$1,300,000
Exodus Intelligence	$500,000-$1,100,000

If all active sellers described in Table 1 performed similarly, total U.S. revenues of the identified firms combined could be about $10 million at the high end. The Grugq, responding to these estimates, states that he sized the market at less than $5 million but calls my figures for the companies in Table 2 "probably about right."[88] However, a considerable gap exists between known government purchasing figures, the revenues of known companies, and the market estimates completed by the Grugq and myself. This gap suggests several possibilities:

- The U.S. government allocates more funds for purchases than it spends;
- More companies exist than are publicly known, operating in relative secrecy; and
- The figures above do not consider government contractor revenue; contractors may be highly active sellers.

The first possibility is unlikely, given market growth in the U.S. and overseas. However, the NSA budget could potentially be used for zero-day vulnerabilities and previously disclosed (one-day, etc.) vulnerabilities, which are generally cheaper and readily available. The second and third explanations probably exist in tandem. Given their existing relationships with the government, contractors probably play a large role in the gray market, and their prices are not reflected in my analysis. Given the relative opacity of the trade, more firms likely exist, operating in secrecy, exacerbating the transparency problems already evident. Overall, despite gaps in data, available information demonstrates the trade is global, lucrative, and opaque.

[88] The Grugq, *Only thing that was interesting was the table showing that the market is <$4m,* TWITTER (June 24, 2014), https://twitter.com/thegrugq/status/481506494416826368.

The zero-day trade lacks transparency on the government and private seller sides – no Freedom of Information Act option exists for companies – and the trade presents security and other policy concerns. Although the trade is lucrative, the zero-day issue is not the highest-grossing or single-most concerning problem in cybersecurity. However, the associated suite of security implications means the unregulated zero-day trade represents a troubling practice. Given these concerns, national and international strategies for controlling the trade should be explored, drawing where possible on past approaches to regulating dual-use technologies. The next two parts of this article undertake this analysis.

III. Domestic Strategies for Regulating the Zero-Day Trade

A. *Introduction*

Three strategies for domestic regulation of zero-day vulnerabilities deserve particular attention – criminalization, export controls, and increased oversight of U.S. government involvement in the zero-day trade. These case studies are useful for three reasons. First, these approaches are different in nature, ranging from stringent criminalization to flexible oversight, providing a diversity of approaches. Second, these strategies have been used in analogous contexts and with dual-use technologies, which permits those experiences to inform thinking about zero-day trade regulation. Finally, each strategy is being considered, to some degree, by policymakers as determined by a review of relevant literature, policy discussions in civil society, and interviews conducted with policy-community members.

B. *Criminalization*

1. *Criminal Law and Zero-Days*

The United States and other countries use criminal law to deter and punish certain activities undertaken through cyber technologies, such as gaining unauthorized access to computers. Applied to zero-days, governments could criminalize sale and/or purchase of zero-day vulnerabilities as a regulatory strategy. For example, in 2007, Germany criminalized the distribution of hacking tools, such as Trojan

Horses or software that extracts data from a hacked computer.[89] Germany adopted this law to implement Article 6 of the Council of Europe's Convention on Cybercrime. [90] The law's adoption raised the question of whether it extended to zero-day vulnerabilities.

The German cybersecurity community objected because the law might apply to their research with, among other things, zero-days. In one of few academic pieces in English on the subject, Dennis Jlussi, then a candidate for a master's in law at Leibniz Universität Hannover, observed that the German adaptation of the Convention on Cybercrime did not incorporate the exception for security researchers the Convention includes.[91] Although I have found no record of prosecutions based on this German law, at least two security researchers who disclosed or planned to disclose vulnerabilities were threatened with legal action grounded in it, demonstrating the possibility of this legal approach affecting security research, potentially including research involving zero-days.[92]

In the United States, the Computer Fraud and Abuse Act (CFAA) criminalizes certain activities on or by a computer. Congress enacted CFAA in 1986 in response to growing concern about cybercrime.[93] As discussed below, the U.S. government has used the CFAA to prosecute a black market zero-day exploit dealer, and academic proposals advocate amending the statute to cover trade in zero-days specifically.[94] Broadly, the CFAA criminalizes committing, conspiring, and attempting to commit seven

---

[89] § 203 BGB.

[90] Dennis Jlussi, *Handle With Care, But Don't Panic: Criminalisation of Hacker Tools in German Criminal Law and its Effect on IT Security Professionals*, EUROPEAN EXPERT GRP. FOR IT SEC. (Nov. 2007), http://www.jlussi.eu/wp-content/uploads/2007/11/jlussi-202c-short.pdf; *Convention on Cybercrime: What Do you Want to Know About This Treaty?*, COUNCIL OF EUROPE (n.d.), http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185.

[91] Jlussi, *supra* note 90; Convention on Cybercrime, Nov. 23, 2001, art 6. sec. 2. CETS No. 85, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[92] *See* Kelly Jackson Higgins, *Another Research Hit with Threat of German Anti-Hacking Law*, DARKREADING (Apr. 27, 2011), http://www.darkreading.com/vulnerabilities---threats/another-researcher-hit-with-threat-of-german-anti-hacking-law-/d/d-id/1135605?; Kelly Jackson Higgins, *Researcher Overcomes Legal Setback over 'Cloud Cracking Suite,'* DARKREADING (Mar. 21, 2011), http://www.darkreading.com/risk/researcher-overcomes-legal-setback-over-cloud-cracking-suite/d/d-id/1135443?.

[93] Office of Legal Education, *Prosecuting Computer Crimes*, DEP'T. OF JUSTICE, http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf, at 1.

[94] *See* Michele Golabek-Goldman, *A New Strategy for Reducing the Threat of Dangerous Zero-Day Sales to Global Security and the Economy: A Policy Analysis Exercise*, HARVARD KENNEDY SCHOOL OF GOV'T, Mar. 25, 2014; Paul Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. & POL'Y REV. 101 (2013).

types of cyber crime (Table 3). The CFAA has been criticized for its "breadth and severity."[95] The law has increasingly been used to prosecute offenses such as violating website terms of service or employer computer policies, not classical hacking.[96]

Table 3: CFAA Basics

The CFAA criminalizes the following offenses completed or attempted through or on a "protected computer:"
• Obtaining national security information, or other protected information. • Trespassing on a government computer. • Accessing a computer to defraud and obtain anything of value. • Intentionally damaging by knowingly transmitting a program or similar code. • Recklessly and negligently causing damage by intentional access. • Trafficking in passwords. • Extorting through computers.[97]

2. *The CFAA's Current Applicability to Zero-Day Exploits, Vulnerabilities*

The U.S. government has applied the CFAA to black-market sales of zero-day exploits.[98] Another case attempted to apply the CFAA to disclosure of zero-day vulnerabilities, but was dismissed.[99] As far as is publicly known, gray-market sellers of zero-day exploits and vulnerabilities have not been targets of CFAA-related investigations. One explanation for this difference is that the CFAA excludes authorized activities of intelligence and law enforcement agencies.[100] The language only excuses the government party, not the seller. However, as Jonathan Mayer, noted CFAA expert, observes, "the government is not going to charge the people who help them."[101] This government agency carve-out is potentially why

[95] Tim Wu, *Fixing the Worst Law in Technology,* NEW YORKER (Mar. 18, 2013), http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.
[96] Wu, *supra* note 95; U. S. of America v. David Nosal, 676 F.3d 854 (9th Cir. 2012).
[97] 18 U.S.C. § 1030.
[98] I thank Jonathan Mayer for the suggestion to examine the Ulbricht case; U. S. v. Ross William Ulbricht (S.D.N.Y. 2014),http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR/US%20v.%20Ross%20Ulbricht%20Indictment.pdf; U. S. v. Liberty Reserve, (S.D.N.Y. 2013), http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf.
[99] *MBTA v. Anderson,* ELECTRONIC FRONTIER FOUND. (Aug. 2008), https://www.eff.org/cases/mbta-v-anderson.
[100] 18 U.S.C.§1030(f).
[101] Skype interview with Jonathan Mayer, Stanford University PhD Candidate (Mar. 18, 2014).

some gray-market sellers restrict sales of zero-day exploits and other offense-oriented tools to government clients. Thus, the CFAA, even in its current form, may incentivize selling certain hacking tools to the government, taking advantage of a "safe harbor" from potential CFAA prosecutions.

3. *Proposal to Amend the CFAA to Address Sale of Certain Zero-Day Vulnerabilities*

A proposal from Paul Stockton, former Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (2009-13), and Michele Golabek-Goldman, a 2014 Yale Law School graduate, advocated amending the CFAA to apply explicitly to aspects of the zero-day trade.[102] The authors argue that Congress should amend the CFAA "to govern dangerous 0-day exploit transactions."[103] They use the term "exploits" but characterize exploits as merely information. As explained above, exploits are more than mere information; they are new code exploiting underlying flaws. Stockton and Golabek-Goldman use the term exploits to refer to vulnerabilities, and "weaponized exploits" to refer to what this document calls exploits.[104] Their proposal has three key elements: they focus on restricting critical-infrastructure (CI) zero-day vulnerabilities, introducing a due diligence requirement for sellers of such vulnerabilities, and the extraterritorial application of this due diligence requirement.

Stockton and Golabek-Goldman suggest amending the CFAA to place an "affirmative duty on the *seller* to conduct due diligence when selling 0-day exploits that can be deployed to gain unauthorized access to critical-infrastructure."[105] The authors dismiss concerns that their proposal would "contribute to what [is] perceive[d] as the CFAA's already 'dangerously broad criminalization of online activity and abuse of prosecutorial discretion.'"[106] The authors suggest their proposal avoids this flaw by being "narrowly circumscribed so that only sellers of the most dangerous exploits that target critical infrastructure would be required to perform due diligence."[107]

---

[102] Stockton & Golabek-Goldman, *supra* note 94.
[103] *Id.* at 123.
[104] *See id.* at 102 ("A zero-day ... and their components").
[105] *Id*. at 124. (emphasis added).
[106] *Id*.
[107] *Id*.

Stockton and Golabek-Goldman turn to the CFAA because they find its extraterritorial reach useful in targeting the zero-day vulnerability trade outside the United States. They argue that "a large number of dangerous 0-day exploit sales originate abroad and are therefore beyond the reach of American export laws … the United States must therefore have the capacity to prosecute researchers located abroad who sell exploits to U.S. adversaries."[108] The authors advocate updating the CFAA to target foreign sellers serving foreign buyers, foreign sellers serving U.S. buyers, and U.S. sellers serving all buyers.

This proposal would expand the CFAA to zero-day vulnerability sales related to CI and enable extraterritorial prosecution of sellers who fail to conduct due diligence about customers. Stockton and Golabek-Goldman attempt to affect the international zero-day market without requiring international cooperation. The U.S. government has used the CFAA to prosecute cyber actors located outside the United States who affected U.S. interests,[109] but identifying and prosecuting such actors is difficult.

Still, the CFAA is not the appropriate approach to the zero-day problem. Mayer acknowledges that hooking the zero-day trade issue to the CFAA is a convenient way to achieve extraterritoriality. However, Mayer questions the fit: "It's not clear to me why this needs to be under CFAA except for drafting convenience."[110] Problems also exist with applying their proposal for due diligence extraterritoriality: it represents an expansion of the CFAA that would enable the United States to target foreign sellers doing business with foreign buyers, an expansion that would anger other states and create severe practical difficulties, such as the refusal of foreign governments to engage in law enforcement cooperation.

Stockton and Golabek-Goldman's proposal also raises multiple definitional problems that undermine its value. They call for only "the most dangerous exploits that target critical infrastructure" to be included in an amended CFAA.[111] Defining what threshold zero-days must cross to be considered most dangerous would prove difficult. Indeed, in a later proposal (discussed below), Golabek-Goldman rejects

---

[108] *Id*. at 123.
[109] *See, e.g., Russian Man Sentenced for Hacking Into Computers in United States*, U.S. DEP'T. OF JUSTICE (Jul. 25, 2003), http://www.justice.gov/criminal/cybercrime/press-releases/2003/ivanovSent.htm.
[110] Mayer, *supra* note 101.
[111] Stockton & Golabek-Goldman, *supra* note 94, at 124.

a CI approach because "software deployed by critical infrastructure sectors is used elsewhere," making it "challenging to determine whether a buyer aimed to deploy the purchased zero-day to target critical infrastructure."[112] Last, although Stockton and Golabek-Goldman present CI as a narrowing feature of their proposal, the U.S. government defines CI expansively; Presidential Policy Directive 21 identified 16 CI sectors.[113] These definitional issues demonstrate that this proposal is not sufficiently clear and could be interpreted broadly. If such a proposal were implemented without clarification, it could be considered too vague to be fair, raising Fifth Amendment due process concerns; aspects of the CFAA have already been challenged on these grounds.[114]

Further, Stockton and Golabek-Goldman suggest amending the CFAA to penalize sellers, not buyers or users. Sellers would be required to conduct due diligence to ensure clients have no intentions of harming U.S. CI. If sellers fail to do so, it would face criminal penalties. This type of liability is somewhat akin to negligent entrustment, which recognizes tort liability if someone gives another person a dangerous tool (e.g., lending a car to a drunk).[115] In its current form, the CFAA could be used to prosecute someone for accomplice liability or conspiracy to commit a CFAA violation (see Ulbricht prosecution above). Seller-based liability would introduce a new kind of criminal liability to the CFAA, "a weird species of secondary liability," Mayer argues.[116] "You would be an accomplice" to a CFAA violation "by merely failing to do due diligence. I'm not aware of anything else that follows that kind of model, as opposed to getting someone because they handed a dangerous product to someone else without adequately checking them."[117] Thus, contrary to the authors' intent to amend the CFAA narrowly, their proposal would broaden the already broad CFAA in controversial ways.

---

[112] Golabek-Goldman, *supra* note 94.
[113] *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, WHITE HOUSE OFFICE OF THE PRESS SEC'Y (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[114] Orrin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1562 (2010).
[115] Mayer, *supra* note 101.
[116] *Id.*
[117] *Id.*

In light of definitional uncertainty, the expansive nature of the amendment, controversy over a new type of liability, and the criminal nature of the penalties, both zero-day sellers and current CFAA opponents would likely resist including zero-day vulnerabilities sales in the CFAA. Given these problems, amending the CFAA as Stockton and Golabek-Goldman recommend is not a good strategy.

4. *Golabek-Goldman's Proposal: Updating the CFAA without Extending Extraterritoriality*

After publication of her article with Stockton, Golabek-Goldman released a second paper on regulation of the zero-day trade in which she still proposes updating the CFAA to "impose an affirmative duty on zero-day sellers to 'know their customers' or only sell to particular [approved] entities."[118] However, Golabek-Goldman does not limit the proposal to CI and argues Congress should specify that this addition to the CFAA "would not apply extraterritorially" to foreign sellers.[119]

Golabek-Goldman's rejection of extraterritoriality requires explanation, given that her proposal with Stockton embraced extraterritoriality as critical to their recommendation. In her proposal, Golabek-Goldman takes the opposite approach, arguing that "extending the CFAA to researchers operating abroad who recklessly sold zero-days to foreign buyers would constitute a vast expansion of extraterritoriality ... [and] could generate backlash, undermining the United States' other efforts to achieve much-needed international cooperation in this field."[120] Although Golabek-Goldman's revised proposal does not apply to foreign sellers serving foreign buyers, whether Golabek-Goldman still intends this amendment to apply to foreign persons selling to U.S. buyers (a different form of extraterritorial application) is not clear. Subjecting U.S. sellers, but not foreign sellers serving U.S. clients, to criminal liability for engaging in the same activity would undermine the usefulness of a criminal law approach to the trade and create a major loophole.

With at least one type of extraterritoriality rejected, Golabek-Goldman focuses on amending the CFAA to impose an affirmative duty on U.S. sellers to conduct due diligence about customers or sell only

[118] Golabek-Goldman, *supra* note 94.
[119] *Id.* at 54.
[120] *Id*.

to pre-approved customers. This proposal means, as discussed above, U.S. sellers would face criminal liability if they violated due diligence requirements. The risks involved with criminal liability, as Golabek-Goldman argues, could drive U.S.-based zero-day sellers to "safe harbor" options, including white-market and gray-market buyers such as the U.S. government or government contractors.

Although her more recent paper addresses shortcomings of her co-authored article, Golabek-Goldman's proposal still raises questions. First, it still advocates adding a "weird species of secondary liability"[121] and does not address problems associated with this idea discussed above. Second, it is not clear whether she rejects all problematic forms of extraterritorial application, or just the foreign seller to foreign buyer case. Other forms of extraterritorial application pose similar problems. Last, that Golabek-Goldman altered critical components of her co-authored article – the CI and extraterritorial elements – quite soon after its publication underscores the complexities, difficulties, and controversies that would accompany using a criminalization strategy to regulate the zero-day trade.

5. *Summary of the Criminalization Strategy*

National criminalization as a strategy to control the zero-day trade faces numerous problems. First, as demonstrated with Germany's anti-hacking law and the dismissed CFAA case, application of criminal statutes to the discovery and disclosure of zero-day vulnerabilities generates serious concerns for security researchers, including potential free speech issues.[122] Microsoft's Scott Charney emphasizes this issue: "A lot of security involves research. Disclosures are First Amendment protected here, and elsewhere, even if they [other countries] don't have the equivalent of the First Amendment, there is a strong commitment to protecting them. It is not healthy to solve the problem by criminalizing the finding or reporting of vulnerabilities."[123]

[121] Mayer, *supra* note 101.
[122] *M.B.T.A. v. Anderson, supra* note 99.
[123] Interview with Scott Charney, Corporate Vice President, Trustworthy Computing Group, Microsoft, in Stanford, Cal. (May 1, 2014).

Second, the CFAA is already contested given how the U.S. government has interpreted and applied it.[124] Using the CFAA as the basis for dealing with the zero-day trade might trigger increased opposition to the CFAA, diluting the potential for the CFAA to become a foundation for dealing with the zero-day trade.

Third, the existing proposals to amend the CFAA to deal with zero-days demonstrate the problems a criminalization strategy faces. Cornerstone elements of Stockton and Golabek-Goldman's proposal – the CI focus and application of the amendment extraterritoriality – are abandoned by Golabek-Goldman in the proposal she independently made soon after her co-authored article appeared. The elements constant across proposals – imposing criminal liability on sellers for failure to conduct due diligence on buyers – could create incentives for sellers to turn to white-market buyers or a limited set of gray-market purchasers, such as the U.S. government. However, the core approach generates so many problems, including threatening security research, the unusual nature of the proposed liability, potential due process problems from defining this liability, and opposition to such liability make criminalization an inappropriate approach.

C. *U.S.-Based Export Controls as a Regulatory Strategy for the Zero-Day Trade*

1. *Introduction to Export Controls*

Export controls have been used to restrict export of software products and information, including those relating to cryptography. Using U.S. cryptography export controls as a case study, this section analyzes such controls as a possible model for regulating the zero-day trade.

The 1970s-1990s application of U.S. export controls to cryptography generated controversy, spawning the so-called "crypto-wars." The U.S. government viewed emergence of commercial cryptography as a threat to its intelligence capabilities and foreign policy interests.[125] The government

[124] Kerr, *supra* note 114.
[125] Jeanne Grimmet, *Encryption Export Controls*, CONGRESSIONAL RESEARCH SERV., Jan. 11, 2001, http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30273_01112001.pdf, at 3.

sought to limit availability of U.S.-originating cryptographic information and products abroad.[126] Opponents argued that export controls harmed U.S. competitiveness, infringed First Amendment rights, and created domestic insecurities because export controls reduced availability of highly secure encryption products domestically.

The "crypto wars" share similarities with the challenge of regulating trade in zero-day vulnerabilities. Both cases exhibit a U.S. government interested in preventing the spread of a strategic dual-use technology abroad. Additionally, U.S. policy in both cases is perceived to generate domestic insecurities. Government purchasing of zero-days pulls business away from the white market, leaving vulnerabilities undisclosed and computer users at risk. With cryptography, export controls weakened available domestic cryptography, because many companies did not make distinct domestic and foreign products for cost reasons.[127] Finally, both situations involve regulation of technology that is less physical than abstract. Cryptography and zero-day vulnerabilities are, at their core, knowledge enabling technical developments. This feature introduces First Amendment concerns into debates about controlling cryptography and zero-day vulnerabilities.

However, cryptography export controls also differ from the zero-day vulnerability challenge. With cryptography, the government played a strong development role, and the United States was the clear technological leader. With zero-days, the government has been less involved and the trade is already global. These differences will affect how well export controls can apply to zero-days.

U.S. export controls on cryptography were introduced through the Arms Export Control Act (AECA), which took its current name and form in 1976 and is administered by the State Department, and the 1979 Export Administration Act (EAA). Initially, nearly all encryption tools were classified under AECA as defense articles or services subject to export controls.[128] AECA provides strong enforcement

[126] WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION, UPDATED AND EXPANDED EDITION 122 (2007).
[127] Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th and 21st Centuries*, SUN MICROSYSTEMS LABORATORIES: THE FIRST TEN YEARS, 1991-2001, OCT. 2001; Grimmet, *supra* note 125, at 3,5.
[128] Grimmet, *supra* note 125, at 3,5.

and criminal and civil penalties and is not subject to judicial review.[129] If an item falls under AECA, the item will typically require an individually approved export license, with a designated customer, application, and conditions for use and resale.[130]

Under the less strict EAA, a seller can obtain a license exporting to a category of customers rather than one specific buyer.[131] Penalties for violation of these Department of Commerce (DoC) administered regulations are generally less severe than AECA penalties.[132] The DoC must also sometimes consider foreign availability of controlled products when setting export restrictions.[133]

2. *Opposition and Changes to Cryptography Export Controls*

Cryptography export controls encountered opposition from the computer industry, which argued that restrictions hindered competitiveness by allowing foreign firms to sell to customers U.S. firms could not.[134] Companies argued that controls slowed technological development and harmed domestic security, because firms resisted developing separate U.S. versions, producing only a less robust, exportable version.[135]

Export controls also encountered First Amendment opposition. Three major court cases dealt with this issue, and each decision hinged on whether the court held encryption code was functional or expressive. The government argued that encryption was functional and required control, while plaintiffs argued that encryption transmits ideas.[136] One court case decided export controls represented unconstitutional prior restraints on speech.[137] A second decision held that export controls on certain

---

[129] *Id.*
[130] Diffie & Landau *supra* note 126, at 121.
[131] *Id.*
[132] Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 HOUS. J. OF INT'L L. 441, 511-12 (2002).
[133] Ian F. Fergusson, *The Export Administration Act: Evolution, Provisions, and Debate,* CONGRESSIONAL RESEARCH SERV., Jul. 15, 2009, http://fas.org/sgp/crs/secrecy/RL31832.pdf, at 8;
Diffie & Landau, *supra* note 126, at 121.
[134] Diffie & Landau, *supra* note 127.
[135] *Id;* Grimmet, *supra* note 125, at 3.
[136] Grimmet, *supra* note 125, at 10.
[137] Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999).

functional information were allowable.[138] A third case held the First Amendment applies to encryption source code.[139] Taken together, this inconsistent case law contributed to the controversy and confusion surrounding encryption export controls.

Industry resistance, judicial rulings, and a changing international political climate resulted in cryptography export control liberalization. Changes in the early 1990s transferred authority over most encryption to the less strict DoC lists.[140] The Clinton administration also retreated from only allowing export of encryption having a U.S. government-accessible key-recovery system.[141] The military began to realize that export controls hampered finding cheap, commercial products meeting military security needs. Because companies often developed only an exportable product, the military had to commission more secure products for its use at high cost.[142] Congressional opposition was also strong, culminating in a 1999 Security and Freedom through Encryption (SAFE) Act, which would have mandated changes to encryption export controls.[143] The bill was on its way to a House vote when the Clinton administration capitulated.[144] The administration announced encryption of any key length could be exported after technical review to most end users, except users in designated state sponsors of terrorism.[145] A post-export reporting requirement would be in effect for keys over 64 bits.[146]

The ECHELON scandal also influenced liberalization.[147] It revealed U.S. intelligence targeted major commercial communication channels, including satellites.[148] To bolster defenses against U.S. intelligence, the EU ended encryption export controls within the EU and for close trading partners.[149] Given Europe's lowered barriers, the Clinton administration removed the requirement for export licenses

[138] Karn v. U.S. Dep't of State, 925 F. Supp. 1 (D.D.C. 1996).
[139] Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).
[140] Grimmet, *supra* note 125, at 6.
[141] *Id*.
[142] Diffie & Landau, *supra* note 126, at 256.
[143] H.R. Res. 850, 106th Cong. (1999).
[144] Diffie & Landau, *supra* note 126, at 256.
[145] Grimmet, *supra* note 125, at 7.
[146] *Id.*
[147] Lawrence D. Sloan, *ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation,* 50 DUKE L. J. 1467 (2001).
[148] Diffie & Landau, *supra* note 126, at 255.
[149] Diffie & Landau, *supra* note 127.

for cryptographic products destined for EU members and additional destinations.[150]

September 11 somewhat slowed liberalization. With new emphasis on homeland security, the DoC export control group was rechristened the more cautious Bureau of Industry and Security.[151] Still, one more significant round of liberalization occurred in 2002. Mass-market encryption products greater than 64 bits could be exported after a 30-day review, the lightest barrier yet.[152]

3. *The Fall of Cryptography Export Controls: Lessons*

When encryption export controls were first instated in the 1970s, the United States had the "economic power to make export control an effective element of foreign policy."[153] As the dominant source for particular products, U.S. export controls could affect global product availability. With globalization, "many more products [are] available from non-U.S. sources," meaning U.S. export controls are less effective.[154] The availability of products means that "the cost to U.S. businesses of export controls" is greater.[155] This situation is particularly true for computer companies, which derive considerable revenue from foreign sales and must manufacture exportable products to be competitive.[156]

The post-Cold War environment contributed to the U.S. government's diminished political power to encourage countries to implement equivalent national export controls. In this environment, "other countries, even close allies, do not always share the U.S. view that a particular country is a strategic threat."[157] Other countries may welcome U.S. export controls as an economic opportunity and move to supply that market. In the post-Cold War era, it also became less clear what specific *global* threat dual-use technologies posed. If no rival superpower was waiting to snatch up encryption, why keep such technologies closely held? A country whose access becomes restricted may view such a policy as overly

---

[150] *Id;* Corr, *supra* note 132, at 489; Grimmet, *supra* note 125, at 8.
[151] Corr, *supra* note 132, at 459; Industry and Security Programs: Change of Agency Name, 81 Fed. Reg. 20,630 (2002).
[152] Corr, *supra* note 132, at 491.
[153] Diffie & Landau, *supra* note 127.
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] Corr, *supra* note 132, at 456.

punitive. Technologically, the rise of the Internet and other forms of digital communication increased demand for cryptographic products and made export controls focusing on physical goods less effective.[158]

Additionally, during the 1990s, the U.S. military sought to maximize its budget by purchasing commercial rather than custom products. Since cryptography export controls restricted the supply of domestically available, rigorous encryption products, the military had to fund development of expensive custom products, which brought them to support loosened export controls.[159]

First Amendment challenges to cryptography export controls played a crucial role in their demise. A growing and vocal community of activists supported these challenges. This community catalyzed by the crypto wars would later go on to fight the Stop Online Piracy Act (SOPA), the PROTECT IP Act (PIPA), and NSA surveillance programs.

4. *Analysis of Export Controls and Zero-Day Vulnerabilities*

Export controls are a supply-side solution. Foreign buyers deal with secondary effects of export controls, such as resale restrictions, but the primary burden falls on sellers. As such, export controls would not address concerns about U.S. government purchasing and use of zero-days. Instead, like criminalization, export controls would address U.S. concerns about U.S.-based sellers supplying foreign buyers.

Export controls limit potential foreign buyers of U.S. products, furthering the U.S. goal of preventing certain countries or groups from accessing zero-day vulnerabilities. Export controls may reduce the volume of foreign trade. Instead of dealing with export regulations, sellers may turn to U.S.-based purchasers, including the U.S. government. This impact would likely positively affect security by keeping more trade within U.S. and, perhaps, slowing the global market. However, many obstacles exist to achieving these benefits.

---

[158] Diffie & Landau, *supra* note 127.
[159] *Id.*

Trade in zero-day vulnerabilities is global. Geopolitical and economic realities mean U.S.-based export controls would not wield the force cryptography export controls did when first instated. Major non-U.S. vendors of zero-day vulnerabilities exist (see Table 1), so restricting export of U.S.-based vulnerabilities would not materially reduce the suite of vulnerabilities buyers could access. Microsoft's Scott Charney highlights this problem, observing "export controls do not work in a globally connected Internet and it is not only one country that can find bugs."[160] Given this global availability, U.S. companies may resist export controls as damaging their global competitiveness.

If the United States enacted unilateral export controls, it could seek to pressure allies to institute parallel national controls, as with encryption controls.[161] The resistance U.S. leadership encountered to spreading key escrow policies abroad, and to unilateral U.S. leadership after the Snowden disclosures, could suggest that it would be difficult for the United States to convince countries enjoying economic advantages from the trade to join a U.S.-led effort to restrict it. To overcome doubts about U.S. leadership and achieve international buy-in, a coordinated export controls approach, such as through the Wassenaar Arrangement, would have to be sought, as discussed below.

Encryption export controls raised the question whether source code constituted protected speech and whether digital and analogue information should be treated differently. Today's zero-day trade takes place in a digital realm facilitated by the Internet. The "functional v. expressive" distinctions courts made between books, physical diskettes, and source code during the crypto wars are not as helpful with zero-days. The zero-day vulnerability trade is based on selling knowledge of flaws in code, not code itself. Such knowledge-based vulnerabilities are not "functional," because they do not involve new code. Under this perspective, export controls on zero-day vulnerabilities may constitute prior restraints on speech in violation of the First Amendment. However, transmission of knowledge about a zero-day may not be fully expressive speech, either, because it transfers information about someone else's code rather than

[160] Charney, *supra* note 123.
[161] Diffie & Landau 2007, *supra* note 126, at 245.

being an expressive act, such as writing code. In sum, First Amendment issues would complicate export controls on zero-day vulnerabilities, but it is not clear which way courts would rule.

Zero-day exploits, new code written to utilize a zero-day vulnerability, could more easily be included under export-control mechanisms, because exploits are more readily definable as functional. However, as newly created code, exploits are also potentially expressive. The existence of zero-day vulnerabilities and exploits in the same market, often sold by the same companies, complicates attempts to navigate First Amendment considerations when regulating this trade.

D. *Oversight Mechanisms*

The third domestic regulatory strategy involves implementing more robust oversight of zero-day vulnerability purchasing and use within the U.S. government. From what is publicly known, much of U.S. government zero-day purchasing and use occurs within the intelligence community, which has a history of both being subject to and frustrating various oversight mechanisms. Additionally, high-profile applications of zero-days, including in Stuxnet, have been considered covert operations,[162] suggesting oversight of such operations may be a useful source of ideas. This section analyzes how existing oversight systems for intelligence and covert activities might inform oversight for the zero-day trade.

1. *Overview of Intelligence and Covert Operations Oversight*

A. *Legislative Oversight*

Congress is a significant source of oversight of intelligence activities and covert operations. The 1947 National Security Act authorizes the CIA to perform functions at the President's direction, which

[162] Max Boot, *Covert Action Makes a Comeback*, WALL ST. J., Jan. 5, 2011, http://online.wsj.com/news/articles/SB10001424052748703909904576051991245498326.

has been interpreted to include covert actions – actions intended to influence political, economic, or military conditions abroad, but where a U.S. role will not be apparent.[163]

Congress strengthened oversight for covert actions by requiring the President to make a written finding on the national security importance of a covert action and providing information on all covert actions to the appropriate intelligence committees.[164] Congress also prohibited use of appropriated funds for covert actions unless there is a written Presidential finding, and appropriated funds may only be used for intelligence activities reported to the committees.[165] Additionally, Congress also required regular reporting of all intelligence actions to the intelligence committees.[166] It has taken recent steps to strengthen internal checks and balances in the intelligence community, including establishing the Office of the Intelligence Community Inspector General (IG) in the Office of Director of National Intelligence (ODNI) in 2010.[167]

In light of the Snowden disclosures, many questioned whether congressional oversight of intelligence community (IC) activities is effective. The House attempted to prohibit the NSA's phone records collection program in July 2013, but the bill was narrowly defeated. [168] The House approved a similar bill in 2014, but the Senate failed to secure enough votes to bring its version to a floor debate, leaving the path to legislative NSA reform highly unlikely. [169] Many proposals have been made to address this sense of failure of congressional oversight of intelligence. For instance, Fred Cate, a privacy and

---

[163] Marshall Curtis Erwin, *Covert Action: Legislative Background and Possible Policy Questions,* CONGRESSIONAL RESEARCH SERV., Apr. 10, 2013, http://fas.org/sgp/crs/intel/RL33715.pdf , at 1.
[164] 50 U.S.C. § 413b.
[165] 50 U.S.C. § 414.
[166] 50 U.S.C. § 413a.
[167] *Office of Intelligence Community Inspector General*, Office of the Director of National Intelligence (2015), http://www.dni.gov/index.php/about/organization/office-of-the-intelligence-community-inspector-general-who-we-are.
[168] Jonathan Weisman, *House Defeats Efforts to Rein in N.S.A. Data Gathering,* N.Y. TIMES (Jul. 24, 2013), http://www.nytimes.com/2013/07/25/us/politics/house-defeats-effort-to-rein-in-nsa-data-gathering.html?pagewanted=all.
[169] Jonathan Weisman & Charlie Savage, *House Passes Restraints on Bulk Data Collection,* N.Y. TIMES (May 22, 2014), http://www.nytimes.com/2014/05/23/us/politics/house-votes-to-limit-nsas-collection-of-phone-data.html; Charlie Savage, *Rival House Bills Aim to Rein in N.S.A. Phone Data Program,* N.Y. TIMES (May 6, 2014), http://www.nytimes.com/2014/05/07/us/politics/rival-house-bills-aim-to-rein-in-nsa-phone-data-programs.html; Ellen Nakashima & Ed O'Keefe, *Senate Fails to Advance Legislation on NSA Reform,* WASH. POST (Nov. 18, 2014), http://www.washingtonpost.com/world/national-security/senate-fails-to-advance-legislation-on-nsa-reform/2014/11/18/a72eb7fc-6f70-11e4-8808-afaa1e3a33ef_story.html.

cybersecurity expert, suggests creating an independent agency separate from both Congress and the executive branch to provide stronger oversight. [170]

B. *Executive Branch Oversight*

Oversight initiated and executed by the executive branch plays a significant role in monitoring intelligence activities and covert action programs. Executive Order 12333, initially signed by President Reagan, gives the Attorney General authority to approve techniques for foreign intelligence gathering.[171] It also authorizes the CIA to conduct covert activities approved by the President.[172]

In 2013, the Obama administration's 2012 Presidential Policy Directive 20 (PPD-20) was leaked. The document established classified policy for U.S. cyber operations. PPD-20 contained "broad and strict" restrictions for cyber operations, including establishing distinctions between defensive and offensive procedures and requiring Presidential consent for certain operations.[173]

An additional component of the system of executive branch oversight is the role of Inspector General in various departments. For instance, in 2010 Congress established the Office of the Intelligence Community Inspector General (IG) in the Office of Director of National Intelligence (ODNI).[174] The ODNI IG is tasked with conducting audits and investigations into intelligence community activities. Similar Inspector General positions perform the same function in parallel agencies across the government.

C. *Judicial Review as Oversight*

Generally, federal courts provide venues for challenges to the legality of U.S. government actions. In the intelligence context, the 1978 Foreign Intelligence Surveillance Act (FISA) instituted a

---

[170] Fred Cate, *Comments Submitted to The President's Review Group on Intelligence and Communications Technology*, CENTER FOR APPLIED CYBERSECURITY RESEARCH, Sept. 9, 2013, at 4.
[171] Edward C. Liu, *Reauthorization of the FISA Amendments Act*, CONGRESSIONAL RESEARCH SERV., APR. 8, 2013, http://fas.org/sgp/crs/intel/R42725.pdf, at 3.
[172] Executive Order 12333: United States Intelligence Activities, 46 Fed. Reg. 59,941 (1981).
[173] Ellen Nakashima, *Obama Signs Secret Directive to Help Thwart Cyberattacks*, (Nov. 14, 2012), WASH. POST http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.
[174] *Office of Intelligence Community Inspector General*, *supra* note 167.

legal regime for governing foreign intelligence conducted within the United States, including roles for the judiciary. FISA established the Foreign Intelligence Surveillance Court (FISC) to oversee U.S. government surveillance to collect foreign intelligence information in the United States.[175] Specifically, the court has jurisdiction to grant approvals for electronic surveillance, physical searches, pen register/tap and trace surveillance, and orders compelling the production of tangible things.[176]

Broadly, FISA allows surveillance against a person within the United States to be approved based on probable cause that the target is a foreign power or agent of a foreign power.[177] The FISC is composed of seven federal district court judges appointed by the Supreme Court Chief Justice, and it hears arguments only from the Department of Justice.[178] FISA also plays a role in foreign intelligence operations targeting non-U.S. persons outside the United States, such as the PRISM program disclosed by Snowden, in which the NSA gained broad access to Internet communications stored or transmitted within the United States of non-U.S. persons believed to be located abroad.[179]

2. *U.S. Government Zero-Day Policy and Practice*

A. *Pre-2014*

As the introduction noted, the U.S. government released details in 2014 about its policy regarding use and disclosure of zero-day vulnerabilities. Before analyzing these changes, what is known about pre-2014 activities deserves examination. The NSA, and likely other agencies, purchased zero-day vulnerabilities. As discussed, the NSA allocated $25.1 million to purchasing vulnerabilities during fiscal year 2013, correlating with about 100 to 625 vulnerabilities minimum per year.[180] Reports indicated that

---

[175] *Foreign Intelligence Surveillance Act,* ELECTRONIC PRIVACY INFO. CENTER (2013), http://epic.org/privacy/terrorism/fisa/.
[176] Andrew Nolan & Richard Thompson III, *Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes,* CONGRESSIONAL RESEARCH SERV., Jan. 16, 2014, http://fas.org/sgp/crs/intel/R43362.pdf, at 18.
[177] *Foreign Intelligence Surveillance Act*, *supra* note 175.
[178] *Id.*
[179] Timothy Lee, *Here's Everything We Know About PRISM To Date,* WASH. POST (June 12, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.
[180] Gellman & Nakashima, supra note 6; Frei, *supra* note 6, at 15.

zero-days were used in Stuxnet.[181] Additionally, the NSA is thought to stockpile and use zero-day vulnerabilities to aid in inserting tracking and other implants on targeted computers.[182]

These NSA activities were widely criticized. Concerning zero-days, the government seemed to maintain the following policy: when it discovered or purchased a vulnerability, the default was not to disclose the vulnerability to affected companies, instead stockpiling it for later use, leaving citizen and industry users vulnerable.[183] The NSA may have had internal policies governing disclosure versus stockpiling, but there is little public indication that such policies existed. Richard Clarke, who advised President Bush on cybersecurity, commented, "[t]here is supposed to be some mechanism for deciding how they use the [vulnerability] information, for offense or defense. But there isn't."[184] The government seemed, by default, to prioritize national security and intelligence needs over broader cybersecurity.

In addition, the 2014 National Defense Authorization Act (NDAA) included language requesting the establishment of "an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate."[185] The NDAA indicated Congress' and the military's awareness of the international security problems created by, among other things, trade in zero-days.

B. *The President's Review Group on Intelligence and Communications Technologies*

Zero-day vulnerabilities were not at the forefront of Snowden's revelations, but the presidential panel tasked with proposing reforms in light of these revelations recommended increased oversight of

---

[181] Nicholas Falliere, Liam O. Murchu, & Eric Chien, *W.32 Stuxnet Dossier Version 1.4*, SYMANTEC SEC. RESPONSE (February 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
[182] *See, e.g.*, Bruce Schneier, *Attacking Tor: How the NSA Targets Users' Online Anonymity,* GUARDIAN (Oct. 4, 2013), http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.
[183] *Expert Warns of Growing Trade in Software Security Exploits*, *supra* note 10.
[184] Andrea Peterson, *Why Everyone is Left Less Secure When the NSA Doesn't Help Fix Security Flaws,* WASH. POST (Oct. 4, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/.
[185] National Defense Authorization Act for Fiscal Year 2014, *supra* note 11.

zero-day vulnerability use. The panel recommended an interagency process managed by the National Security Council to review zero-day vulnerability use.[186] The panel suggested instituting a default policy of disclosing or patching zero-day vulnerabilities, rather than stockpiling.[187] This suggestion is a strong indication that the existing default had been to stockpile rather than disclose. In "rare instances, U.S. policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments."[188]

Peter Swire, a Review Group member, illuminates the thinking behind the zero-day recommendation. Despite being largely absent from Snowden's revelations, focusing on zero-day policy represented an opportunity to stress the attitude the Review Group wanted to encourage in the U.S. government. Swire says, "We didn't decide at the start to go after zero-days. The institutional big picture suggested a worry that offense is greater than defense and one way to address this concern is to address zero-days ... Given our commitment to these broader themes, our recommendation on zero-days was a logical component of our report."[189]

Swire is right to ground zero-days in broader problems; zero-days do not exist in isolation from other cyber considerations. Still, the Review Group's recommendations represent a shift towards greater oversight of zero-days, adding a specific zero-day component to discussions about post-Snowden oversight regimes. The recommendations, however, did not address government purchase of vulnerabilities, a problematic and inseparable aspect of the zero-day problem.

C. *NSA Director Confirmation Hearing Remarks*

In March 2014, Vice Admiral Michael S. Rogers addressed U.S. policy towards zero-day disclosure in his confirmation hearings for becoming Director of the NSA and Commander of U.S. Cyber

---

[186] *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, THE WHITE HOUSE, Dec. 12, 2013, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf , at 219.
[187] *Id.* at 219.
[188] *Id.* at 219-20.
[189] Telephone Interview with Peter Swire, Member, President's Review Group on Intelligence and Communications Technologies (Apr. 17, 2014).

Command. Rogers indicated that the "NSA is now working with the White House to put into place an interagency process for adjudication of 0-day vulnerabilities."[190] Rogers' language echoes the Review Group's, raising the possibility that the Group's zero-day recommendation was being implemented. Rogers also indicated that the NSA has an existing "equity resolution process" for determining what to do with discovered zero-days. The process' "default is to disclose vulnerabilities in products and systems used by the U.S. and its allies."[191]

Rogers' testimony was the first public description of NSA zero-day policy. Although his suggestion that the NSA has a "default to disclose" is initially appealing, what characteristics of vulnerabilities trigger a decision not to disclose a zero-day? What are the consequences of the requirement that the vulnerability should be present in "products and systems used by the U.S. and its allies" to merit disclosure? With only Rogers' testimony to examine, these questions remain unanswered.

D. *After Heartbleed, Senior Officials Detail Policy*

After the discovery of Heartbleed and the subsequent controversy about potential government knowledge of the vulnerability, senior Obama administration officials provided more details on the administration's policy towards vulnerability disclosure. Caitlin Hayden, a National Security Council spokesperson, indicated that the zero-day review process is "biased toward responsibly disclosing such vulnerabilities."[192] Again, this statement contains ambiguities – what percentage of vulnerabilities does this "bias" indicate? In what circumstances does the government decide not to disclose?

The officials further indicated that President Obama decided that, "when the National Security Agency discovers major flaws in Internet security" the NSA "should – in most circumstances – reveal them ... rather than keep them mum so that the flaws can be used."[193] The officials noted President Obama

---

[190] Michael S. Rogers, *Advance Questions, Nominee for Commander, United States Cyber Command Before the Senate Armed Services Committee*, 113th Congress (Mar. 13, 2014).
[191] *Id.*
[192] David Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, N.Y. TIMES (APR. 12, 2014), http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html.
[193] *Id.*

created "a broad exception for 'a clear national security or law enforcement need,'" a loophole which Sanger indicates will "likely allow the NSA to continue to exploit security flaws both to crack encryption on the Internet and to design cyberweapons." [194]

Jack Goldsmith, Harvard Law professor and former Bush administration official, raised questions about these statements. He argues that the statements imply two exceptions: "not every software vulnerability constitutes a 'major flaw in Internet security' and thus those vulnerabilities that do not rise to that level need not be disclosed" and "the phrase 'in most circumstances' implies that sometimes the NSA will not reveal even a major flaw in Internet security."[195] Are vulnerabilities in Microsoft programs, such as those used in Stuxnet, not covered by this new policy? Goldsmith also points out that the phrase "in most circumstances" could encompass broad exceptions.[196] For instance, although it denied prior knowledge of Heartbleed, the administration did not deny the possibility that it would have withheld rather than disclosed the vulnerability had it known about it.

Goldsmith wonders if this announcement represents any change from prior practice, and whether the exceptions will have any practical impact on the NSA's practices. Goldsmith argues that, "these exceptions, taken together, appear to be quite a lot broader than Recommendation 30 [of the Review Group], which (among other things) presumes that all zero-day vulnerabilities will be disclosed (and not only those that constitute a major flaw in Internet security), and allows exceptions only for an urgent national security priority."[197]

Peter Swire discounts these criticisms. He perceives that Recommendation 30 was generally adopted. When I asked him how he would respond to critics who suggest the national security exceptions in the announced policy are too broad, he responded, "It's the job of the ACLU to say that."[198] Swire elaborates, "If you have a zero-day to get into the Iranian facilities and you eliminate it, that is a very

---

[194] *Id.*
[195] Jack Goldsmith, *More on USG Policy on Cyber Vulnerabilities*, LAWFARE (Apr. 12, 2014), http://www.lawfareblog.com/2014/04/more-on-usg-policy-on-cyber-vulnerabilities/.
[196] *Id.*
[197] Jack Goldsmith, *Did President Obama Accept Recommendation 30?*, LAWFARE (Apr. 19, 2014), http://www.lawfareblog.com/2014/04/did-president-obama-accept-recommendation-30/.
[198] *Id.*

consequential decision. Any president would think long and hard before giving up on national security targets like that."[199]

Goldsmith's questions do not reject Swire's assessment of the need for high-priority exceptions, and Goldsmith is not from the ACLU. Still, Swire's perception that the announcement represents change is supported by circumstantial facts. Zero-days were not a prominent feature of Snowden's documents, so less public pressure existed to change zero-day policy. President Obama made earlier policy announcements regarding changes to NSA policy and did not mention vulnerability disclosure. These circumstances could suggest the recent policy statements are more than window dressing.

Perhaps the most concerning omission in the policy announcement is lack of language addressing *purchased* vulnerabilities. The language highlights "when the National Security agency *discovers"* a vulnerability, the bias should be towards disclosure.[200] Does the disclosure bias extend to purchased vulnerabilities? If not, this represents a significant loophole.

Regulating purchase of zero-days, however, is complex. When asked about this potential loophole, Microsoft's Scott Charney reflected that, given appropriate oversight, encouraging government purchasing of vulnerabilities could be beneficial, in order to get vulnerabilities off the market and (mostly) patched.[201] Alternatively, purchased and non-disclosed vulnerabilities could be more valuable, dangerous, or discoverable by third parties, making a lack of oversight even more dangerous to ordinary computer users.[202] If current disclosure policy only extends to vulnerabilities discovered in-house by government agencies, the U.S. government's participation in the gray market remains without evident oversight.

After the *New York Times* article, the White House released a blog post, authored by Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator.[203] Daniel asserts the Obama administration "re-invigorated our efforts to implement existing policy with respect to disclosing

[199] *Id*.
[200] Sanger, *supra* note 192.
[201] Charney, *supra* note 123.
[202] *Id*.
[203] Daniel, *supra* note 5.

vulnerabilities."[204] Is Daniel suggesting that, previously, policy was not implemented with sufficient vigor? Despite cryptic language, Daniel identified questions the administration employs when deciding to disclose or stockpile a vulnerability:

- "How much is the vulnerable system used in the core Internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else was exploiting it?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?"[205]

Goldsmith reads the list to suggest that the administration takes advantage of vulnerabilities "in a wider array of circumstances than (as the Review Group said) in 'rare instances' and only for 'high priority intelligence collection.'"[206] Microsoft's Scott Charney characterizes these questions as a policy of "We'll share unless we don't."[207]

Goldsmith notes, however, that these questions reveal the disclosure equities process is more complex than the Review Group acknowledged. Still, Goldsmith argues that Daniel's post is noteworthy for several reasons, including that it "makes clear that the USG takes defense of the Internet, and

[204] *Id.*
[205] *Id.*
[206] Jack Goldsmith, *Thoughts on White House Statement on Cyber Vulnerabilities*, LAWFARE (Apr. 28, 2014), http://www.lawfareblog.com/2014/04/thoughts-on-white-house-statement-on-cyber-vulnerabilities/.
[207] Charney, *supra* note 123.

disclosure of vulnerabilities, very seriously, and that it has gone to greater lengths than any other nation to make public its policy guidelines."[208]

3. *Analysis of Oversight Mechanisms and U.S. Government Zero-Day Vulnerability Purchase and Use*

Existing oversight specific to zero-days stems primarily from the executive branch. Congress did include calls for the creation of an interagency process that would go on to establish policies to control "proliferation of cyber weapons," but it is unclear what progress on such a group has been made, and whether controlling "proliferation" includes addressing the government's own practices.

The Obama administration has set standards to encourage greater vulnerability disclosure, and could continue to augment that policy. An executive order or presidential policy directive could establish common definitions and policies across agencies, with flexibility to change as needed.[209] An executive order could, for instance, require the approval of the president or an executive branch department head (e.g., Secretary of Defense) for purchase, use, or disclosure of vulnerabilities. It could also mandate interagency cooperation to facilitate greater price and other transparency between competing government purchasers, an idea addressed more below. Scott Charney of Microsoft suggests additional possibilities: "you can do things like an Inspector General's report [i.e. to relevant Congressional committees], an outside review, and independent audit by cleared people."[210] In sum, executive oversight is a relatively low-barrier path to increased oversight and is more easily adapted to changing circumstances than legislative or judicial oversight. Executive oversight may lack high levels of public transparency, but a congressional or judicial approach would also be considerably shrouded from public view given intelligence and military needs for secrecy.

---

[208] Goldsmith, *supra* note 206.
[209] Such mechanisms may exist but are classified.
[210] Charney, *supra* note 123.

The judicial review mechanisms established by FISA deal with authorization of foreign intelligence activities. As such, they are tool-neutral: foreign intelligence surveillance enabled by a zero-day vulnerability or telephone wiretapping would be evaluated under the same legal standards. Given this reality, there is not an obvious role for judicial oversight of use of zero-day vulnerabilities. The nature of FISC's review of foreign intelligence means it would have no role evaluating the purchase of zero-days. Federal court oversight of the purchase, use, or disclosure of zero-days is not in keeping with the judiciary's legislated role in monitoring foreign intelligence within the United States. Attempts to increase the judiciary's oversight role concerning zero-days would likely be opposed by the IC as heavy-handed and unnecessary. The IC would likely, and perhaps rightly, question whether an operation using a purchased zero-day vulnerability deserves greater judicial scrutiny than other intelligence operations.

Congress could impose limits on purchase, use, and disclosure of zero-days. As it has done with intelligence activities and covert actions, it could require reporting from agencies and/or Inspector Generals to relevant congressional committees when a zero-day is purchased, used, disclosed, and/or not disclosed. Such requirements could be accompanied by the threat of withheld appropriations if the executive branch fails to follow oversight rules. However, congressional oversight is likely politically difficult to achieve. Snowden has made cyber topics politically fraught, and Congress is perceived as dysfunctional. Congressional oversight has also traditionally applied to broad programs, such as foreign intelligence activities within the United States or covert operations overseas, not a specific means of accomplishing law enforcement, intelligence, or military objectives.

4. *Select Possibilities for Expanded Executive Branch Oversight of Zero-Day Vulnerabilities*

This section presents several specific possibilities for greater oversight I developed through conversations with experts. While not fully formed, they demonstrate the range and flexibility such mechanisms could possess, and address perceived holes in current policy. Particularly, these possibilities

conceive of oversight that could address both use and purchase of zero-day vulnerabilities, whereas current oversight appears to focus on use and disclosure.

Based on existing executive branch oversight of zero-days and its advantages for implementation and alteration, oversight by the executive branch appears to have the most promise as a zero-day oversight mechanism. The first potential way to expand executive branch oversight would be to encourage increased transparency about government practices. Transparency is a typical first-stage oversight approach and could take a variety of forms. Currently, U.S. government agencies seem to make zero-day purchases separately, without coordination, potentially bidding prices up.[211] To address this issue, one mechanism might be to have government agencies participate in a registry, where prices for purchases are shared.[212] Economists have demonstrated that price transparency generally leads to lower prices, although effects vary between products.[213] Using transparency to achieve lower prices, although benefitting government purchasers, would also serve to equalize white-market and gray-market cost incentives. To address bidding wars driving prices high or low, Mayer suggested instituting "a priority list, so if DEA [Drug Enforcement Agency] and NSA bid on a vulnerability, NSA could get it."[214]

This shared-list mechanism would constitute buyer coordination, which can lower prices.[215] Intelligence agencies have resisted public disclosure of prices for zero-day vulnerabilities,[216] but buyer coordination could represent a middle path, hopefully resulting in lower prices for agencies while not requiring public sharing of prices.

---

[211] Miller, *supra* note 43.
[212] I credit Chris Soghoian for the inspiration for this idea.
[213] D. Andrew Austin & Jane G. Gravelle, *Does Price Transparency Improve Market Efficiency? Implications of Evidence in Other Markets for the Health Sector,* CONGRESSIONAL RESEARCH SERV., Apr. 29, 2008, at 2; Robert Bloomfield & Maureen O'Hara, *Market Transparency: Who Wins and Who Loses?*, 12 REV. FIN. STUD. 5 (1999). In financial and online markets, especially price comparison sites for insurance and airline tickets, transparency decreased prices (see Austin & Gravelle, at 2). In some markets, particularly involving intermediate goods or middlemen, price transparency can make seller collusion easier, raising prices (see Austin & Gravelle, at 7).
[214] Mayer, *supra* note 101.
[215] R. Owen Phillips, Dale J. Menkhaus, & Kalyn T. Coatney, *Collusive Practices in Repeated English Auctions: Experimental Evidence on Bidding Rings,* 93 AM. ECON. REV. 965 (2003), at 965; United States Department of Agriculture, *Assessment of Cattle and Hog Industries Calendar Year 2000,* GRAIN INSPECTION, PACKERS, AND STOCKYARDS ADMIN. (2001), at 30.
[216] NSA-Vupen Contract, *supra* note 69.

Transparency mechanisms can be criticized as weak measures. Mayer suggests several ways to help ensure transparency mechanisms are more than gestures. As one example, he envisioned a policy that would threaten banning purchase of zero-days after a certain period, unless players respond well to the transparency mechanisms.[217] However, Mayer concedes, little political appetite for pressure on industry currently exists.[218]

Beyond transparency, executive branch oversight could strengthen the equities process for disclosure of vulnerabilities, extending what was recently announced. Particularly, instituting a post-use or post-stockpiling review could ensure reevaluation of vulnerabilities previously exempted from disclosure. This review could ensure that the original national security need for exempting the vulnerability from disclosure continues to validate keeping the vulnerability secret. Charney reflected on the prospect of such a review process, and commented that, indeed, after Stuxnet, it might be interesting to see whether the government adequately balanced competing equities.[219] Moreover, if purchased vulnerabilities are not currently subject to the same initial review as vulnerabilities discovered in-house, post-use or post-stockpiling review would extend the equities process to this important category of vulnerabilities.

E. *Summary of Domestic Regulation Strategies*

This part analyzed three domestic strategies for regulating the zero-day trade – criminalization, national export controls, and increased oversight. Criminalization might motivate sellers to participate in the white market or sell only to certain gray-market buyers, such as the U.S. government. The CFAA carve-out for government agency activities may already somewhat encourage this outcome. However, criminalization has downsides, including debates about what form of liability it would take, due process concerns about definitional precision, the potential to chill security research, its limited impact on the global scale of the trade, and its inapplicability to U.S. government behavior.

---

[217] Mayer, *supra* note 101.
[218] *Id*.
[219] Charney, *supra* note 123.

Export controls could reduce the range of customers who can access vulnerabilities sold by U.S. companies. Additionally, the burden of dealing with export regulations might incentivize sellers to turn to U.S.-based customers, including the U.S. government.[220] Still, export controls face geopolitical, economic, technical, and First Amendment obstacles.

Policies governing U.S. government purchase and use of zero-days, and details of the gray market, need clarification for effective oversight mechanisms to be crafted. Theoretically, executive branch oversight has the best chance of encouraging U.S. government agencies to disclose rather than stockpile vulnerabilities and of resetting the equities calculus between defense and offense. Additional oversight mandated by the President could reduce the number of vulnerabilities the U.S. government purchases. Alternatively, if oversight reduces exploitable vulnerabilities (by encouraging disclosure), but the government does not decrease purchasing, the government could function like a bug bounty, buying vulnerabilities but ensuring most get disclosed and fixed.[221] Dan Geer of In-Q-Tel, which has links to the CIA, has advocated this approach.[222] However, if oversight encourages a reduction in government-purchased vulnerabilities, what happens to the vulnerabilities the government would have purchased is an open question. A decrease in U.S. government buying could reduce demand and lead gray-market companies to diversify product offerings or turn to white-market options. Or, gray-market companies may find foreign buyers less favorable to U.S. interests.

From the examined options, pursuing expanded executive branch oversight of zero-day use and procurement seems the most feasible and potentially effective option. Such oversight would address U.S. government participation in the market, a critical component of the gray-market system, and represent a politically attainable and adaptable approach to regulating the zero-day trade. However, executive branch oversight is opaque and may not increase public trust in how zero-days are handled. Oversight of U.S. government use and procurement of zero-days also cannot address gray-market buyers and sellers beyond

[220] It is also, however, feasible that companies would relocate overseas to avoid export controls.
[221] *See, e.g.*, Jean Camp, *The State of Economics of Information Security*, I/S: J. L. AND POL'Y IN THE INFO. SOC'Y (2006).
[222] Kim Zetter, *CIA Insider: U.S. Should Buy All Security Exploits, Then Disclose Them*, WIRED (Aug. 6, 2014), http://www.wired.com/2014/08/cia-0day-bounty/.

U.S. borders. The zero-day market is manifestly global, and the United States would have no guarantee that allies or foes would follow U.S. restraint. The next part addresses this weakness of domestic mechanisms and investigates prospects for international strategies to control the zero-day vulnerability trade.

IV. International Strategies for Regulating the Trade in Zero-Day Vulnerabilities

A. *Introduction*

The global nature of the zero-day problem means collective action strategies should be analyzed. The strategies examined in this article reflect the range of mechanisms available for international cooperation, including binding international law, voluntary coordination, and collective action among allies. The strategies were chosen to reflect, where possible, policy options under consideration. For example, a policymaker engaged with this issue indicated that the Wassenaar Arrangement (analyzed below) was being discussed as a collective action strategy for zero-days in September 2013.

B. *Using International Law to Regulate the Zero-Day Trade*

1. *International Law as an Instrument of International Governance*

International law is an important instrument of international governance, with its distinguishing feature being the binding nature of the commitments it facilitates. Although not always successful, states use international law to facilitate cooperation on problems of mutual interest requiring coordinated action. The global nature of the zero-day trade, and the global effects of countries' zero-day decisions, raises the need to think about collective action through international law as one way to regulate the trade.

2. *Controversies Concerning International Law in Cyberspace: The UN Governmental Group of Experts*

Applying international law to cyberspace has been controversial, as illustrated by the deliberations of the UN Governmental Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE).[223] The GGE grappled with whether principles of international law apply to cyberspace. The first GGE in 2004 failed to produce any report.[224] Subsequent meetings adopted reports, but the GGE did not reach agreement on application of international law to cyberspace. The 2012-13 report was heralded as a breakthrough when the GGE reached consensus that international law, including the UN Charter, applies to cyberspace.[225] This report is considered the first time a UN-level group reached consensus about norms for responsible cyberspace behavior.[226] The United States welcomed the report, saying it signaled that states must act in accordance with international law in cyberspace.[227] However, agreeing that the UN Charter applies to cyberspace brings existing problems with this treaty (e.g., on the use of force) into the cyber realm and does not address how the cyber context challenges longstanding rules of international law.

The GGE could discuss how international law should inform regulation of the zero-day trade. This trade fits within the GGE's mandate to explore developments with information and communications technologies affecting international security, and the GGE's experience might give it more credibility than a new mechanism. However, consensus that international law applies in cyberspace does not provide much of a foundation on which to have productive discussions about the zero-day trade. This trade does not obviously violate principles of international law enshrined in the UN Charter, meaning states would

[223] *Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security,* UNITED NATIONS OFFICE FOR DISARMAMENT AFF. (June 2013), http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.
[224] *Id*.
[225] Rep. of the Group of Governmental Experts on Developments. in the Field of Information and Telecommunications in the Context of International Security, Jun. 24, 2013, U.N. Doc. A/68/98; GAOR, 68th Sess. 2013. http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.
[226] David Wolter, *The UN Takes a Big Step Forward on Cybersecurity,* ARMS CONTROL TODAY (September 2013), http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity.
[227] Jen Psaki, *Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues,* U.S. DEP'T OF STATE (Dec. 7, 2013), http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

need to negotiate specific rules to regulate this trade.[228] That need raises questions about whether the GGE, which struggled simply to reach consensus on whether international law applied to activities in cyberspace, could negotiate tailored international rules to govern the zero-day trade.

3. *International Law and Internet Governance: The International Telecommunication Regulations*

The Internet currently is governed through "multi-stakeholder processes," which involve governmental, corporate, and civil society actors. These processes operate outside international legal frameworks in part to allow non-governmental actors to participate in ways not normally seen with international legal mechanisms. Advocates for the multi-stakeholder process, including the United States, have opposed bringing Internet governance under international law and inter-governmental control. Other states, especially China and Russia, advocate for Internet governance to come under inter-governmental control by formal rules.

As global communications developed, global bodies instituted mechanisms to govern them, including the International Telecommunication Regulations (ITRs), a binding treaty adopted in 1988 by the International Telecommunication Union (ITU).[229] The ITRs came up for amendment in December 2012 at the ITU's World Conference on International Telecommunications (WCIT). The Conference debated extending the ITRs to the Internet, a debate that involved deciding whether international law should play a more prominent role in Internet governance.

---

[228] The challenges presented by the zero-day trade are so new that state practice and *opinio juris* have not developed to the point where rules of customary international law on this issue have formed. This reality necessitates focusing on treaty law as the most likely source of binding international law on zero-days.

[229] *World Conference on International Telecommunications (WCIT-12)*, INT'L TELECOMM. UNION (2014), http://www.itu.int/en/wcit-12/Pages/default.aspx.

At WCIT, the United States argued that extending the ITRs to the Internet would undermine existing multi-stakeholder governance.[230] China, Russia, the United Arab Emirates, and other countries, supported amending the ITRs to bring Internet governance within the treaty and closer to ITU control.[231] The United States defeated a binding proposal, but a non-binding resolution gained majority support. The United States rejected the entire outcome of the negotiations. WCIT ended with a sense that the advocates for greater state and inter-governmental control over Internet governance had momentum.

WCIT demonstrates another instance where nations struggled to gain consensus about applying international law to cyberspace. Using the ITRs or the ITU as a venue for negotiating international legal rules for the zero-day trade would face resistance, given the disagreements already experienced at WCIT. The revised ITRs, as a treaty, and the ITU, as a diplomatic venue, are too politically controversial, and are unlikely places to support development of international legal mechanisms for governing the zero-day trade.

4. *Council of Europe Convention on Cybercrime*

The Council of Europe's Convention on Cybercrime seeks to harmonize national criminal law on cybercrime and strengthen international law enforcement cooperation on cybercrime, making it a direct application of international law to a cybersecurity problem. The Obama administration recently stated that the Convention was "effective in breaking down barriers to transnational cooperation" and the United States is "able to respond to potential threats more quickly and effectively than ever" as a result of this collaboration.[232] Still, the Convention experiences serious problems. According to critics, the treaty achieved consensus by adopting broad definitions and including a plethora of requested items rather than

---

[230] Stewart M. Patrick, The Obama Administration Must Act Fast to Prevent the Internet's Fragmentation, COUNCIL ON FOREIGN REL. (Feb. 26, 2014), http://blogs.cfr.org/patrick/2014/02/26/the-obama-administration-must-act-fast-to-prevent-the-internets-fragmentation/.
[231] *Russia, UAE, China, Saudi Arabia, Algeria, Sudan, and Egypt: Proposals for the Work of the Conference*, WCITLEAKS (Dec. 3-14, 2012), http://files.wcitleaks.org/public/Merged%20UAE%20081212.pdf.
[232] Eric Holder, Attorney General Eric Holder Speaks at the Rollout of the U.S. International Strategy for Cyberspace with the U.S. Department of Justice (May 16, 2011), http://www.justice.gov/iso/opa/ag/speeches/2011/ag-speech-110516.html.

focusing on consensus issues.[233] The Convention also provides broad grounds for states parties to shirk obligations.[234]

Eleven Council of Europe members have not ratified the treaty.[235] Of non-Council members involved in the Convention's activities, only 6 of 17 ratified.[236] Only 42 states in total have ratified the Convention,[237] which represents approximately 20 percent of UN members. Goldsmith points to disagreements between Western and non-Western states about Convention definitions and rules as reasons for lack of non-Western participation. Goldsmith takes lack of adoption by more Western states as a strong sign that "nations significantly disagree about what digital practices should be outlawed and are deeply skeptical about even the weakest forms of international cooperation in this area."[238] Even on an issue, such as cyber crime, which harms all parties, an international legal approach has proved extremely difficult. Goldsmith argues that this fact bodes poorly for cooperation on cyber issues more directly affecting sensitive issues of sovereignty or national security.[239]

One strategy for dealing with the trade in zero-day vulnerabilities through the Convention on Cybercrime might be to update Article 6, which requires parties to adopt legislation prohibiting "the production, sale, procurement for use, import, distribution or otherwise making available of" tools that can be used to commit cyber crimes.[240] States parties could update this article to regulate directly the distribution of zero-day vulnerabilities. Alternatively, the Convention could place restrictions or transparency obligations on governments purchasing vulnerabilities.

Working within an existing treaty carries advantages: the specific change is the focus of debate, not the form and purpose of the whole agreement. However, the Convention was not designed with the

---

[233] Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View,* KORET-TAUBE TASK FORCE ON NAT'L SEC. AND LAW FUTURE CHALLENGES ESSAY SERIES, HOOVER INST. (2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf, at 3; Amalie M. Weber, *The Council of Europe's Convention on Cybercrime* 18 BERKELEY TECH. L. J. 425 , 444 (2003).
[234] Goldsmith, *supra* note 233, at 3-4.
[235] *Convention on Cybercrime: Status as of 26/8/2014,* COUNCIL OF EUROPE (Aug. 26, 2014).
[236] *Id.*
[237] *Id.*
[238] Goldsmith, *supra* note 233, at 4.
[239] *Id.*
[240] *Convention on Cybercrime: Status*, *supra* note 235.

zero-day trade in mind. Different countries have diverse zero-day use and purchasing behaviors, which would complicate negotiation and weakens incentives parties have to craft new obligations in this area. Additionally, the treaty was designed to harmonize cyber crime laws. Given how little national policy and law currently exists regarding zero-days, addressing this issue through an instrument focused on established criminal activities might be premature, even in trying to use the Convention as the basis for starting discussions.[241]

5. *International Law and Dual-Use Technologies – The Biological Weapons Convention*

The zero-day problem involves the challenge of regulating a dual-use technology, a problem states encounter in other technological contexts. International laws regulating science and technology associated with biological agents are perhaps the closest dual-use analogues for laws regulating cyber technologies. Both biology and cyber share hard-to-distinguish peaceful, defensive, and offensive uses. Furthermore, technical "on-ramps" for both are low. Technological advances are making powerful tools available to more people than before in both domains. Both biology and cyber technologies operate in contexts that make verification of the peaceful nature of research and development difficult to design and execute. Given these similarities, examining the use of international law to address biology as a "dual use" technology might provide insights on challenges facing use of international law to regulate the zero-day issue. Critical differences, exist, however, including that zero-days are discovered, not developed, and are used for espionage, not just military purposes, raising questions whether a Biological Weapons Convention (BWC)-type strategy is appropriate, despite the similarities identified above.

The BWC constitutes a landmark attempt to use international law to prevent biological weapons proliferation. The treaty prohibits development, production, stockpiling, retention, or acquisition of biological agents and toxins in "*types and quantities* that have no justification for prophylactic, protective,

[241] Procedural and political concerns also exist. The Convention has yet to undergo significant revision, so the amendment process would confront political uncertainty.

or other peaceful purposes."[242] The BWC also prohibits the development, production, stockpiling, retention, or acquisition of "[w]eapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict."[243] States parties cannot transfer biological agents, toxins, weapons, equipment, and means of delivery the treaty prohibits.[244] Article X provides that states should facilitate, and retain the right to, the exchange of information, equipment, and materials relating to using biological agents and toxins for peaceful purposes.[245]

The BWC provides lessons for thinking about a zero-day trade treaty. The BWC experienced controversy about the scope of prohibited and permissible activities. The BWC addressed this problem with objective criteria, relying on analysis of types and quantities of biological agents to determine compliance. Still, events have challenged established definitions. For instance, the Bush administration pursued what it called "biodefense research," attempting to replicate an anthrax-dissemination weapon supposedly developed by Russia. Although the administration claimed they only wanted to understand the threat, critics pointed out that these activities could be considered an Article I violation.[246] This episode demonstrated the increasingly controversial role of intent in assessing BWC compliance. A zero-day treaty would likely confront similar problems. What criteria would be a zero-day equivalent for the BWC's type and quantity criteria? Even distinguishing between dangerous and less dangerous vulnerabilities runs into problems, because vulnerabilities in seemingly mundane software (e.g., software running a printer or controlling heating/cooling) can be exploited to devastating effect.

Controversy surrounding Article X demonstrates that divergent economic and trade interests could also complicate a dual-use treaty on zero-days. Article X states that BWC parties will "facilitate, and have the right to participate in" transfer of biological technologies for peaceful purposes.[247]

---

[242] Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, U.N.T.S. 1015 [hereinafter BWC] (emphasis added).
[243] *Id.*
[244] George W. Christopher, et al., *Biological Warfare: A Historical Perspective,* 278 JAMA 412 (1997), at 415.
[245] BWC, *supra* note 242.
[246] DAVID P. FIDLER & LAWRENCE GOSTIN, BIOSECURITY IN THE GLOBAL AGE: BIOLOGICAL WEAPONS, PUBLIC HEALTH, AND THE RULE OF LAW (2008), at 93.
[247] BWC, *supra* note 242.

Developing countries have sought formalization of this technology transfer, but developed states have resisted for nonproliferation and intellectual property reasons.[248] With zero-days, a similar conflict between cyber "haves" and "have nots" could emerge.

The BWC also highlights the difficulties of building verification mechanisms into treaties on dual-use technologies. Attempts to add confidence-building mechanisms to the BWC (e.g., increased transparency through reporting) have generally been unimpressive. Negotiations to adopt a binding verification protocol failed. With the definitional issues associated with dual-use activities and political resistance to verification mechanisms, it is difficult to see what other compliance-enhancing strategies might work. Both of these issues are present with trade in zero-days; verification would likely be a major challenge for any zero-day treaty.

Most critically, the BWC attempts to eliminate a class of weapons while allowing peaceful research. It is not apparent what parallel aim a treaty on trade in zero-days would achieve. Zero-days cannot be eliminated in the same way that the BWC prohibits biological weapons; vulnerabilities are an inevitable part of software development. A treaty could only regulate purposeful discovery, distribution, and use. Further, zero-days are useful for purposes that do not have biological parallels. Particularly, zero-days can be used in espionage and law enforcement investigations, not just military activities. States that find zero-days useful for these purposes might resist a treaty. As a dual-use issue, zero-days and their trade present problems that existing international law on dual-use technologies does not adequately address.

6. *Summary of an International Legal Approach to Trade in Zero-Day Vulnerabilities*

An international treaty to regulate trade in zero-day vulnerabilities would bring the legitimacy often associated with negotiated, binding commitments. A legally binding mechanism potentially

[248] *Id.*

increases cost of noncompliance with the regime.[249] Given the verification issues that would emerge with dual-use zero-day vulnerabilities, a legally binding mechanism may be the only way to achieve reasonable expected adherence to an international control regime.[250]

An international legal approach to the vulnerability trade, however, is likely politically impossible. States exhibit a "fundamental clash of interests" concerning activities in cyberspace[251] (a reality Snowden exacerbated), making a binding zero-day mechanism unlikely. Existing controversies about how to apply, interpret, and enforce international law in cyberspace would complicate zero-day international law. Moreover, the multi-stakeholder Internet governance approach and advocates for expanded governmental and inter-governmental control over the Internet would clash in any effort to develop an international legal approach to trade in zero-days. Last, even though biology and cyber are both dual-use technologies, biological weapons can kill people, but zero-day vulnerabilities cannot. This difference will affect state calculations when weighing international cooperation.

The nature of the zero-day trade also does not appear addressable in treaty form. A range of actors use zero-days for many purposes, a more complicated milieu than the state actors targeted by the BWC. Scope, definitional, and verification concerns would exist regarding any zero-day treaty. Although international law is versatile, its binding nature can deter states when complexity and uncertainty are prominent elements of the problem. In such situations, states might prefer flexible, non-binding strategies, at least until a path to effective, binding commitments is clearer.

In addition to political conflict, economic concerns would affect formulation of a zero-day treaty. The zero-day trade is lucrative. As seen in the BWC context, balancing nonproliferation, development, and intellectual property interests of states parties is challenging, and states with strong zero-day industries and states without may disagree about whether and how to restrict access to zero-days.

---

[249] Richard L. Williamson, *Hard Law, Soft Law, and Non-Law in Multilateral Arms Control: Some Compliance Hypotheses,* 4 CHI. J. INT'L L. 59 (2003), at 71.
[250] *Id*.
[251] Goldsmith, *supra* note 233, at 12.

C. *Voluntary Collective Action to Regulate the Zero-Day Trade: The Wassenaar Arrangement*

1. *Voluntary Collective Action and the Zero-Day Trade*

States can also choose to cooperate on issues in a nonbinding setting, allowing flexibility and fewer formal limits on sovereignty than international law. The Wassenar Arrangement (WA) is such a voluntary arrangement among a diverse group of countries, designed to harmonize export controls on conventional arms and dual-use technologies.[252] The WA is a middle ground between uncoordinated national export policies and a treaty imposing binding obligations to harmonize export controls. Dual-use technologies, including encryption, have been on WA control lists for years.[253] According to an off-the-record interview I conducted, policymakers were considering the WA as a potential option for controlling the zero-day trade in September 2013. Changes to the WA in December 2013 raised the question whether the WA applied to zero-day vulnerabilities. Given that the WA has been subject to zero-day specific debate, it is a particularly important option to investigate.

2. *Details of the Wassenaar Arrangement*

The WA seeks to prevent destabilizing proliferation of conventional arms and dual-use technologies.[254] The WA serves as an information gathering and sharing mechanism, encouraging transparency about transfers.[255] The WA maintains lists of controlled items, and members are expected to implement national laws consistent with these lists.[256] WA members are asked to notify other members of certain transfers and denials of export licenses.[257]

---

[252] *Introduction*, THE WASSENAAR ARRANGEMENT WEBSITE (May 19, 2014), http://www.wassenaar.org/introduction/.
[253] Ron Smith & Bernard Udis, *New Challenges to Arms Export Control: Whither Wassenaar?*, NONPROLIFERATION REV. 81 (Summer 2001), at 81.
[254] Jamil Jaffer, *Strengthening the Wassenaar Export Control Regime*, 3 CHI. J. INT'L L. 519 (2002), at 521, at 520.
[255] Smith & Udis, *supra* note 253, at 88.
[256] *Wassenaar Arrangement*, INVENTORY OF INT'L NONPROLIFERATION ORG. AND REGIMES, CENTER FOR NONPROLIFERATION STUDIES (Jun. 12, 2012), http://cns.miis.edu/inventory.
[257] Jaffer, *supra* note 254, at 520; Smith & Udis, *supra* note 253, at 88.

At the WA's heart are control lists for conventional arms and dual-use goods. The dual-use list includes items ranging from components of marine and aviation navigation systems to information security tools.[258] The WA updates the lists through a slow-moving review process.[259]

Wassenaar members cannot veto including or excluding items from the lists.[260] The WA does not maintain a list of restricted countries and does not require reporting to the WA before export of goods.[261] Instead, the WA requests aggregate, *post facto* notification of exports and license denials at regular intervals.[262] This system allows national governments to retain discretion about whether to adhere to WA consensus.[263] Since the WA is voluntary, the WA does not have formal compliance mechanisms.[264]

The WA has attempted to update procedures for controlling intangible technology transfer, especially as it included new cyber tools on its lists (see below). The group developed a Statement of Understanding on Intangible Technology, directed at closing "wide discrepancies" among member practices.[265] The WA group considered this effort a priority, because "lack of controls on intangible transfers very much undermined all of the other efforts of control."[266]

3. *Challenges and Benefits of Multilateral Export Controls*

Multilateral export controls offer advantages over national export controls, enabling coordination that achieves greater effectiveness than national-only approaches, particularly when actions of one state

[258] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Technologies: List of Dual-Use Goods and Technologies and Munitions List, December 2013, http://www.wassenaar.org/controllists/.
[259] Smith & Udis, *supra* note 253, at 88.
[260] Corr, *supra* note 132, at 455.
[261] *Id*.
[262] *Id*.
[263] *Wassenaar Arrangement*, *supra* note 256.
[264] *Id*.
[265] Samuel Evans, *Technological Ambiguity & the Wassenaar Arrangement (2009) (unpublished DPhil dissertation, Oxford University)(on file with Oxford University)*, at 292.
[266] *Id*. at 303.

have little effect on the overall problem.[267] However, countries have historically hesitated to place export controls under international law, preferring to cooperate voluntarily to maintain greater autonomy.[268]

Coordination of export controls also carries risk. [269] Multilateral export controls often involve parties with different interests, resulting in problems establishing, monitoring, and enforcing controls. For instance, it only takes one sale of a dual-use technology to undermine the objective of denying an adversary access to that technology. The difficulties of defining and enforcing definitions of dual-used items, the economic costs to participants of complying with controls, and the different interests of participants make effectiveness hard to create and sustain. Additionally, the costs of control often fall on the private sector, instead of governments.

Other challenges come from states targeted by the WA. These states can perceive export controls as attempts by wealthy nations to restrict supply to raise prices.[270] Restricting supply can also encourage indigenous development of restricted items and illicit activities to gain access to them.[271] For instance, countries such as Egypt and Syria, if formally denied zero-days through the Wassenaar, may turn instead to actors within their country or the black market. Even though a multilateral export control mechanism could prevent companies located in member states from doing bad things, the actions of targeted countries would be beyond the mechanism's control.

Zero-day buyers and sellers are globally distributed. The repercussions of stockpiling can be felt globally, because an undisclosed vulnerability potentially puts every user of globally distributed software at risk. The wide dissemination of, and global participation in, the zero-day trade means that export controls must be multilateral in nature to curtail the trade. Additionally, multilateral export controls are trade-based mechanisms. In comparison with other international approaches to dual-use technologies (e.g., the BWC), multilateral export control mechanisms are built with trade in mind, making this

---

[267] *Id*.
[268] *Id;* Kenneth Abbott & Duncan Snidal, *Why States Act Through Formal International Organizations,* 42 J. CONFLICT RESOL. 3 (1998).
[269] Jaffer, *supra* note 254, at 521; Michael Beck, *Reforming the Multilateral Export Control Regimes,* NONPROLIFERATION REV. 91 (Summer 2000), at 93.
[270] Smith & Udis, *supra* note 253, at 85.
[271] *Id.* at 86.

approach relevant for dealing with trade in zero-days.

4. *Criticism of the Wassenaar Arrangement*

The WA has been criticized for weakness and ineffectiveness and critiqued by developing countries as a way for developed nations to maintain a high technology monopoly.[272] The WA has also been criticized for its inability to gain consensus. The WA includes members that do not agree on all aspects of security, with members Russia and the United States as a salient example.[273] The WA's reliance on majority rule and lack of a veto mechanism complicate achieving consensus. Although perhaps politically necessary, the lack of a veto mechanism means that states with problems with the control lists have no way to express disapproval except through noncompliance, weakening the regime.[274] The informal nature of the lists, which allow national discretion regarding implementation, also means compliance is not consistent.[275]

Another significant problem is undercutting. The WA requests aggregate sharing of information about exports every six to twelve months, depending on the technology.[276] The lack of time-sensitive data can result in negative consequences. For instance, members are asked to report denials of export licenses for certain items.[277] This policy means that members who deny export permission signal to other members that "there may be an export opportunity available" and provides little opportunity for countries to exercise effective influence over other members' export decisions.[278]

5. *Do Recent Wassenaar Arrangement Changes Apply to Zero Day Vulnerabilities?*

[272] Jaffer, *supra* note 254, at 521; Smith & Udis, *supra* note 253, at 89; Beck, *supra* note 269, at 93, 96.
[273] Beck, *supra* note 269, at 94.
[274] Jaffer, *supra* note 254, at 521; *Wassenaar Arrangement*, *supra* note 256.
[275] Beck, *supra* note 269, at 95, 101.
[276] I*d.* at 97.
[277] Jaffer, *supra* note 254, at 521.
[278] *Id.*

In December 2013, member states amended the WA control lists to include "intrusion software." The original proposals for this change came from France and the United Kingdom.[279] Privacy advocates worked to raise awareness in the French and British governments about the need to keep surveillance software from repressive regimes, human rights violators, and other bad actors.[280] Initially, it seemed the changes might apply to zero-days. This section examines the conversation that occurred as relevant parties debated 1) whether or not the changes applied to zero-days and 2) the problems and benefits of such an application. This recent debate is a crucial to include when assessing the WA's suitability as a potential control mechanism for zero-days.

The changes are difficult to parse. Eric King of Privacy International was involved in advocating for the changes, but notes, "it took us about two weeks to figure out what it meant, and there's still uncertainty and a number of other people will probably read into them."[281] Sam Evans, a WA expert, agrees: "the language seems massively broad."[282]

Table 4: Wassenaar Arrangement Definition of Intrusion Software[283]

"Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network capable device, and performing any of the following: a. The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Table 5: Wassenaar Arrangement Controls Related to Intrusion Software[284]

[279] Edin Omanovic, *International Agreement Reached Controlling Export of Mass and Intrusive Surveillance Technology*, PRIVACY INT'L (Dec. 9, 2013), https://www.privacyinternational.org/blog/international-agreement-reached-controlling-export-of-mass-and-intrusive-surveillance.
[280] Telephone interview with Eric King, Head of Research at Privacy International (Jan. 16, 2014).
[281] *Id.*
[282] Skype interview with Samuel Evans, Associate Director for Research, Center for Science, Technology, Medicine and Society at University of California Berkeley (Apr. 21, 2014).
[283] *The Wassenaar Arrangement*, *supra* note 258, at 209.
[284] *Id.* at 73, 74.

- 4. A. 5. Systems, equipment, and components therefore, specially designed or modified for the *generation*, *operation* or *delivery* of, or *communication* with, "intrusion software". [Emphasis added] (73)
- 4. D. 4. "Software" specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software." (74)
- 4. E. 1. c "Technology" for the "development" of "intrusion software." (74)

The following interpretation represents the consensus of the civil society members interviewed for this article, on- and off-record, who were also involved with advocating for the changes. The changes sought to curb trade in software systems used to disseminate and implement "intrusion software," including large-scale, commercial surveillance tools. The intent was not to control dissemination of malware, root kits, or zero-day vulnerabilities that can be components of surveillance software or legitimate security research tools.

King explains, "There is confusion between how intrusion software is defined [in the WA] and what is actually controlled. The definition of intrusion software is broad, but that isn't actually controlled. What is controlled are systems, equipment, and components, specially designed for the generation, operation or delivery of, or communication with, intrusion software. It's targeting the complete package."[285]

For instance, the changes would target products from companies such as the U.K.-based Gamma Group, which makes the FinFisher surveillance software enabling remote computer monitoring. It would also target the Italy-based Hacking Team, which sells the Remote Control System software enabling access to computers by taking advantage of vulnerabilities. CitizenLab suspects zero-day vendor VUPEN is Hacking Team's primary vulnerability supplier.[286]

[285] King, *supra* note 280.
[286] *Id*.; Bill Marczak, et. al., *Mapping Hacking Team's 'Untraceable' Spyware*, CITIZENLAB (Feb. 17, 2014), https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

King adds, "As we understand it, the U.K. government had no intention of controlling zero-day exploits" through the recent changes, but interpretation is distinct from intent.[287] King emphasizes, "Implementation is where the problems would be."[288]

Evans also points to implementation problems:

> The problem with all list-based mechanisms is the difficulty of moving between text and object. There are different interpretations that the text controls this and not this. It is difficult with cannons and tanks, more difficult with things like circuits and hardware, and super hard with software. But it is not impossible. It just means there is much more work that needs to be done outside of the listing itself to make controls meaningful.[289]

When first released publicly, it seemed the changes might have intended to control exports of zero-day vulnerabilities and/or zero-day exploits. Indeed, in the wake of the changes, VUPEN, a leading zero-day seller, indicated it considered the new restrictions applicable to its exploit products. It announced that it would restrict sales of exploits, supplying only approved government agencies in approved countries, and would automatically exclude countries subject to other European Union, U.S., or UN trade restrictions.[290]

King cast doubt on VUPEN's analysis of the Wassenaar changes: "If they were actually controlled, they would not be as delighted as they appear to be. They would be in serious business trouble, their compliance costs would skyrocket, given their current client base."[291] Rather, King argued, VUPEN may embrace the Wassenaar changes as a way to head off further, more specific zero-day regulation.

Despite King's confidence that "if we keep the text as is, we're fine," the existing language raises questions. It attempts to differentiate between, for instance, a root kit and the tool deploying the root kit. This difference matters because it determines the tools actually controlled by the change. In theory, this distinction regulates surveillance tools but not surveillance tool components. It would control the system using a zero-day vulnerability, but not the zero-day itself. This difference would mean security

---

[287] King, *supra* note 280.
[288] *Id.*
[289] Evans, *supra* note 282.
[290] *Applicable Regulations and Restrictions,* VUPEN (2014), http://www.vupen.com/english/services/lea-index.php.
[291] King, *supra* note 280.

researchers could continue to use tools vital to their work, because they do not typically deploy the same large-scale systems as the targeted companies deploy.

Despite not targeting zero-days, the distinction may have secondary effects on zero-days. For instance, VUPEN is suspected of supplying Hacking Team with zero-days.[292] If Hacking Team's market for surveillance systems decreases, they may not buy as many zero-days, decreasing VUPEN's customer base. However, VUPEN appears to have many other clients besides surveillance-system sellers, particularly government clients, so these secondary effects on companies such as VUPEN may not be dramatic.

The distinction also raises technical questions. When are lines of code "specially designed" for installation of intrusion software? Is it just the line that says "install rootkit.exe" that is controlled?[293] If so, the regulation would be meaningless, because such a line is easily added or removed. Is any program that includes an install line included? If so, the regulation is overbroad. These examples are simple, because one line of code is often not the extent of installation architecture, but it demonstrates the point. Without greater regulatory and technical clarity about the distinction between peripheral software and components of intrusion software, the attempt to control digital surveillance tools may be thwarted or damage legitimate security research.[294]

6. *Analysis of the Wassenaar Arrangement and Trade in Zero-Day Vulnerabilities*

[292] Marczak, *supra* note 286.

[293] Jennifer Granick & Mailyn Fidler, *Update: Changes to Export Control Agreement Intended to Apply to Surveillance Technology, not Exploits, but Confusion and Ambiguity Remain*, JUST SECURITY (Feb. 19, 2014), http://justsecurity.org/7276/update-export-control-arrangement-intended-apply-surveillance-technology-exploits-confusion-ambiguity-remain/.

[294] As countries implement the WA changes, new controversies about the WA and security research are arising. The 2015 Pwn2Own Contest, a prominent white-market hacking event, sparked such controversy. An email reportedly circulated by a group involved in organizing the contest warned that "exploits are export controlled items & participants should work with their legal counsel on proper handling." Based on Twitter messages, European participants seemed most concerned, perhaps based on the European Parliament's interpretation of the WA changes. Regardless, this situation demonstrates that controversy and confusion continue over how the WA affects security research. See Pauli, Darren, *Hackers Fear Arms Control Pact Makes Exporting Flaws Illegal*, THE REGISTER (Feb. 16, 2015), http://www.theregister.co.uk/2015/02/16/smaller_prizes_tougher_laws_make_hackers_pwn2owns_first_scalp/.

One of the core problems with the zero-day trade is that some governments are concerned that vulnerability sellers might sell zero-days to unfriendly governments or other end-users of concern. This problem reflects the general dilemma the WA was set up to address: coordinate national export policies on dual-use technologies for national security purposes. The WA, then, is fit for the mission of regulating the zero-day trade.

As a potential platform for international governance of the zero-day vulnerability trade, the WA offers various benefits. Namely, it engages a wide swath of actors. A major limitation of unilateral U.S.-based export controls is their lack of impact on the global nature of the trade. The WA, by contrast, includes 41 states.[295] In particular, the WA engages a "captive" audience. The WA does not need to attract new participants to address zero-days, because it can rely on existing membership and procedures. Although the WA does not include many confirmed purchasing governments, such as Israel, Brazil, and India, the WA includes many nations where major zero-day sellers are located, including the United States, United Kingdom, France, Malta, and Italy.[296]

Organizationally, the WA is one of the only international mechanisms that could address the zero-day problem without significant institutional change. The WA offers an efficient forum for negotiations on export of zero-days, because it already exists, deals with export controls on dual-use technologies, and has already moved into the cybersecurity arena with controls on surveillance technologies.

Last, as a flexible mechanism, the WA has the potential to achieve international coordination without making unrealistic demands of participants. Its relatively low demands on sovereignty raise the likelihood that nations will constructively participate. Obtaining agreement to add an item to an existing mechanism will likely be easier than obtaining agreement to join a new, untested, potentially more stringent mechanism.

Despite these advantages, addressing the zero-day trade through the WA confronts difficulties. Defining which aspects of a dual-use technology, especially a cyber technology, to control can be

[295] *Participating States*, WASSENAAR ARRANGEMENT (n.d.), http://www.wassenaar.org/participants/.
[296] *Id.*

difficult, as demonstrated by the definitional challenges surrounding controls on intrusion software. Specifically, the WA would have to work to develop a definition that controls targeted items while allowing security research to continue. Security researchers play a legitimate and significant role in identifying vulnerabilities,[297] including Heartbleed,[298] and have historically opposed export controls as threats to their work. The WA would need to achieve a definition that exempts security research while still controlling targeted items.

The WA also encounters problems with national implementation. Members implement WA-issued guidelines on a national level, giving the WA a flexibility that attracts participants, but could mean that countries control more or less than intended. King expressed concern about the former case: "I would be concerned the government would use such controls in a discretionary manner to go after people they don't like, as we've seen some evidence of in the past."[299] Moreover, on a national level, implementing WA changes would encounter the suite of problems with domestic export controls identified earlier.

Similarly, the WA has little power to ensure compliance, another consequence of the WA's non-binding flexibility. The WA's existing compliance problems would likely be evident with zero-days, too. The lucrative nature of the vulnerability trade presents an economic opportunity for countries, encouraging member states to oppose inclusion of zero-days in the WA, or engage in noncompliance. Given the reputation of the WA as a relatively weak organization, pursuing international control through the WA could be criticized as ineffective.

Cyber technologies are inherently more difficult to control than large missile components, but some cyber technologies seem more easily controllable than others. For instance, the online nature of the zero-day trade and well-developed black market could make compliance with a WA-based control mechanism easy to fake. Changing the WA control list to include surveillance technologies attempted to address compliance issues by targeting weak parts in the chain between production and use. Surveillance technologies, unlike zero-days, involve meetings, on-site visits, telecommunications companies and in-

[297] Charney, *supra* note 123.
[298] Perlroth, *supra* note 1.
[299] King, *supra* note 280.

country partners, equipment installation, software updates, and personnel training.[300] "It's a complete operation," King says, "with multiple points for identification and control."[301] King expresses concern that trade in zero-days does not exhibit the same prolonged relationships between seller and client that have been useful in regulating information-based technologies. "A zero-day is something I can knock together in my bedroom and send to you," King says.[302] Controlling zero-days may present more challenges than the recent WA forays into controlling certain cyber tools.

Last, the WA is a supply-side solution. It would regulate the behavior of a limited number of sellers. Other mechanisms have greater ability to affect demand-side behavior. For instance, a treaty mechanism (see above) or collective defense organization (see below) could include restrictions on government purchasing and use of zero-days. The WA could nominally do this through a Statement of Understanding (a non-binding expression of common opinion), or a similarly low-impact mechanism, but this effort would not be as much in the spirit of the WA as it would be in the spirit of other mechanisms. However, as suggested elsewhere, restrictions on government behavior through other mechanisms may be politically difficult to obtain. As such, the WA presents an attractive balance of multilateral practicality and reach as an international option for controlling the zero-day vulnerability trade, despite its problems.

D. *Collective Defensive Organizations and the Zero-Day Trade: The North Atlantic Treaty Organization*

Collective defense organizations have become increasingly concerned about cybersecurity. Particularly after the 2007 Estonia cyberattacks, the North Atlantic Treaty Organization (NATO) developed organizational structures and policies for cyber defense.[303] Given interest in cyber issues by such organizations, this section analyzes the potential of collective defense organizations as forums for achieving international control of the zero-day trade. Collective defense organizations offer the benefits of

[300] *Id*.
[301] *Id*.
[302] *Id*.
[303] *NATO and Cyber Defense*, NORTH ATLANTIC TREATY ORG. (Aug. 7, 2014), http://www.nato.int/cps/en/natolive/topics_78170.htm.

closer thinking among allies, strong organizational and historical basis for cooperation, and the continued need to engage constructively with other member states on security issues. This section focuses on NATO, which, given its membership, history, and structure, is arguably the leading collective defense organization in the world. NATO has made an explicit effort to integrate cyber issues into its collective defense mission. Additionally, NATO's membership includes many known government buyers and gray-market sellers.

1. *NATO: Background and Cyber Defense Activities*

A. *Background*

NATO is the primary Western collective defense organization. Formed in World War II's aftermath, the alliance sought to deter expansion of Soviet influence and encourage European integration.[304] With 28 member nations, NATO is treaty-based, and its central missions are collective defense and cooperative security.[305] After the Soviet Union's fall, NATO found new challenges in maintaining a unified Europe, including dealing with the breakup of former Soviet states, and focused on more global matters, including piracy off the Horn of Africa and terrorism.[306]

B. *Cyber Defense*

The 2007 Estonia attacks were NATO's cyber awakening. In this incident, Estonian government, commercial, and news web capabilities were taken down by cyber attacks in response to controversy about moving a Soviet-era war memorial in Tallinn. The Estonia attacks demonstrated to NATO the

[304] *A Short History of NATO,* NORTH ATLANTIC TREATY ORG. (N.D.), http://www.nato.int/history/nato-history.html.
[305] *NATO Member Countries*, NORTH ATLANTIC TREATY ORG. (N.D.), http://www.nato.int/cps/en/natolive/nato_countries.htm; *Active Engagement, Modern Defense: Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization,* NORTH ATLANTIC TREATY ORG. (Nov. 2014), http://www.nato.int/cps/en/natolive/official_texts_68580.htm.
[306] *A Short History, supra* note 304; David Fidler, Richard Pregent, & Alex Vandurme, *NATO, Cyber Defense, and International Law*, 4 ST. JOHN'S J. INT'L & COMP. L. 1,3 (2013).

"technical scale and political implications of potential cyber attacks."[307] The 2008 Bucharest Summit addressed these implications. NATO established two institutions: the Cyber Defense Management Authority (CDMA) and the Cooperative Cyber Defense Center of Excellence (CCDCOE).[308] The CDMA helps coordinate member state cyber defense, reviews capabilities, and conducts risk management. The CCDCOE helps improve cyber defense cooperation through research, information sharing, and convening thought leaders. For instance, in 2009, the CCDCOE requested that experts analyze how international law applies to cyber warfare.[309] Although the resulting 2013 report is not official doctrine, it provides important analysis about how NATO members might think about international law, conflict, and cyberspace.[310]

In June 2011, NATO adopted the Cyber Defense Policy and Action Plan, the most advanced step in the maturation of NATO's cyber capabilities.[311] The document enumerated steps to enhance the political and operational readiness of NATO to respond to cyber incidents, including defining minimum requirements for the security of national networks critical to NATO's operations.[312] The CDMA transitioned to a group called the Cyber Defense Management Board, which has been carrying out the Action Plan.[313] The 2012 Chicago Summit reaffirmed these efforts, and NATO Defense Ministers met for the first time in 2013 to focus exclusively on cyber defense.[314]

C. *NATO's Offensive Cyber Debate*

[307] Jason Healey & Leendert Bochoven, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow,* ATLANTIC COUNCIL (2011), at 2.
[308] *Id*.
[309] *The Tallinn Manual on the International Law Applicable to Cyber Warfare,* NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2013, http://www.ccdcoe.org/tallinn-manual.html.
[310] *Id;* Fidler et al., *supra* note 306, at 16.
[311] Healey & van Bochoven, *supra* note 307, at 3.
[312] *Id*.
[313] *Id*.
[314] Fidler et al., *supra* note 306, at 6; *Defense Ministers Make Progress on Cyber Protection,* NORTH ATLANTIC TREATY ORG. (June 3, 2013), http://www.nato.int/cps/en/natolive/news_101143.htm.

NATO's cyber strategy focuses on defense.[315] Even though NATO is a military organization, NATO's leadership "has not yet discussed, let alone authorized, the development of offensive capabilities, doctrine, or rules of engagement in the cyber realm."[316] Meanwhile, the United States, China, and Russia seem to increasingly rely on a wide range of cyber capabilities, including offensive tools – some utilizing zero-day vulnerabilities – responding to mounting geopolitical tensions affecting cyberspace.[317]

NATO members, however, are "extraordinarily sensitive to the alliance having any offensive cyber capabilities or even discussing the need to think about the value of cyber capabilities and operations in missions NATO might undertake," as NATO has done with previous technological developments affecting its mission.[318] Some of this hesitancy stems from NATO members with cyber capabilities not wanting to share with less cyber-capable alliance partners. Additionally, the Snowden disclosures adversely affected prospects for advancing NATO discussions about offensive cyber capabilities because of increased mistrust toward the United States, particularly after revelations of U.S. spying on NATO allies.[319]

The closest NATO has come to addressing offensive capabilities was during the 2011 Libyan campaign. The Obama administration considered "a cyberoffensive to disrupt and even disable the Qaddafi government's air-defense system."[320] Administration officials ultimately decided against the plan.[321] Had the plan been adopted, the debated cyber offensive would likely have been conducted separately, supporting NATO's mission, but not embedded within NATO's chain of command.[322] Recently, Russia reportedly used cyber tactics to disconnect Ukrainian forces from command and control

[315] Healey & van Bochoven, *supra* note 307, at 6.
[316] Fidler et al., *supra* note 306, at 24; Healey & van Bochoven, *supra* note 307, at 6.
[317] Fidler et al., *supra* note 306, at 24.
[318] *Id*.
[319] *Id*. at 25.
[320] Healey & van Bochoven, *supra* note 306, at 6; Eric Schmitt & Thom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, N.Y. TIMES (Oct. 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.
[321] Schmitt & Shanker, *supra* note 320.
[322] Healey & van Bochoven, *supra* note 307, at 7.

as Russian-affiliated forces entered Crimea,[323] demonstrating that adversaries of NATO members are developing sophisticated military cyber capabilities. Cyber seriously affects NATO interests, and at some point, NATO must confront the issue of offensive capabilities.

Equipping NATO with both offensive and defensive capabilities has advantages, but it could also fuel the perceived global "cyber arms race."[324] Perhaps NATO's defense-focus carries advantages of signaling restraint. Alternatively, offensive technologies are integral to cyberspace agility, and, if NATO remains a cyber defense-only organization, its capabilities could fall behind the global technological curve.[325] NATO has the potential to have significant influence in global cybersecurity, but it must be empowered to play both halves of the game.[326]

2. *Analysis of NATO as an Institution for Zero-Day Trade Discussions*

NATO is an influential body, and, if it addressed trade in zero-days, its policies would have global importance. NATO has been relatively successful in addressing new collective defense challenges, so it may have the institutional flexibility to take on zero-days. NATO membership maps well with participants in the zero-day market, including countries with notable buyers and sellers. Additionally, because NATO is a collective defense organization for allies, conceptions of the underlying security problem and opinions about approach may be more aligned than among states not engaged in collective defense. Given the difficulties of other forms of international cooperation, achieving consensus among allies might be strategically attractive.

NATO has developed a focus on cyber defense, and zero-days are relevant to that agenda. Not only could trade in zero-days facilitate attacks against NATO networks, but the stockpiling behavior of member states also leaves other members vulnerable. Key NATO members, such as the United States and

[323] Michael R. Gordon, *Russia Displays a New Military Prowess in Ukraine's East,* N.Y. TIMES (APR. 21, 2014), http://www.nytimes.com/2014/04/22/world/europe/new-prowess-for-russians.html.
[324] Fidler et al., *supra* note 306, at 22.
[325] *Id*. at 24.
[326] *Id*. at 25.

United Kingdom, are purchasers of zero-days.[327] NATO's commitment to cyber defense has resulted in the development of a cyber policy- and decision-making structure and processes that could also be used to address the zero-day issue without significant alteration.

Despite this institutional base, NATO would have to experience a policy shift before addressing zero-days. Zero-days are inherently exploitable: although they have significant implications for cyber defense, they are also closely tied with offensive capabilities of member states and the potential for NATO offensive capabilities. NATO, as an organization, is currently not positioned to discuss offensive cyber issues and has demonstrated wariness of an expanded cyber mandate. Still, as demonstrated by Libya and Russia's actions in Crimea, cyber is an increasing reality of security threats facing NATO. NATO must address cyber capabilities, not just passive cyber defense. Zero-days, as a technology that overlaps both categories, could be a useful place to start this shift.

If this shift occurred, NATO could use its existing structure to foster guidelines for addressing zero-days. The Cyber Defense Management Board (CDMB), which implemented the 2011 Action Plan, could be a starting place for discussions about zero-day policy. NATO could do this in several ways, including using CDMB to increase transparency and information sharing about zero-day issues within member states.

For instance, NATO could establish zero-day a threat-sharing program, in which governments share information about the nature of the zero-day threats they face. This kind of program would probably be least resisted by member states, but NATO could go further. NATO could institute a group disclosure program: when one member stockpiles a vulnerability, it could also disclose the vulnerability to a NATO clearinghouse. NATO members could then protect themselves against that vulnerability or make use of it. NATO could also push for harmonized purchasing policies, perhaps agreeing that NATO members will only purchase or stockpile certain vulnerabilities from certain countries or suppliers.

However, given NATO's lack of appetite for discussing offensive capabilities, NATO can, at best, function as a place to start a conversation among likeminded states. For instance, the CDMB could

[327] Perlroth & Sanger, *supra* note 7.

facilitate discussion of the zero-day issue at the next NATO defense ministers meeting. But even that, as demonstrated, may be a difficult topic to broach. NATO simply may not be ready to address something as complex and controversial as the zero-day trade.

NATO is also not an entity designed for addressing trade in dual-use technologies. It could discuss zero-days, particularly government use and purchasing of zero-days, but it is not designed to influence global trade. NATO has only 28 members; even though many members are active buyers or host active sellers, and may share enough interests to come to consensus, an agreement among a limited group could only produce governance of limited global effect.

Moreover, despite being composed of allies, NATO faces fragmentation of member policies and opinions. NATO members sometimes have domestic political or legal constraints affecting NATO decisions, and the complicated legal ecosystem affecting NATO, made up of national law, transnational law, and international law, creates legal divergence.[328] As indicated by post-Snowden wariness, NATO members do not always share consensus on what activities, particularly in cyberspace, are permissible under international law, especially when activities touch sovereignty and non-intervention issues.[329] Last, in 2014, NATO has been preoccupied with the Ukrainian crisis. Even though cyber played a role in the Ukrainian crisis, the cyber threats are marginal compared to the kinetic, territorial, and political security threats posed by Russian behavior.

E. *Summary of International Legal Approaches*

This section investigated international law, voluntary collective action mechanisms, and collective defense organizations as possible approaches to regulating the international zero-day trade. These international mechanisms display two broad challenges of controlling the zero-day problem. The first challenge deals with the nature of the zero-day trade and applies to all international approaches. Defining which elements of the zero-day trade would be restricted (including technical details) is

[328] Fidler et al., *supra* note 306, at 13.
[329] *Id.* at 23-4.

challenging, especially doing so in a way that would allow legitimate security research. Furthermore, the zero-day trade has few "choke points," in contrast with other cyber technologies. Transfer can happen quickly and without sustained contact between buyer and seller. This feature of the zero-day trade makes verification of compliance with international mechanisms difficult.

The second challenge relates to the forms of the examined approaches. Organizational benefits and downsides vary between the options. An international law approach offers legitimacy, seriousness, and higher expected compliance. However, given current tensions regarding the application and interpretation of international law in cyberspace, a binding mechanism would face political opposition. The lucrative nature of the zero-day trade would likely also generate economic opposition to legally binding regulations. The potential resistance to a binding mechanism suggests that such a mechanism may not garner much support and adherence. Questions also exist about fit: is there a clear subset of the zero-day problem that could be addressed by a binding legal mechanism, or is the technical and political complexity of the trade suited to a more flexible mechanism?

Collective defense organizations offer, in some ways, different features from an international law approach. Although treaty-based, using a collective defense organization such as NATO to address the zero-day problem would mean working among states committed to preserving collective interests; political conflict would likely be less and cooperation higher. NATO offers a policy and decision-making infrastructure experienced with cyber issues. This infrastructure could be used to address the zero-day issue with little modification. However, NATO has not yet addressed policy matters beyond passive cyber defense. To address zero-days, NATO would have to undergo an organizational and policy shift, not an easy change.

The Wassenaar Arrangement, a voluntary, collective export control mechanism, seems a better fit for regulating the zero-day trade. Designed to deal with trade issues, the WA has policies and structures that could be adapted to the zero-day problem. The WA also has experience dealing with adding new cyber technologies to its control lists. The WA has the potential for relatively high adoption, given its flexibility and the experience WA members have with implementing updated WA control lists. However,

under the WA, member states are responsible for implementing the WA control lists. This approach gives states flexibility to decrease or increase the strictness of controls, potentially resulting in harmful discrepancies in zero-day policy.

In sum, definitional and verification challenges extend across all mechanisms, while organizational fit varies. NATO offers an interesting possibility of effective collective action among a small group of likeminded states. However, given the organizational limitations of NATO – the bias towards defense – voluntary collective action through export controls using the WA seems to offer the best chance for collective action on controlling the trade. Still, the WA has severe drawbacks. Specifically, care would be needed in addressing definitional, verification, and implementation challenges. Despite these challenges, the WA offers a workable, existing organizational structure and a way to reach a critical mass of participating nations. The WA seems the most conceptually plausible and politically possible of the international policy options available.

V. CONCLUSION

Current national and international approaches towards zero-day vulnerabilities and their trade embody confusion, controversy, and competition far more than consensus on the cybersecurity threats the zero-day problem creates. Despite lack of consensus, the adverse consequences of the problem are severe enough to have already sparked debate. This article contributes to this debate by suggesting the best national strategy is improved executive branch oversight of U.S. zero-day policies. This approach builds on existing capabilities and the U.S. government's declared bias for disclosure, is politically feasible, and can be calibrated to address changing government needs. For example, executive branch monitoring, review, and disclosure of post-use or post-stockpiling of zero-day vulnerabilities could provide oversight of purchased vulnerabilities and ensure the U.S. government continuously addresses the use-versus-disclosure calculus.

The zero-day market and its problems are global, requiring collective action. This article concludes that using the Wassenaar Arrangement to harmonize export controls on zero-day vulnerabilities

appears the most realistic and suitable international strategy. The WA deals with trade-related security issues and would not need institutional alteration. The Arrangement includes many confirmed buyer and seller nations and is large enough to achieve impact on the zero-day problem through collective action. However, U.S. leadership is required to catalyze international cooperation. To achieve such cooperation, the United States would need to establish policy clarity, signaling to other nations its seriousness about collective action. As Clarke and Swire argued, because international cooperation is currently unlikely, the United States should "step up its efforts" and create "the basis for an international norm of behavior."[330]

The solutions presented here do not solve all problems associated with the zero-day trade. For instance, analysis of the zero-day trade suffers because of market opacity. We need better data to inform how to regulate this trade. Strengthening executive branch oversight and pursuing collective action through the WA would have some transparency-enhancing effects. These strategies would test the U.S. government's commitment to its policy announcements about zero-days, and increased government transparency might increase pressure on sellers to be more transparent. Better information from governments and sellers will help determine whether further regulation is needed. We must continue to revisit how to approach the zero-day trade as new information emerges.

On the international side, the WA provides a politically and substantively workable approach to the zero-day trade, but even this strategy leaves many actors beyond its reach. For instance, using the WA would not directly affect China's policies and practices concerning zero-day purchases, if any, it makes on the international or domestic gray market.

Beyond purchased zero-days, in-house capabilities of foreign governments, including China, to discover zero-days pose a serious problem. Nations may build initial cyber capabilities by purchasing zero-days from the gray market, but many will eventually develop internal capabilities and decrease their reliance on the market.[331] Regulation of the gray market may speed up this process. Greater reliance on in-house capabilities would mean zero-day use would become even more difficult to address, particularly

[330] Richard Clarke & Peter Swire, *The NSA Shouldn't Stockpile Web Glitches,* THE DAILY BEAST (April 18, 2014), http://www.thedailybeast.com/articles/2014/04/18/the-nsa-shouldn-t-stockpile-web-glitches.html.
[331] Bejtlich, *supra* note 55.

through collective action. Regulating legal trade in zero-day vulnerabilities is one problem, but grappling with threats crafted in secret using dual-use cyber tools, beyond effective reach of international action, constitutes an entirely different challenge.