YALE LAW & POLICY REVIEW

Curbing the Market for Cyber Weapons

Paul N. Stockton and Michele Golabek-Goldman***

* President, Cloud Peak Analytics; Managing Director, Sonecon, LLC; former Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (2009 -2013).

** Yale Law School, J.D. expected 2014; Harvard Kennedy School of Government, M.P.P. expected 2014. The authors wish to thank Michael Sulmeyer, Robert Butler, Mark Weatherford, Amy Chua, Matthew Bunn, Jack Goldsmith, Theodore Kassinger, Robert Shaw, Matthew Waxman, and Jonathan Zittrain for their invaluable comments and suggestions. We also thank Saurabh Agarwal and Salzburg Cutler Fellow Program participants for their helpful insights.

INTRODUCTION

President Obama recently warned that "foreign governments, criminal syndicates and lone individuals are probing our financial, energy and public safety systems every day" and that "in a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home."[1] Until recently, the technical challenges of identifying and exploiting U.S. computer vulnerabilities impeded all but the most powerful of nations from acquiring such capabilities. These impediments have vanished. Now, criminals, terrorists, and rogue nations can simply buy what they need in a booming online market for the most dangerous exploits of all: weaponized "Øday" exploits.

A Øday is a software vulnerability that is unknown to the computer user and software manufacturer.[2] The idea is that the software manufacturer has "zero days" to remedy the vulnerability if a hacker discovers it first and exploits it to gain unauthorized access to computer systems. Such Øday exploits can also be weaponized: they can be modified to not only gain access to but also to disrupt, disable, or destroy computer networks and their components. Armed with weaponized Øday exploits, attackers have launched cyber operations such as the "Flame" cyber strikes against Middle Eastern nations and the "Aurora" operation against Dow Chemical, Northrup Grumman, and other major U.S. corporations.[3] These highly publicized attacks have provided a marketing bonanza for companies that openly sell Øday exploits on the web, often in weaponized form, and brag about the effectiveness of their products.[4]

---

1. Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J., July 19, 2012, http://online.wsj.com/news/articles/SB10000872396390444330904577535492693044650.

2. *See What is a Zero-Day Vulnerability?*, PC TOOLS, http://www.pctools.com/security-news/zero-day-vulnerability (last visited Nov. 1, 2013). Some experts instead define a "Øday" as a vulnerability for which there is no patch available. *See Vulnerability Trends*, SYMANTEC, http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends &aid=zero_day_vulnerabilities (last visited Nov. 26, 2013).

3. Pierluigi Paganini, *Cyber-Espionage: The Greatest Transfer of Wealth in History*, INFOSEC INST. (Feb. 12, 2013), http://resources.infosecinstitute.com/cyber-espionage-the-greatest-transfer-of-wealth-in-history; Emil Protalinski, *Google Aurora Attackers Still at Large, Targeting Mainly US Finance, Energy, and Education Companies*, TNW NEWS (Sept. 7, 2012), http://thenextweb.com/insider/2012/09/07/google-aurora-attackers-still-large-targeting-mainly-us-finance-energy-education-companies.

4. *See* 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; Lucian Constantin, *ReVuln Showcases Vulnerabilities in SCADA Software, but Won't Report Them to Vendors*, TECHWORLD (Nov. 22, 2012, 2:30 PM), http://news.

Criminals buy and use weaponized Øday exploits to steal passwords, intellectual property, and other data through computer exploitation attacks. Terrorists or rogue nations can also use weaponized Øday exploits to pose a still greater threat: that of targeting the applications layer of the industrial control systems on which the U.S. electric grid and other critical infrastructure sectors depend. Eric Rosenbach, Deputy Assistant Secretary of Defense for Cyber Policy, recently highlighted the implications of this cyberweapons bazaar for U.S. security. He explained that the black market for Øday exploits and malware tools, combined with the proliferation of programs that scan for vulnerabilities in industrial control systems, are "what worries us the most," because they so dramatically expand the array of adversaries who can acquire cyberweapons and attack America.[5]

The Senate Armed Services Committee deserves great credit for raising the visibility of this proliferating threat and for calling for measures to address it. As of this writing, section 946 of the National Defense Authorization Act for Fiscal Year 2014 recommends that the President "establish an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative export controls, law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate."[6]

Yet it remains wholly unclear how such controls should be structured. At one end of the policy debate, skeptics argue that any effort to curtail the market for weaponized Øday exploits is doomed to fail because these transactions are intangible and extraordinarily difficult to regulate.[7] Regulations may simply drive sellers onto the underground market. They contend that rather than promulgating futile regulations, the international community should learn to "coexist" with this market.[8] This perspective overlooks the severity of the weaponized Øday exploit threat and the imperative to develop innovative measures to curb it.

At the other end of the spectrum, a growing number of cybersecurity experts contend that the companies that write computer software should be held liable

techworld.com/applications/3412614/revuln-showcases-vulnerabilities-in-scada-software-but-wont-report-them-to-vendors.

5. John Reed, *The Cyber Threats Keeping DoD Officials Awake Right Now*, FOREIGN POL'Y (Sept. 13, 2012, 5:35 PM), http://killerapps.foreignpolicy.com/posts/2012/09/13/the_cyber_threat_thats_keeping_dod_officials_awake_right_now.

6. S. 1197, 113th Cong (2013).

7. *See* James Ball, *Secrecy Surrounding 'Zero-day Exploits' Industry Spurs Calls for Government Oversight*, WASH. POST, Sept. 1, 2012, http://www.washingtonpost.com/world/national-security/secrecy-surrounding-zero-day-exploits-industry-spurs-calls-for-government-oversight/2012/09/01/46d664a6-edf7-11e1-afd6-f55f84bc0c41_story_2.html; Paul Rosenzweig, *The Market in Zero-Day Exploits*, LAWFARE (July 14, 2013, 1:27 PM), http://www.lawfareblog.com/2013/07/the-market-in-zero-day-exploits.

8. *See* Ball, *supra* note 7.

for damages caused by exploits since defects in their software created the opportunities for those exploits in the first place.[9] However, substantial legal uncertainties surround efforts to establish this liability regime. Imposing liability on the software industry could also risk unintended economic damage, such as stifling vital innovation and growth of U.S. software companies.

Instead, we recommend three measures to mitigate the threat posed by Øday exploits to national security. We focus on what we perceive to be the greatest danger—that of "weaponized" Øday exploits capable of disrupting control systems for the electric grid and other critical infrastructure sectors. Weaponized Øday exploit attacks against these targets are dangerous because they can physically damage critical infrastructure equipment and disrupt the flow of electricity and other services vital to the economy, public health and safety, and national security.[10] While we are most concerned with Øday exploits that have already been weaponized, our proposals also address sales of exploits that are capable of being weaponized.

First, we propose creating additional incentives for industry to eliminate defects in critical infrastructure industrial control systems and applications layer software. The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (Safety Act) provides an especially promising means to strengthen these incentives.[11] The Safety Act grants providers of anti-terrorism technologies significant third-party liability protections for claims arising out of, relating to, or resulting from an act of terrorism, if the Department of Homeland Security (DHS) first determines that the technology satisfies key security criteria.[12] Although the

9. *See* Tom Espiner, *Expert: Hold Developers Liable for Flaws*, ZDNET (Oct. 14, 2005, 1:37 AM), http://www.zdnet.com/expert-hold-developers-liable-for-flaws-2039278665; Jaikumar Vijayan, *Hold Vendors Liable for Buggy Software, Group Says*, COMPUTERWORLD (Feb. 16, 2010, 12:05 PM), http://www.computerworld.com/s/article/9157218/Hold_vendors_liable_for_buggy_software_group_says.

10. The damage caused by the rupture of a gasoline pipeline owned by Olympic Pipeline Company in Bellingham, Washington—although not caused by a cyberattack—demonstrates the extent of damage that may occur following a weaponized Øday-exploit attack against critical infrastructure ICS. The rupture caused three deaths, multiple injuries, $45 million dollars in damage, significant environmental harm, and the company's bankruptcy. *See* MARSHALL ABRAMS & JOE WEISS, BELLINGHAM, WASHINGTON, CONTROL SYSTEM CYBER SECURITY CASE STUDY (2007), http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf; JOE WEISS, ASSURING INDUSTRIAL CONTROL SYSTEM (ICS) CYBER SECURITY 12 (2008), http://csis.org/files/media/csis/pubs/080825_cyber.pdf.

11. Pub. L. No. 107-296, 116 Stat. 2238.

12. *Frequently Asked Questions*, SAFETY ACT, https://www.safetyact.gov/jsp/faq/samsFAQSearch.do(last visited Oct. 21, 2013).

Safety Act currently includes "software development services" as one of the product categories available for liability protections,[13] the statute must be expanded to cover critical infrastructure industrial control systems (ICS) and applications layer software. We recommend that legislators collaborate with DHS and software companies to adapt current certification criteria and extend Safety Act coverage into this realm. Implementing this proposal would secure critical infrastructure from both weaponized Øday-exploit attacks and other types of malware.

In order to increase the costs associated with selling dangerous Øday exploits to U.S. adversaries, we also recommend that the international community establish uniform export controls for these sales. Through the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, nations should develop criteria for which Øday-exploit sales should be authorized and which should be denied, focusing on the end-use and end-destination of such transactions. While sales of Øday exploits to rogue nations, terrorist organizations, and other entities that target critical infrastructure industrial control systems and their components must be outlawed, sales to software vendors aiming to rectify vulnerabilities should be granted export license exceptions. This multilateral effort would constitute an important first step in establishing international norms on legitimate Øday-exploit purchases.

Finally, it is vital that the United States augment its ability to rigorously prosecute those who sell Øday exploits that target critical infrastructure to U.S. adversaries. If researchers faced a significant risk of prosecution for such sales rather than continuing to enjoy de facto immunity, many would be deterred from conducting these transactions. The Computer Fraud and Abuse Act should be amended to impose an affirmative duty on sellers to conduct due diligence before selling Øday exploits that target U.S. critical infrastructure ICS and their applications layer software.[14] Through this amendment, the United States would be able to prosecute researchers located both domestically and abroad who recklessly sell dangerous exploits to those who harm us.

Part I describes the mechanics of Øday exploits and some important terminology for understanding this threat. Part II provides an overview of the current financial incentives and structure of the global Øday-exploit market and some of the prominent computer firms involved in these transactions. Part III sets forth our three recommendations for addressing this market. Part IV identifies critical policy issues that remain unresolved—most notably, the tradeoffs between curbing the Øday-exploit market and the potential benefits for U.S. agencies to be able to access the unimpeded market that exists today.

13. *The SAFETY Act: Risk Management for Anti-terrorism Products and Services*, SMITH, GAMBRELL & RUSSELL, LLP, http://www.sgrlaw.com/resources/trust_the_leaders/leaders_issues/1343/1347 (last visited Nov. 30, 2013).

14. Further analysis will be needed to determine the precise definition and scope of "targeting" under this amended statute.

I. TERMINOLOGY AND THE MECHANICS OF ØDAY EXPLOITS

Before determining how to regulate and curb the weaponized Øday-exploit market, it is useful to understand the processes of developing and patching Øday exploits, and to know which Øday exploits are most dangerous. This Part therefore provides a broad overview of these mechanics, as well as key terminology.

A "Øday vulnerability" is a weakness in software that is unknown to the software manufacturer.[15] Since code is highly complex and varies significantly among software, each Øday vulnerability is unique.[16] However, since many computer systems deploy the same software, finding a Øday vulnerability in one software program would empower a hacker to penetrate multiple computer systems.

The ethical response to discovering a Øday vulnerability is to report the flaw to the software manufacturer. This is called "responsible disclosure."[17] Once the software vendor learns of the flaw, the company will issue a security patch, which rectifies the vulnerability to prevent future exploitation. Accordingly, the "lifetime" of a Øday vulnerability generally includes (1) the vendor learning of the flaw, (2) the vendor disclosing the nature of the flaw to the public, (3) the vendor releasing a security patch and (4) the patch being downloaded and installed on vulnerable systems.[18] If the Øday vulnerability is especially dangerous, software vendors may patch it before disclosing details of the danger to the public, preventing potential attackers from learning about and exploiting the vulnerability.[19]

As an alternative to engaging in "responsible disclosure," a researcher could instead "exploit" or weaponize the Øday vulnerability, and then sell it to third parties.[20] Some Øday-exploit sales only enable the buyer to gain unauthorized

15. *Vulnerability Trends, supra* note 2.

16. *See* Tim Lloyd, *Israeli Cyber-Security Experts Discuss Zero-Day Exploits, Virtual Money Laundering Techniques*, VENTUREBEAT (June 3, 2013, 1:31 PM), http://venturebeat.com/2013/06/03/israeli-cyber-security-experts-discuss-zero-day-exploits-virtual-money-laundering-techniques. For a discussion of software's complexity, see Gary McGraw, *Software [In]security: Modern Malware*, INFORMIT (Mar. 22, 2011), http://www.informit.com/articles/article.aspx?p=1695979.

17. MICHAEL SUTTON & FRANK NAGLE, EMERGING ECONOMIC MODELS FOR VULNERABILITY RESEARCH 16 (2006), http://weis2006.econinfosec.org/docs/17.pdf.

18. LEYLA BILGE & TUDOR DUMITRAS, BEFORE WE KNEW IT: AN EMPIRICAL STUDY OF ZERO-DAY ATTACKS IN THE REAL WORLD 3 (2012), http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf.

19. *See, e.g.*, ANDREW CENCINI ET AL., SOFTWARE VULNERABILITIES: FULL-, RESPONSIBLE-, AND NON-DISCLOSURE 26 (2005), http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf.

20. SUTTON & NAGEL, *supra* note 17, at 15; *see* BILGE & DUMITRAS, *supra* note 18, at 3.

access to a computer system and become its "administrator." Other Øday exploits are "weaponized," or mated with a launch pad, like a botnet, to cause the computer system to malfunction.[21]

Transforming the vulnerability into a weaponized exploit may require significant investments of time, money, and resources. Experts estimate that the time required for the discovery, design, and weaponization can often exceed five hundred days, depending on the sophistication of the weaponized exploit.[22] Furthermore, after researchers turn a Øday vulnerability into a weaponized exploit, they often spend ample time testing the exploit to ensure that it will penetrate or attack its target covertly.[23]

Øday exploits are dual-use.[24] They can be deployed by good-willed researchers to test computer systems for vulnerabilities and therefore safeguard systems against attacks.[25] However, they can also be deployed to gather sensitive commercial or intelligence information, incapacitate computer systems, or inflict widespread physical damage. For example, a weaponized Øday exploit targeting the air-traffic control system could send false signals to planes in the air, causing them to crash or collide.[26] Department of Transportation audits have confirmed that the U.S. air-traffic control system remains highly vulnerable to cyberattacks.[27] An attack on the electric grid could leave entire regions of the country in the dark for weeks, incapacitating the economy and resulting in numerous casualties.[28]

---

21. A botnet is a network of computers that are taken over by an attacker remotely and ordered to perform certain functions. Dennis Fisher, *What is a Botnet?*, KASPERSKY LAB (Apr. 25, 2013), http://blog.kaspersky.com/botnet.

22. SANDRO GAYCKEN & FELIX F.X. LINDNER, ZERO-DAY GOVERNANCE: AN (INEXPENSIVE) SOLUTION TO THE CYBER-SECURITY PROBLEM (2012), http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf.

23. *Id.*

24. Ryan Gallagher, *Cyberwar's Gray Market*, SLATE (Jan. 16, 2013, 9:00 AM), http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html.

25. *Id.*

26. *See* Paul Marks, *Air Traffic System Vulnerable to Cyber Attack*, NEW SCIENTIST (Sept. 12, 2011), http://www.newscientist.com/article/mg21128295.600-air-traffic-system-vulnerable-to-cyber-attack.html#.UpVulmTk80M.

27. *See* David Perera, *FAA Air Traffic Control Systems Open to Possible Cyber Attack, Says IG*, FIERCEGOVERNMENTIT (Sept. 7, 2010), http://www.fiercegovernmentit.com/story/faa-air-traffic-control-systems-open-possible-cyber-attack-says-ig/2010-09-08.

28. *See* Antone Gonsalves, *Damage From Attack on Power Grid Would Surpass Sandy*, CSO MAG. ONLINE (Nov. 29, 2012), http://www.csoonline.com/article/722579/damage-from-attack-on-power-grid-would-surpass-sandy.

As the threats to the air-traffic control system and electric grid make clear, the most potent and dangerous Øday-exploit attacks are those that target the nation's "critical infrastructure" sectors. The 2013 Presidential Policy Directive on Critical Infrastructure Security and Resilience defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[29] The air-traffic control system and other transportation systems are considered critical infrastructure, along with the chemical, communications, emergency services, financial, water, power, and nuclear reactor sectors.[30]

A high percentage of America's critical infrastructure is owned and operated by private civilian companies.[31] These companies generally operate and monitor critical infrastructure by relying on industrial control systems (ICS), including Supervisory Control and Data Analysis (SCADA) systems, distributed-control systems, and programmable-logic controllers.[32] These systems enable companies to open and shut water pump valves, react to pressure, and change volume levels automatically and remotely.[33] As technology has evolved, companies have sought to improve operational efficiency by designing ICS systems that are Internet compatible.[34] Internet connectivity has rendered these systems and their applications layer much more susceptible to Øday-exploit attacks since perpetrators can access and penetrate them more easily.[35] Today's Øday-exploit attacks are especially targeted at the vulnerable applications layer.[36]

29. Directive on Critical Infrastructure Security and Resilience, 2013 DAILY COMP. PRES. DOC. 92 (Feb. 12 2013).

30. *Critical Infrastructure Sectors*, U.S. DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/critical-infrastructure-sectors (last visited May 15, 2013).

31. Glenn Derene, *How Vulnerable is U.S. Infrastructure to a Major Cyber Attack?*, POPULAR MECHANICS (Oct. 1, 2009, 12:00 AM), http://www.popularmechanics.com/technology/military/4307521.

32. *ICS: Industrial Control Systems Security*, SANS ICS, http://ics.sans.org/ (last visited Oct. 19, 2013).

33. *See* WEISS, *supra* note 10; William T. Shaw, *SCADA System Vulnerabilities to Cyber Attack*, ELECTRIC ENERGY ONLINE, http://www.electricenegyonline.com/?page=show_article&article=181 (last visited May 16, 2013).

34. *See Cyber Threats to SCADA Networks*, UNICRI, http://www.unicri.it/special_topics/cyber_threats/cyber_crime/explanations/scada (last visited May 15, 2013); *Save Money with Innovative SCADA Solutions*, INDUS. CONTROL LINKS, http://www.iclinks.com/SCADA-Value (last visited Nov. 23, 2013).

35. *Cyber Threats*, *supra* note 34.

36. *See* SECUNIA, SECUNIA VULNERABILITY REVIEW 2013: KEY FIGURES AND FACTS FROM A GLOBAL IT-SECURITY PERSPECTIVE 5 (2012), http://secunia.com/?action=fetch&filename=Secunia_Vulnerability_Review_2013.pdf; SYMANTEC, INTERNET SECURITY

In spite of this increased threat, private companies have failed to adequately invest in cyber measures to secure critical infrastructure from attack. The government has also failed to provide sufficient support to private companies to safeguard the nation's critical infrastructure. According to the Department of Homeland Security's recent Inspector General Report, the United States Computer Emergency Readiness Team (US-CERT) is "understaffed" and lacks the legal authority to require private companies to implement stronger protections against cyber intrusions.[37]

II. The Market for Øday Exploits

The market for Øday exploits has "exploded" in recent years due to the rise of cybercrime and nations' increased recourse to offensive cyber operations and cyber espionage.[38] In the past, computer researchers voluntarily reported vulnerabilities in software that they discovered to software vendors. Vendors therefore lacked the incentive to pay researchers for their discoveries and instead publicly acknowledged them when issuing security patches or organized events honoring them for their work.[39] Today, while public recognition or benevolence may persuade some researchers to report their findings to software vendors, many are instead motivated by the substantial profits available by selling their discoveries to governments and other customers with "deeper pockets."[40]

The Øday-exploit market currently consists of three categories: the white market, in which so-called "white-hat" vulnerability researchers sell Ødays to software vendors or other companies that help the developers rectify security flaws; the black market, where researchers sell Øday exploits, often in weaponized form, to criminal organizations; and the intermediate "gray market," where researchers sell Øday exploits, also frequently in weaponized form, to government agencies and other buyers seeking to deploy them for offensive purposes.[41]

THREAT REPORT APPENDIX 87 (2013), http://docsforssl.com/docs/symantec/b-istr_appendices_v18_2012_221284438.en-us.pdf.

37. *The Unreadiness Team*, WASH. POST, June 20, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/19/AR2010061902645.html.

38. *See* Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012, 9:43 AM), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits; *Zero-Day Market, the Governments are the Main Buyers*, SECURITY AFF. (May 21, 2013), http://securityaffairs.co/wordpress/14561/malware/zero-day-market-governments-main-buyers.html.

39. SUTTON & NAGEL, *supra* note 17, at 12-17.

40. Greenberg, *supra* note 38.

41. Robert Lemos, *Private Market Growing for Zero-Day Exploits and Vulnerabilities*, SEARCHSECURITY.COM, http://searchsecurity.techtarget.com/feature/Private-market-growing-for-zero-day-exploits-and-vulnerabilities (last visited Nov. 30, 2013).

In response to the compensation offered to vulnerability researchers by other buyers, software companies were induced to begin paying researchers for their discoveries in the white market—either through direct payments or exploit competitions.[42] For example, the Zero Day Initiative is a program designed to reward security researchers for "responsible disclosure" of flaws to software vendors.[43] Recently, Facebook and Microsoft collaborated to create "HackerOne," a bug bounty initiative that offers researchers $300 to $5,000 for a given vulnerability.[44]

Yet most software vendors still provide inadequate compensation to compete with buyers in the gray and black markets.[45] For example, a researcher or firm could sell a newly discovered exploit to a software company in the white market for approximately $300 to $5,000, or it could earn "10 or even 100 times" that amount by selling the exploit to a government agency or criminal organization.[46] White-hat researchers are therefore motivated not only by financial compensation but also by morals.[47]

In stark contrast to the white market, there is an anarchic black market for Øday exploits where vulnerability researchers often sell exploits to criminal hackers, terrorist organizations, and rogue nations. Vulnerability researchers have described this market as a "Wild West, where legality is rarely of paramount importance."[48] The transactions occur in "invite-only" chat rooms, in which researchers sell weaponized exploit toolkits to the highest-paying buyer.[49] According to Deputy Assistant Secretary of Defense for Cyber Policy Eric Rosenbach, the black market is facilitated by recently developed Google-like search engines, which enable users to locate computer systems connected to the Internet and find software weaknesses.[50] Many of the websites used for these transactions,

42. *Id.*

43. *Id.*; *Why Did We Create the Zero Day Initiative?*, ZERO DAY INITIATIVE, http://www.zerodayinitiative.com/about (last visited Feb. 1, 2013).

44. Stephanie Mlot, *Facebook, Microsoft Launch Internet Bug Bounty Program*, PC MAG. (Nov. 7, 2013, 3:20 PM), http://www.pcmag.com/article2/0,2817,2426877,00.asp?mailingID=64A8C50555E08B19EEF2B55C437F5E32.

45. *See* Taylor Armerding, *Facebook Locks in on Bounties for Security*, NETWORKWORLD (June 5, 2012, 7:37 AM), http://www.networkworld.com/news/2012/060412-facebook-locks-in-on-bounties-259854.html?page=1; Lemos, *supra* note 41.

46. *See* SUTTON & NAGEL, *supra* note 17, at 12; Greenberg, *supra* note 38; Mlot, *supra* note 44.

47. *See* Lemos, *supra* note 41.

48. Gallagher, *supra* note 24.

49. Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, BLOOMBERG BUSINESSWEEK (July 20, 2011), http://www.businessweek.com/printer/articles/540-cyber-weapons-the-new-arms-race.

50. Reed, *supra* note 5.

such as the "Silk Road" website recently shut down by the FBI, are located on the underground "Deep Web" and concealed from traditional search engines.[51]

In between the white and anarchic black markets for Øday exploits, there is an unregulated, burgeoning gray market, where bona fide companies sell Øday exploits to government agencies and other unreported customers.[52] Many of these companies serve as brokers—they purchase Øday exploits from outside researchers and then resell them to customers at higher prices.[53] Other gray market firms develop and weaponize Øday exploits "exclusively from in-house research efforts."[54]

The largest customers include the U.S. government and other nations' government agencies, which are often willing to expend $250,000 for a single Øday exploit.[55] The *Washington Post* reported that the U.S. National Security Agency spent $25 million on exploit purchases in 2013 alone.[56] U.S. law enforcement agencies frequently purchase Øday exploits to disrupt criminal operations and "sneak spy software onto suspects' computers or mobile phones."[57] Other prominent buyers allegedly include the governments of Brazil, Britain, India, Israel, Malaysia, North Korea, Russia, and Singapore.[58] Governments and other clientele that purchase vulnerability information in the gray market often seek to exploit the information for offensive operations or espionage missions. Therefore, although it would be in civilian computer users' best interest to disclose the vulnerability to software vendors so that they could issue patches, intelligence agencies

51. Ryan W. Neal, *What You Need to Know About the Silk Road Black Market*, DAILYFINANCE (Oct. 3, 2013, 11:40 AM), http://www.dailyfinance.com/2013/10/03/silk-road-black-market-deep-web-site-what-to-know.

52. *See* Gallagher, *supra* note 24.

53. Aarti Shahani, *Hacking and the Value of a Zero Day*, MARKETPLACE TECH (Oct. 7, 2013), http://www.marketplace.org/topics/tech/hacking-and-value-zero-day#story-content.

54. *Vupen Exclusive & Sophisticated Exploits for Offensive Security*, VUPEN SECURITY, http://www.vupen.com/english/services/lea-index.php (last visited Oct. 10, 2013).

55. Greenberg, *supra* note 38; *see Zero-Day Market*, *supra* note 38.

56. 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.

57. Nick Farrell, *Zero-Day Black Market Bolstered by 'Malware Industrial Complex,'* TECHEYE.NET (Feb. 14, 2013, 11:06 AM), http://news.techeye.net/security/zero-day-black-market-bolstered-by-malware-industrial-complex; *see* Shahani, *supra* note 53.

58. Perlroth & Sanger, *supra* note 4.

withhold the information from the public.[59] Such policies have unleashed widespread criticism, with many condemning Øday-exploit sales as "security for the 1%."[60]

However, the more grave concern is that in the absence of market regulation, bona fide companies are legally selling weaponized Øday exploits to rogue governments and other entities seeking to harm the United States and its allies.[61] For example, the Malta-based company ReVuln advertises that it discovers and sells weaponized Øday exploits that allow attackers to "remotely execute arbitrary code, download arbitrary files, execute arbitrary commands, open remote shells or hijack sessions on systems running the vulnerable SCADA software."[62] The company, whose motto declares "invincibility lies in the defense[,] the possibility of victory in the attack," operates legally and is registered at the Malta Registry of Companies.[63] ReVuln sells to "world-wide" customers and the company's cofounder, Donato Ferrante, openly acknowledges, "I don't see bad guys or good guys . . . [i]t's just business."[64] He contends that his firm cannot be held accountable for cyberattacks because it merely sells information and "the way the information is used is up to the customer; it's not up to us."[65] The company purportedly sells Øday exploits that target ICS software used by General Electric, Schneider Electric, Siemens, and many major U.S. critical infrastructure sectors.[66] On its website, the company boasts that one of its senior researchers has discovered the greatest number of security vulnerabilities in SCADA software.[67]

Another high-profile company operating in the gray market is the French-based Vupen. Although Vupen at least restricts its sales to NATO nations or allies that are not subject to United States, European Union, or United Nations sanctions,[68] this screening policy is still far too lenient to safeguard critical U.S. infrastructure from attack. Under its policy, nations such as Russia, Kazakhstan, and

59. *See* Dan Auerbach & Lee Tien, *Dangerously Vague Cybersecurity Legislation Threatens Civil Liberties*, ELEC. FRONTIER FOUND. (March 20, 2012), https://www.eff.org/deeplinks/2012/03/dangerously-vague-cybersecurity-legislation.

60. *Id.*

61. Gallagher, *supra* note 24.

62. Constantin, *supra* note 4.

63. REVULN, http://revuln.com/about.php?id=company (last visited Mar. 15, 2013).

64. Tom Gjelten, *In Cyberwar, Software Flaws Are a Hot Commodity*, NPR NEWS (Feb. 12, 2013, 3:25 AM), http://www.npr.org/2013/02/12/171737191/in-cyberwar-software-flaws-are-a-hot-commodity.

65. *Id.*

66. Constantin, *supra* note 4.

67. REVULN, *supra* note 63.

68. Mike Wheatley, *NSA Keeps Its Hands Clean, Buys Zero-Day Vulnerabilities from French Firm Vupen*, SILICONANGLE (Sept. 18, 2013), http://siliconangle.com/blog/2013/09/18/nsa-keeps-its-hands-clean-buys-zero-day-vulnerabilities-from-

Bahrain can purchase weaponized Øday exploits,[69] even though the Russian government is a leading sponsor and perpetrator of cyberattacks against other nations. Even though Vupen's screening protocols officially preclude direct sales to countries like Iran or North Korea, Vupen's customers could foreseeably resell weaponized Øday exploits to rogue nations seeking to harm America.[70] Critics have therefore condemned the company for being the "modern-day merchants of death" and selling "the bullets for cyberwar."[71]

III. Addressing the Øday-Exploit Market

To help guide U.S. policymakers as they consider how to address the threat of weaponized Øday exploits to critical infrastructure, we propose a three-pronged strategy. First, the United States should address the threat's root cause by incentivizing developers of critical infrastructure ICS and applications layer software to enhance their products' security. To ensure that efforts to augment software security do not inadvertently stifle innovation, Congress should amend the Safety Act to extend coverage for developers of critical infrastructure ICS and applications layer software. Second, the international community should develop criteria for "illegitimate" Øday-exploit sales and establish uniform export controls through the Wassenaar Arrangement. Finally, the United States should strengthen its capacity to prosecute individuals who sell Øday exploits targeting critical infrastructure to U.S. adversaries.

A. Leveraging the Safety Act to Incentivize Software Security and Innovation

A robust solution to the cyber threat must entail improving the security of critical infrastructure ICS and applications layer software. Investing in stronger security would undermine researchers' ability to discover and weaponize Ødays to inflict widespread destruction.[72]

Some security experts and scholars argue that, in order to strengthen incentives for software companies to invest in this fashion, software companies should be held liable when their products are compromised.[73] Proponents of this ap-

---

french-firm-vupen; *see* Matthew J. Schwartz, *NSA Contracted With Zero-Day Vendor Vupen*, INFORMATIONWEEK (Sept. 17, 2013, 10:19 AM), http://www.informationweek.com/security/government/nsa-contracted-with-zero-day-vendor-vupe/240161389.

69. Gallagher, *supra* note 24.

70. *Id.*

71. *Id.*

72. *Id.*

73. *See* Kevin R. Pinkney, *Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43, 82 (2002); Frances E. Zollers et al., *No More Soft Landings for Software: Liability*

proach reason that although software insecurity is the "root cause" of all cyberattacks, software companies currently evade all liability by including standard exculpatory clauses in their contracts with consumers.[74] Most other industries that manufacture potentially dangerous products, including the car and toy manufacturing industries, are frequently held liable when defects in their products inflict harm.[75] If developers of critical infrastructure ICS and applications layer software also feared confronting a multi-billion dollar lawsuit following a cyberattack, they might be compelled to invest in stronger security.

However, it is uncertain whether extending liability to such companies is feasible, much less desirable. Companies may not fear liability because they may frequently succeed at undermining plaintiffs' prima facie case that their products "caused" the damage resulting from cyberattacks.[76] A cyberattack against critical infrastructure involves a number of diverse and potentially culpable parties, including the attacker, the developers of the weaponized Øday exploit, the hardware designer, the software developer, the vendors, and the maintainers of critical infrastructure.[77] Developers of critical infrastructure ICS and applications layer software could therefore contend, for example, that a cyberattack succeeded not because their software was defective, but rather because of the maintainer's negligence.

In addition to these challenges, our particular concern is that initiatives to enhance software security must not stifle innovation. If writing software exposed programmers to liability, they would be reluctant to risk developing newer, and potentially better, products.[78] Developing new software would be especially risky

---

for Defects in an Industry That Has Come of Age, 21 SANTA CLARA COMP. & HIGH TECH. L.J. 745, 746 (2005); Bruce Schneier, *Liability and Security*, CRYPTO-GRAM NEWSL. (Apr. 15, 2002), https://www.schneier.com/crypto-gram-0204.html; Vijayan, *supra* note 9.

74. *See* Reid Skibell, *The Phenomenon of Insecure Software in A Security-Focused World*, 8 J. TECH. L. & POL'Y 107, 124-25 (2003); David Banisar, *Save the Net, Sue a Software Maker*, SECURITYFOCUS (Dec. 17, 2001), http://www.securityfocus.com/columnists/47; Jonathan Dowdall, *Florian Walther's One-Shot Cyber-Security Solution*, POLICYMIC (Nov. 24, 2011), http://www.policymic.com/articles/2566/florian-walther-s-one-shot-cyber-security-solution.

75. *See* Banisar, *supra* note 74.

76. For an analysis of available defenses to strict products liability claims, see in general Gary D. Spivey, *Products Liability: Contributory Negligence or Assumption of Risk as Defense Under Doctrine of Strict Liability in Tort*, 46 A.L.R.3d 240 (1972).

77. *See* Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 328-29 (2006).

78. TYLER MOORE, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACK: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 10 (2010).

because, due to software's complexity, "vulnerabilities are inherently embedded in software architecture."[79]

To incentivize industry without risking adverse effects on software innovation, we propose that developers of critical infrastructure ICS and applications layer software should have the opportunity to receive liability protections under an amended version of the Safety Act. Congress enacted the Safety Act following September 11th to ensure that liability concerns would not deter companies from developing technologies that mitigate the consequences of terrorism.[80] In exchange for demonstrating that their "anti-terrorism" products are highly safe and effective, companies may receive significant liability protections.[81] Protection varies depending on whether products receive "designation" or "certification" as Qualified Anti-Terrorism Technology (QATT). For example, QATT "designation" provides companies with a liability cap in the event of a terrorist event, assurance of exclusive action in federal court, and protection from punitive damages and joint and severable liability.[82] Applicants must purchase liability insurance in the amount of the liability cap determined by DHS.[83] If companies satisfy a higher safety threshold and receive "certification" as QATT, DHS immunizes them from all liability in terrorist-related claims.[84]

A few law firms and policymakers have recently recommended leveraging the Safety Act to incentivize companies to strengthen their cybersecurity.[85] However, they have failed to consider the importance of extending Safety Act coverage to developers of critical infrastructure ICS and applications layer software. Under current law, only "anti-terrorism" technologies—defined as technologies "designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism"—are eligible for liability protections.[86] Since the primary purpose of critical infrastructure ICS and applications layer software is to operate and monitor critical infrastructure equipment, such software would not qualify for coverage. Given that this software's

79. Taiwo A. Oriola, *Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities*, 28 J. MARSHALL J. COMPUTER & INFO. L. 451, 465-67 (2011).

80. *Frequently Asked Questions*, *supra* note 12.

81. *Id.*

82. *Id.*

83. *Id.*

84. *Id.*

85. *See, e.g.*, Rachel King, *Companies Look to Safety Act to Limit Legal Liability in Cyber Attacks*, WALL. ST. J. (May 2, 2013, 9:16 PM), http://blogs.wsj.com/cio/2013/05/02/companies-look-to-safety-act-to-limit-legal-liability-in-cyber-attacks; *Cyber Sticks and Carrots: How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You*, VENABLE, LLP (Sept. 25, 2013), http://www.venable.com/cyber-sticks-and-carrots—how-the-nist-cybersecurity-framework-incentives-and-the-safety-act-affect-you-09-25-2013.

86. *Frequently Asked Questions*, *supra* note 12.

security is just as vital to the nation's ability to defend against cyberterrorism, its developers should also be able to utilize the statute's safety incentives. To achieve this goal, one approach would be for DHS to collaborate with the software industry and the National Institute of Standards and Technology (NIST) to develop "safety" benchmarks for determining whether applicants' software warrants protection.[87]

In addition to receiving liability protections, developers of critical infrastructure ICS and applications layer software that invest in security and receive Safety Act approval will also benefit from strengthened brand image. They will be able to place a DHS-approved Safety Act seal on their software, informing customers that DHS conducted a comprehensive review and determined that their software is "effective, reliable, and safe."[88] The seal will be a substantial "market differentiator" because it will guarantee that the software company is the only "entity that may be sued for damages to third parties."[89] Critical infrastructure owners who purchase the software will be immune from liability.[90] With such marketing benefits, many software companies would be enticed to invest in security and apply for Safety Act coverage. Incentivizing investments in security would help mitigate the threats posed by both weaponized Øday exploits and other types of malware to critical infrastructure.

Although inducing software companies to invest in stronger safety would reduce defects and make it harder to discover and weaponize Øday exploits, latent vulnerabilities would inevitably remain. Therefore, efforts to expand the Safety Act to promote security must be accompanied by robust efforts at the international and domestic levels to regulate Øday-exploit sales targeting critical infrastructure. We turn next to demonstrating how multilateral export controls adopted through the Wassenaar Arrangement, and subsequently implemented at the domestic level, could raise the costs of selling dangerous Øday exploits while permitting white-hat researchers to continue to operate.

87. In Executive Order 13636, President Obama assigned NIST to collaborate with key stakeholders to develop a voluntary framework for addressing cybersecurity threats to critical infrastructure. NIST has convened multiple workshops to achieve this objective and released a Preliminary Cybersecurity Framework, which can help guide the development of Safety Act benchmarks. *See Cybersecurity Framework*, NIST (Feb. 12, 2013), http://www.nist.gov/itl/cyberframework.cfm.

88. *See Safety Act Certified*, PREPARED RESPONSE, INC., http://www.preparedresponse.com/DHS-SAFETY-Act.html (last visited Sept. 1, 2013); *Safety Act*, HUNTON & WILLIAMS LLP, http://www.hunton.com/SAFETY_Act (last visited Sept. 1, 2013).

89. Dismas Locaria, *SAFETY Act: A Cybersecurity Win-Win For Gov't, Industry*, LAW360 (Apr. 24, 2013, 3:20 PM), http://www.law360.com/articles/435580/safety-act-a-cybersecurity-win-win-for-gov-t-industry; *see Frequently Asked Questions*, *supra* note 12.

90. *Id.*

B. *Implementing Domestic and International Export Controls of Øday Sales through the Wassenaar Arrangement*

Instituting export controls for Øday-exploit sales—and thus requiring certain gray market sellers of dangerous exploits to obtain licenses from the Department of Commerce—would provide another hurdle to selling dangerous exploits to those seeking to target the United States. As of this writing, section 946 of the proposed National Defense Authorization Act for Fiscal Year 2014 (NDAA) envisions establishing such export controls to curb the proliferation of cyberweaponry.[91]

Yet before export controls are established, there must be criteria for determining which sales should be authorized and which should be denied. This is crucial because given the dual-use nature of Øday exploits, not all sales should be prevented. Sales by white-hat researchers for purely "defensive purposes" should not be subject to the same stringent controls as those designed to incapacitate critical infrastructure systems. Indeed, the Senate Armed Services Committee acknowledges in its accompanying report to the NDAA that there is a need to develop "definitions and categories for controlled cyber technologies" that can guide export controls.[92]

While the proposed NDAA requires establishing an interagency process to identify which types of cyberweapons sales should be controlled either "unilaterally or cooperatively with other countries," we believe that developing this list multilaterally is the only viable option.[93] The "Wild West" market for Øday exploits transcends national boundaries. A unilateral American effort to develop a list of "acceptable" and "unacceptable" transactions would provoke backlash and fail to secure much-needed international support.

We therefore recommend that the United States collaborate with the international community to develop export control criteria through the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.[94] Established in 1996, the Wassenaar Arrangement is a multilateral export control regime that aims to "contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus

91. *See* National Defense Authorization Act for Fiscal Year 2014, S. 1197, 113th Cong (2013).

92. *Id.*

93. *Id.*

94. *See* David Fidler, *Zero-Sum Game: The Global Market for Software Exploits*, ARMS CONTROL L. (July 18, 2013), http://armscontrollaw.com/tag/zero-day-exploits.

preventing destabilizing accumulations."[95] The arrangement, which currently includes forty-one member nations,[96] strives to achieve this objective by establishing uniform "control lists" of dual-use technologies, sharing information on dual-use transfers, and consulting with members on national export policies and denials of export license applications.[97] Members compile the control lists collectively and are encouraged to implement corresponding controls through domestic export licenses.[98]

A key benefit of utilizing the Wassenaar Arrangement to curb dangerous Øday exploit sales is that nations would be able to address this rapidly proliferating market much more quickly than if they had to enter into a new cyberspace arrangement. Entering into a new cyberspace agreement would involve significant political and organizational hurdles and may take years to operationalize.[99] With the Wassenaar Arrangement, the infrastructure, procedures, and guidelines are already in place to create uniform export controls on dangerous Øday exploits.

Furthermore, the Wassenaar Arrangement already provides for controls of "intangible technology," which members have agreed are "critical to the credibility and effectiveness of [a Participating State's] domestic export control regime."[100] The Arrangement defines "intangible technology" as "specific information necessary for the 'development,' 'production' or 'use' of a product," including "technical data or technical assistance."[101] Selling technical knowledge on how to exploit vulnerabilities in computer software aptly falls under this definition.[102]

---

95. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Initial Elements, § I.1, July 12, 1996, http://www.wassenaar.org/docs/IE96.html; *Introduction*, WASSENAAR ARRANGEMENT, http://www.wassenaar.org/introduction/index.html (last visited Sept. 3, 2013).

96. *Frequently Asked Questions*, WASSENAAR ARRANGEMENT, http://www.wassenaar.org/faq (last visited Nov. 28, 2013).

97. Jamil Jaffer, *Strengthening the Wassenaar Export Control Regime*, 3 CHI. J. INT'L L. 519, 520 (2002).

98. *See* Lillian V. Blageff, *Nonproliferation Export Controls on Weapons of Mass Destruction and Related Technologies*, 22 INT'L Q. (2010).

99. *See* James Lewis, *A Cybersecurity Treaty Is a Bad Idea*, U.S. NEWS & WORLD REP. (June 8, 2012), http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/a-cybersecurity-treaty-is-a-bad-idea.

100. *Best Practices for Implementing Intangible Transfer of Technology Controls*, WASSENAAR ARRANGEMENT (2006), http://www.wassenaar.org/guidelines/docs/ITT_Best_Practices_for_public_statement.pdf.

101. *Id.*

102. Ødays are often comprised of changeable code that is uninstantiated, meaning that it contains "data whose storage type and values are unknown." *See What Is Instantiation?*, IBM, http://pic.dhe.ibm.com/infocenter/spssmodl/v15romo/index.jsp

As Wassenaar members develop criteria for export controls of Ødays, we strongly recommend that they focus on the exploit's end-use, end-purchaser, and country of destination. Although sales of dangerous exploits to terrorist organizations, rogue states, and other entities seeking to target critical infrastructure must be denied, controls must not impede legitimate white-hat researchers from selling exploits to software vendors.

The United States should implement the Wassenaar Arrangement's recommended exploit controls through its Commerce Control List (CCL).[103] Since Øday exploits would constitute "controlled items" and receive an Export Classification Number, sellers would need to apply for licenses with the Department of Commerce's Bureau of Industry and Security (BIS).[104] To ensure that this licensing regime does not impose excessive regulatory burdens on white-hat researchers, BIS should create and make available a license exception to those who export exploits to software vendors and other categories of pre-authorized entities in approved countries of destination.[105] Sellers with license exceptions would still be responsible for conducting due diligence and screening end-users. If they failed to do so, they would be subject to substantial administrative or criminal penalties.[106] Nevertheless, an export exception would enable them to sell their discoveries to vendors quickly, thereby minimally impacting their business operations and facilitating timely security patches.

In addition to enumerating specific categories of Øday exploits on the Wassenaar Arrangement's and CCL's controlled items lists, member nations could

---

?topic=%2Fcom.ibm.spss.modeler.help%2Ftypenode_instantiation.htm (last visited Oct. 19, 2013). They are difficult to characterize, particularly when mated with launch pads. Since the Wassenaar Arrangement defines intangible technology in terms of technical data that is instantiated and can be verified, further analysis will be needed to determine how to apply its controls to Ødays. However, the fact that the Arrangement already governs certain code and encryption software indicates that such application is feasible. *See* Mark T. Pasko, *Re-Defining National Security in the Technology Age: The Encryption Export Debate*, 26 J. LEGIS. 337, 341-42 (2000).

103. For an overview of the Commerce Control List, see *Overview of U.S. Export Control System*, U.S. DEP'T STATE, http://www.state.gov/strategictrade/overview/ (last visited Sept. 11, 2013).

104. *See* 5 C.F.R. § 732.1 (2012); Jordan Collins, *Same Laws, Different Century: The Bureau of Industry & Security's Role in Global Trade & National Security*, 15 CURRENTS: INT'L TRADE L.J. 108, 110 (2006).

105. "Pre-authorized entities" may include certain governments. For further analysis, see *infra* Part IV. For a detailed analysis of how export control exceptions may reduce regulatory barriers in other contexts, see Joseph A. Schoorl, *Clicking the "Export" Button: Cloud Data Storage and U.S. Dual-Use Export Controls*, 80 GEO. WASH. L. REV. 632, 642-52 (2012). *See also* 15 C.F.R. § 740 (2013).

106. Telephone Interview with Robert Shaw, Exp. Instructor, Monterey Inst. of Int'l Studies (Oct. 7, 2013).

also curb dangerous sales through export "catch-all" provisions.[107] These provisions are defined as controls that "provide a legal and/or regulatory basis to require government permission to export unlisted items when there is reason to believe such items are intended for a WMD/Missile end-use or end-user."[108] Due to the rapidly evolving nature of technologies and discoveries of new vulnerabilities, the international community may be unable to immediately incorporate newly discovered Ødays into their control lists. A catch-all provision for dangerous cyberweaponry sales would therefore provide a critical safety net in the Øday-exploit context.[109]

Some might counter that it is impractical to control "intangible" data transfers like Øday exploits. However, the government has successfully limited exports of dangerous technical data for years under the Export Administration Regulations (EAR) and International Traffic in Arms Regulations.[110] It is indisputable that it has the statutory authority to regulate information that can be deployed in the "development," "production," or "use" of prohibited defense materials.[111] For

107. Catch-all provisions are similar to export license exceptions. If the exporter possesses "knowledge or reason-to-know that an otherwise uncontrolled item will support a proscribed end-use, then the exporter must apply for an export license, regardless of the technical characteristics of the item." *Id.*

108. *Catch-All Controls*, U.S. DEP'T STATE, http://www.state.gov/strategictrade/practices/c43179.htm (last visited Oct. 2, 2013).

109. *Public Statement*, WASSENAAR ARRANGEMENT (Dec. 12, 2002), http://www.wassenaar.org/publicdocuments/2002/public121202.html; Toli Welihozkiy, *Catch-All Controls*, U.S. DEP'T ENERGY, http://www.paei.org/07BuildingWeaponsofMassDestruction/04Catch-AllControls.pdf (last visited Sept. 29, 2013). For current "catch-all" provisions in the EAR, see 15 C.F.R. §§ 744.2, .3, .4 (2012); *Overview of U.S. Export Control System*, U.S. DEP'T STATE 19-21, http://www.state.gov/strategictrade/overview (last visited Sept. 11, 2013). Effective enforcement of catch-all provisions will require strong collaboration between intelligence agents and law enforcement officials. They will need to collect sufficient evidence to demonstrate that the exporter knew or had reason to know that the exploit would be deployed for a prohibited end-use. *See* Telephone Interview with Robert Shaw, *supra* note 106.

110. *See* Robert A. Borich Jr., *Globalization of the U.S. Defense Industrial Base: Developing Procurement Sources Abroad Through Exporting Advanced Military Technology*, 31 PUB. CONT. L.J. 623, 641-43 (2002); Collins, *supra* note 104, at 110-11; Pasko, *supra* note 102, at 337, 350.

111. 15 C.F.R. § 772.1 (2012). "Technical data" subject to export controls may take "a tangible form, such as a model, prototype, blueprint, or an operating manual" or an "intangible form such as technical services." *Id.* The Arms Export Control Act provides the President with the power, "in furtherance of world peace and the security and foreign policy of the United States . . . to control the import and the export of defense articles" and related services, including dangerous technical data. *See* 22 U.S.C.A. § 2778 (a) (1) (West 2012); United States v. Edler Indus., Inc., 579

example, pursuant to these statutes, the government prevents individuals and universities from training or sharing information with foreigners on how to develop a nuclear weapon, missiles, and other dangerous technologies.[112] The "intangible" electronic or digital transmission of "blueprints, diagrams, manuals, instructions, [and] software" related to controlled items is also forbidden.[113] BIS would be able to deploy the same procedures to control information transfers regarding exploiting vulnerabilities in our nation's computer systems.

We concede that using the Wassenaar Arrangement to develop uniform export controls for cyberweaponry is far from a panacea. The Wassenaar Arrangement is voluntary and lacks strong compliance monitoring and enforcement measures. Even if the United States changed its CCL to correspond with the Wassenaar Arrangement's controlled items list for cyberweapons, other participating nations may not follow suit. Even if they did, they may lack the capability to enforce export laws on Øday-exploit sales. Although the United States and other nations routinely enforce export controls of other dangerous data, given the intangible nature of such transactions, enforcement is often very challenging. Since the market is largely anonymous and geographically independent, export controls may simply drive many sellers underground.

A significant limitation of this proposal is that some major purchasers of cyberweaponry and perpetrators of cyberattacks, including China, are not members of the Wassenaar Arrangement.[114] Given that China is rapidly becoming one of the most powerful players on the world stage and is a "prolific" sponsor of cyber espionage, it would be vital to engage China in this initiative.[115] Fortunately, China has made progress in adhering to the international norms and standards of other nonproliferation regimes, including the Nuclear Suppliers Group.[116] Furthermore, since 2004, the Wassenaar Arrangement has held five rounds of dialogue with China on export controls for dual-use technologies.[117] Wassenaar

---

F.2d 516, 520 (9th Cir. 1978); Elizabeth Lauzon, *The Philip Zimmermann Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues*, 48 SYRACUSE L. REV. 1307, 1349 (1998).

112. *See Summary of Federal Laws: Export Administration Act (EAA) and the Arms Export Control Act (AECA)*, CATH. UNIV., http://counsel.cua.edu/fedlaw/eaa.cfm (last visited Nov. 30, 2013).

113. *See* JAMES PLITT, CYBER EXPORT CONTROL INVESTIGATIONS (2005).

114. *Participating States*, WASSENAAR ARRANGEMENT, http://www.wassenaar.org/participants/index.html (last visited Oct. 11, 2013).

115. APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS, MANDIANT 2 (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

116. *See* Xinhua News Agency, *China Joins Nuclear Suppliers Group*, CHINA.ORG (May 28, 2004), http://www.china.org.cn/english/2004/May/96780.htm.

117. *The Wassenaar Arrangement*, MINISTRY FOREIGN AFF. PEOPLE'S REPUBLIC CHINA, http://www.mfa.gov.cn/eng/wjb/zzjg/jks/kjlc/cgjkwt/t577615.htm (last visited Sept. 15, 2013).

members must continue to build on these outreach efforts and invite China to participate in their dialogue on permissible sales of Ødays.[118]

These shortcomings do not undermine the case for extending the Wassenaar Arrangement to Øday-exploit sales. This multilateral effort would help foster international norms on illegitimate Øday purchases and build international consensus on states' responsibility to halt dangerous sales from within their borders. Most importantly, multilateral export controls would increase the costs associated with selling dangerous exploits to those seeking to target critical infrastructure. Many of the leading gray market firms that sell Øday exploits targeting critical infrastructure ICS are located in Wassenaar member nations, including the United States, Malta, and France.[119] These firms would now have to apply for licenses to sell dangerous exploits, move their operations elsewhere, or risk significant criminal penalties for contravening export controls and operating on the black market. For example, intentional violation of the EAR would result in criminal penalties of up to $1 million and prison sentences of up to twenty years.[120] Such high penalties would likely deter many researchers from engaging in illicit transactions. Therefore, as part of a broader effort to stem debilitating Øday-exploit sales, creating uniform export controls through the Wassenaar Arrangement would constitute a critical step forward in safeguarding nations from cyberattacks.

C. *Building a Stronger Prosecutorial Framework to Bring Sellers of Dangerous Øday Exploits to Justice*

Extending the Wassenaar Arrangement to govern dangerous Øday-exploit sales would be ineffective if researchers could evade punishment when they conducted illicit transactions. Failed prosecutorial efforts would undermine domestic and international export controls, enticing more researchers to enter into this lucrative line of business. Therefore, building stronger capacity to prosecute sellers of these exploits both domestically and abroad is pivotal. Once the United States incorporates the Wassenaar Arrangement's recommended export controls into its Commerce Control List, it will be able to prosecute violators under the EAR.

However, to effectively curb sales of Øday exploits, America's prosecutorial capacity must extend further. A large number of dangerous Øday-exploit sales

118. CNT. NONPROLIFERATION STUDIES, THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES 6 (2012), http://cns.miis.edu/inventory/pdfs/wass.pdf.

119. Prominent U.S. firms operating in this market include Netragard, Exodus Intelligence, and Endgame. *See* Perlroth & Sanger, *supra* note 4.

120. Schoorl, *supra* note 105, at 643.

originate abroad and are therefore beyond the reach of American export laws.[121] Furthermore, although the EAR forbids providing dangerous technical data to foreigners within the United States through its "deemed exports" provision, it does not prohibit sharing this information with U.S. persons located inside the country.[122] U.S. persons, however, may also target the United States with weaponized Øday exploits. The United States must therefore have the capacity to prosecute researchers located abroad who sell exploits to U.S. adversaries, as well as those at home who sell exploits to ill-intentioned Americans.

In order to provide the legal basis for these prosecutions, Congress should amend the Computer Fraud and Abuse Act (CFAA) to govern dangerous Øday-exploit transactions.[123] The CFAA, which has explicit extraterritorial reach, is the United States' most significant federal computer-crime statute. It prohibits intentional hacking of a government computer,[124] damaging a government computer, bank computer, or other computer affecting interstate or foreign commerce,[125] and accessing a computer to commit espionage.[126] Since courts have construed "protected computers" liberally to include any computer connected to the Internet, the CFAA prohibits individuals located domestically or abroad from knowingly or recklessly damaging the vast majority of computers within the United States.[127]

Currently, researchers within and outside the United States who sell Øday exploits targeting U.S. critical infrastructure to America's adversaries avoid prosecution under the CFAA. This is because they can contend that they lack the requisite intent to gain unauthorized access to U.S. computer systems.[128] In their own words, they are merely selling instructions for penetrating computer systems

121. For a comprehensive description of the scope of coverage of the EAR, see 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. INT'L L. 441, 471 (2003).

122. *See* Ira S. Rubinstein & Michael Hintze, *Coping with U.S. Export Controls 2000,* PRACTICING L. INST. (Dec. 2000), http://encryption_policies.tripod.com/us/rubinstein_1200_software.htm.

123. For more on U.S. enforcement of export controls, see *Enforcement*, DEPARTMENT COMMERCE: BUR. INDUSTRY & SECURITY, http://www.bis.doc.gov/index.php/enforcement (last visited Sept 29, 2013).

124. Computer Fraud & Abuse Act, 18 U.S.C. § 1030(a)(3) (2006).

125. *Id.* & 1030(a)(5).

126. *Id.* & 1030(a)(1).

127. *See* Freedom Banc Mortgs. Servs. v. O'Harra, No. 2:11-cv-01073, 2012 U.S. Dist. LEXIS 125734 (S.D. Ohio Sept. 5, 2012); U.S. v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001).

128. Gjelten, *supra* note 64. For an overview of the statute and of the courts' interpretations of the required elements of a CFAA claim, see Deborah F. Buckman, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. FED. 101 (2001).

to third parties and the "way the information is used is up to the customer."[129] To rectify this loophole, the CFAA should be amended to impose an affirmative duty on the seller to conduct due diligence when selling Øday exploits that can be deployed to gain unauthorized access to critical infrastructure industrial control systems and their components. Sellers of dangerous exploits should be required to demonstrate that they "reasonably investigated" the purchaser's background and had "reasonable grounds to believe" that the purchaser would not deploy the exploit to attack such industrial control systems.[130] Courts must determine what constitutes a "reasonable investigation" and "reasonable grounds to believe" in this context. A similar affirmative duty to investigate buyers is placed on sellers in other weaponry contexts, such as with handgun purchases from licensed firearm dealers.[131] Tavern owners also have a duty under various statutes and common law to assess whether customers are intoxicated before serving liquor.[132] Sellers of Øday exploits that target America's industrial control systems must be subject to similarly stringent standards.

Although some might be concerned that this amendment would contribute to what they perceive as the CFAA's already "dangerously broad criminalization of online activity" and abuse of prosecutorial discretion, our proposed amendment is narrowly circumscribed so that only sellers of the most dangerous exploits that target critical infrastructure would be required to perform due diligence. Because weaponized Øday exploits that target critical infrastructure ICS may inflict damage surpassing that of a large-scale natural disaster, an affirmative duty to investigate the buyer's background is reasonable and imperative.[133]

Moreover, due to the absence of stable intermediaries in the marketplace for Øday exploits, holding individual sellers accountable is the only viable pathway to curtailing and deterring these sales. Some scholars have proposed a "gatekeeper liability" scheme for other illicit conduct online such as sales of counterfeit products. In those contexts, there are visible and central intermediaries like eBay that profit from such behavior and are ideally situated to monitor and halt illicit

129. Gjelten, *supra* note 64.

130. For similar statutory language requiring an affirmative duty to conduct due diligence, see 15 U.S.C. § 77k (2012).

131. Jennifer A. Wiegleb, *Strong-Arming the States to Conduct Background Checks for Handgun Purchasers: An Analysis of State Autonomy, Political Accountability, and the Brady Handgun Violence Prevention Act*, 48 WASH. U. J. URB. & CONTEMP. L. 373, 376 (1995).

132. *See* Boris Reznikov, *"Can I See Some ID?" Age Verification Requirements for the Online Liquor Store*, 4 SHIDLER J.L. COMPUTER & TECH. 5, 11 (2007); Lawrence Lazzara Jr., *Arizona's Dram Shop Law*, AVVO, http://www.avvo.com/legal-guides/ugc/arizonas-dram-shop-law (last visited Oct. 14, 2013).

133. Gonsalves, *supra* note 28.

behavior on their sites.[134] Holding them liable would constitute an effective enforcement strategy.[135] The marketplace for Øday exploits, however, is widely dispersed, often underground, and lacks visible intermediaries. Since firms like Vupen sell their dangerous exploits directly to buyers, they must be held accountable for failing to implement robust screening measures.[136]

The amended CFAA should empower the United States to prosecute domestic firms that sell Øday exploits to U.S. persons who deploy them to attack critical infrastructure. Given its explicit extraterritorial reach, the amended statute should also enable prosecutions of vulnerability research firms located in the gray market abroad, such as the European-headquartered Vupen and ReVuln. The United States would be able to justify extraterritorial extension of the CFAA under international law through the protective principle of prescriptive jurisdiction. The protective principle authorizes a nation to exercise jurisdiction over conduct outside its boundaries that directly threatens its security or critical government functions. Vulnerability researchers operating abroad who sell Øday exploits targeting U.S. critical infrastructure to American adversaries sufficiently threaten U.S. security to warrant protective-based jurisdiction.[137]

In some cases, the United States should be able to extradite researchers abroad who have violated the CFAA. This is because the foremost gray market sellers of Øday vulnerabilities are located in European Union countries that have extradition treaties with the United States. U.S. indictments could also provide a much-needed deterrent to vulnerability researchers located in countries that do not have extradition treaties with the United States. By indicting these researchers under the CFAA, the United States would prevent them from traveling and conducting business in other countries out of fear of being apprehended by a foreign government and extradited to the United States.[138]

Although the intangible nature of Øday transactions and anonymous nature of the market would make detection of prohibited sales on the underground market difficult, U.S. law enforcement agents could overcome this challenge through

134. Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 275-79 (2005).

135. *Id.*; *see* Carlos Cortes, *Internet Governance Series: Stop Porn, Stop Piracy—the Limits of Intermediary Liability*, LSE MEDIA POL'Y PROJECT (Oct. 7, 2013), http://blogs.lse.ac.uk/mediapolicyproject/2013/10/07/internet-governance-series-stop-porn-stop-piracy-the-limits-of-intermediary-liability.

136. For an illustration of how Vupen interacts with prospective customers directly through its website, see *Receive More Information*, VUPEN SECURITY, http://www.vupen.com/english/sales.php (last visited Oct. 12, 2013).

137. *See* Paul Stockton & Michele Golabek-Goldman, *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, 25 STAN. L. & POL'Y REV. 10 (forthcoming 2014) (on file with authors).

138. *See* Siobhan Gorman, *U.S. Eyes Pushback On China Hacking*, WALL ST. J., Apr. 22, 2013, http://online.wsj.com/artcle/SB10001424127887324345804578424741315433114.html.

international sting operations.[139] International sting operations have proven effective at disrupting other forms of intangible cybercrime.[140] For example, last year, the FBI led an international sting operation that disrupted a multi-million dollar online financial fraud scheme and led to the arrests of twenty-four suspects in thirteen countries and on four continents.[141]

One major disadvantage of sting operations is that they necessitate significant resources and time.[142] The sting operation described above took two years to complete.[143] Nevertheless, even just a few successful and highly publicized operations on the Øday-exploit market would likely compel researchers to think twice before selling their discoveries to prohibited buyers.[144] During each transaction, they would worry whether the professed buyer was an undercover law-enforcement agent and whether their sale would lead to significant criminal penalties under the EAR or CFAA.[145] Such a deterrence strategy has worked effectively to combat conventional terrorism and other types of crimes, illustrating that the United States does not always need a "cyber-specific" strategy to mitigate cyber threats such as weaponized Øday exploits. Global sting operations, combined with robust international and domestic export controls, would therefore help combat Øday-exploit sales that threaten international security.

IV. Policy Issues for Further Consideration

Threading through much of our analysis is an underlying policy issue: the tradeoff for U.S. agencies between the benefits of access to an unfettered market for weaponized Øday exploits, versus the benefits of clamping down on that market. Some have suggested that the United States created the cyberweapons market

139. Jack Goldsmith, *Herb Lin on the Market for Zero-Day Vulnerabilities*, LAWFARE (Feb. 15, 2013, 7:36 AM), http://www.lawfareblog.com/2013/02/herb-lin-on-the-market-for-zero-day-vulnerabilities.

140. *See* Aaron Katersky et al., *Largest Cyber Sting in History Nabs 24 on Four Continents*, ABC NEWS (June 26, 2012), http://abcnews.go.com/Business/largest-cyber-sting-history-nabs-24-continents/story?id=16653993.

141. *Id.*

142. Goldsmith, *supra* note 139.

143. Katersky et al., *supra* note 140.

144. *See* Goldsmith, *supra* note 139.

145. For a general overview of these significant penalties, see *Penalties*, DEPARTMENT COMMERCE: BUREAU INDUSTRY & SECURITY, http://www.bis.doc.gov/index.php/enforcement/oee/penalties (last visited Sept. 20, 2013); CHARLES DOYLE, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 1 (2010), http://www.fas.org/sgp/crs/misc/97-1025.pdf.

by being the first to pay extraordinarily high prices for Ødays.[146] They have accused the United States of "creat[ing] Frankenstein by feeding the market."[147] Others have gone so far as to propose that, rather than regulating the supply side of the market, U.S. government agencies should curb the demand side by relinquishing their own purchases of exploits.[148] If agencies did so, the market would lose some of its most well-paying buyers,[149] potentially deterring suppliers from scouring software for vulnerabilities.

Before relinquishing such purchases, U.S. policymakers would first need to examine the potential costs of doing so in terms of foregoing potentially valuable information from the exploit market. Some analysts have indicated that if U.S. agencies halted their exploit-purchasing program, they would be deprived of critical tools for defending U.S. networks against attack.[150] Law enforcement agencies would likewise forgo valuable technologies for tracking underground criminals.[151] But do these agencies weigh these benefits against the potentially catastrophic risks that the Øday market poses to U.S. security? We have seen no evidence that they do. The time has come for Congress, Executive Branch leaders, the software industry, and scholars to bring this tradeoff analysis into the open and determine whether staying at the extreme end of the policy spectrum—that of de facto support for a dangerous bazaar for Øday-exploits—best serves U.S. national security.

Conclusion

The United States and the international community are enabling a global Øday-exploit market to flourish, which empowers terrorist organizations and rogue states to purchase cyberweaponry targeting our computer networks. In spite of the dire risk posed by the market, policymakers have failed to provide any concrete solutions for mitigating the threat. They have either capitulated to the market's forces, arguing that regulation is futile, or proposed tenuous solutions, such as holding software companies liable for all defects in their products.

146. Perlroth & Sanger, *supra* note 4; *see Zero-Day Market*, *supra* note 38.

147. *See* Perlroth & Sanger, *supra* note 4.

148. For a general discussion of the potential "blowback" stemming from the U.S. government's Øday exploit purchasing policies, see Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, Reuters (May 10, 2013, 9:47 PM), http://in.reuters.com/article/2013/05/10/usa-cyberweapons-idINDEE9490AX20130510.

149. *See Zero-Day Market*, *supra* note 38.

150. *See* Gallagher, *supra* note 24; Farrell, *supra* note 57.

151. *See A Zero Day Exploit Used for Good?*, PCRisk.com (Aug. 13, 2013), http://www.pcrisk.com/internet-threat-news/7304-a-zero-day-exploit-used-for-good.

There is no panacea to this problem. However, pursuing the complementary policies of incentivizing software companies to invest in robust security, developing multilateral and domestic export controls, and strengthening prosecutions of researchers who sell Øday exploits to adversaries would constitute vital first steps in reducing the market's threat. Even if certain sellers were undeterred from selling exploits to those who seek to harm us, they would be compelled to spend more time avoiding detection and less time unearthing dangerous exploits. Fewer weaponized Øday exploits overall would fall into the hands of U.S. adversaries. In the long term, the United States and other government participants in the market must reexamine whether their unlimited access to this market is making us any safer.