Northwestern Journal of Technology and Intellectual Property

Volume 13 | Issue 2 Article 3

Fall 2015

An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement

Innokenty Pyetranker

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement

Innokenty Pyetranker

September 2015 VOL. 13, NO. 2

Northwestern Journal of Technology and Intellectual Property
Volume 13, Number 2 (September 2015)

An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement

By Innokenty Pyetranker*

Scenes of near-apocalyptic devastation resulting from good software gone bad are no longer the stuff of science fiction flicks starring bodybuilders-cum-governors. Lightning-fast technological progress and the ubiquity of the Internet have made it easy for our imaginations, as well as our political leaders, to conjure up realistic images of cyber nightmares come true. Now that fears about what lurks inside cyberspace have gone mainstream, I examine one action ostensibly aimed to allay such fears: the December 2013 amendment to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (commonly known as the Wassenaar Arrangement). My analysis of the December 2013 amendment—which was passed to prevent certain dual-use cyber technologies from falling into the wrong hands—proceeds in three parts. First, I argue that history teaches that cyber products are not generally amendable to export controls. Second, I find that the Wassenaar Arrangement's institutional flaws are so enfeebling that the Arrangement's very utility is questionable. Third, I assert that economic incentives, globalization, and the intangibility of cyber technology all present formidable obstacles to the December 2013 amendment's success. Although the December 2013 amendment is likely doomed to irrelevance, I conclude that concerted action—rather than passive pessimism—must be our response to cyber threats.

TABLE OF CONTENTS

* Frederick Sheldon Fellow, Harvard University, 2013-2014; Visiting Scholar, The Cegla Center for Interdisciplinary Research of the Law at Tel Aviv University, 2014; J.D., Harvard Law School, 2013. I am grateful to Michael Birnhack, Doron Hindin, Nimrod Kozlovski, and Daniel Reisner for their abundant wisdom and generous help. I am indebted to Judith Murciano and Harvard University's Committee on General Scholarships for making this project possible.

I. INTRODUCTION

A. The New (Cyber) Normal

> *It doesn't take much to imagine the consequences of a successful cyber attack. 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. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill.*[1]

¶1 That people now reside in something of a cyber world is a truism; it is a given that a multitude of our experiences from the cradle to the grave—from instagrammed sonogram shots[2] to online education modules[3] to corporate web conferencing[4] to mobile dating apps[5] to virtual memorials for lost loved ones[6]—have gone or will eventually go cyber to some

[1] Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012, 7:15 PM), http://online.wsj.com/news/articles/SB10000872396390444330904577535492693044650.

[2] *See, e.g.*, Esther Lee, *Snooki Shares Sonogram Picture of Baby Girl: Pregnant Star Says Daughter "Already Applying Lipstick" in Womb*, US WEEKLY (May 19, 2014, 5:50 PM), http://www.usmagazine.com/celebrity-moms/news/snooki-sonogram-picture-pregnant-stars-baby-girl-applying-lipstick-2014195.

[3] *See, e.g.*, Sarah Mishkin, *Saudi Arabia to use edX web courses to train unemployed*, FIN. TIMES (July 14, 2014, 7:55 PM), http://www.ft.com/intl/cms/s/0/67fe0cb8-0c3d-11e4-943b-00144feabdc0.html; Chris Parr, *Mooc makeover saves refugee course*, TIMES HIGHER EDUC. (July 17, 2014), http://www.timeshighereducation.co.uk/news/mooc-makeover-saves-refugee-course/2014493.article.

[4] *See, e.g.*, June Bower, *4 Ways Video Conferencing Can Benefit Small Businesses*, MASHABLE (June 2, 2011), http://mashable.com/2011/06/02/online-meetings-small-biz/; Yardena Arar, *Web conferencing showdown: What's the best software for online meetings?*, PCWORLD (Sept. 24, 2012, 3:30 AM), http://www.pcworld.com/article/2010325/web-conferencing-showdown-whats-the-best-software-for-online-meetings.html.

[5] *See, e.g.*, Devjyot Ghoshal, *Mobile dating apps suggest that the World Cup is a potent aphrodisiac*, QUARTZ (June 25, 2014), http://qz.com/225744/the-world-cup-is-a-potent-aphrodisiac-for-mobile-dating-apps/; Julie Spira, *Mobile Love: 10 Dating Apps to Ramp Up Your Love Life*, HUFFINGTON POST (Nov. 27, 2013, 2:08 PM), http://www.huffingtonpost.com/julie-spira/mobile-love-mobile-dating_b_4318293.html.

[6] *See, e.g.*, Maya Socolovsky, *Cyber-Spaces of Grief: Online Memorials and the Columbine High School Shootings*, 24 JAC: A JOURNAL OF RHETORIC, CULTURE & POLITICS 467 (2004); Kenneth Emmerling, *Online memorials and cyber immortality*, EXAMINER (Nov. 9, 2009), http://www.examiner.com/article/online-memorials-and-cyber-immortality; Geoffrey A. Fowler, *Online Memorial Services: After a Death, Celebrating a Life Online*, WALL ST. J. (Jan. 28, 2014), http://online.wsj.com/news/articles/SB10001424052702303553204579348752262042642.

extent.[7] The Internet is so embedded in and indispensable to our day-to-day lives that access to it is described in the language of human rights.[8] All the benefits of living in a networked society are, however, tempered by concomitant risks. In addition to the familiar perils of warfare, crime, espionage, and terrorism, new threats of cyberwarfare, [9] cybercrime,[10] cyberespionage,[11] and cyberterrorism[12] have emerged. In this brave new cyber-world, these dangers and others are poised to exploit our reliance on e-lifestyles.

¶2 Cyberspace is already an established arena for confrontations. Virtual attacks regularly harm or even cripple individual businesses.[13] Cybercriminals threaten entire sectors of the global economy.[14] In late 2014, a single act of "cyber-vandalism" caused a

---

[7] *See* WORLD ECONOMIC FORUM, RISK AND RESPONSIBILITY IN A HYPERCONNECTED WORLD 5 (2014), http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf [hereinafter WORLD ECONOMIC FORUM] ("Digital technology touches virtually every aspect of daily life today. Social interaction, healthcare activity, political engagement or economic decision-making – digital connectivity permeates it all, and the dependence on this connectivity is growing swiftly.").

[8] *See* Nathan Olivarez-Giles, *United Nations report: Internet access is a human right*, L.A. TIMES (June 3, 2011, 6:42 PM), http://latimesblogs.latimes.com/technology/2011/06/united-nations-report-internet-access-is-a-human-right.html.

[9] *See, e.g.*, TED Talks, *Chris Domas: The 1s and 0s behind cyber warfare*, YOUTUBE (June 30, 2014), https://www.youtube.com/watch?v=cWpRxyqDgpM; Ellen Nakashima, *U.S. cyberwarfare force to grow significantly, defense secretary says*, WASH. POST, (Mar. 28, 2014), http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html; Spencer Kimball, *NATO moves to apply armed conflict law to cyber warfare*, DEUTSCHE WELLE (July 2, 2014), http://dw.de/p/1CUid.

[10] *See generally* CYBERCRIME: DIGITAL COPS IN A NETWORKED ENVIRONMENT (Jack M. Balkin, James Grimmelmann, Eddan Katz, Nimrod Kozlovski, Shlomit Wagman & Tal Zarsky eds., 2007); Nimrod Kozlovski, A Paradigm Shift in Online Policing - Designing Accountable Policing (June 2005) (J.S.D. dissertation, Yale Law School) (*available at* http://crypto.stanford.edu/portia/papers/Kozlovski.pdf) (describing the nature of cybercrime).

[11] *See, e.g.*, Lizzie Dearden, *Germany 'may use manual typewriters' to fight cyber espionage*, INDEPENDENT (July 15, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/germany-may-use-manual-typewriters-to-fight-cyber-espionage-9607697.html; Juhana Rossi, *Finland Victim of Long-Term Cyberespionage*, WALL ST. J. (July 2, 2014), http://online.wsj.com/articles/finland-victim-of-long-term-cyberespionage-1404309676.

[12] *See generally* Aviv Cohen, *Cyberterrorism: Are We Legally Ready?*, 9 J. INT'L BUS. & L. 1 (2010); Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?*, UNITED STATES INSTITUTE OF PEACE (May 13, 2004), http://www.usip.org/sites/default/files/sr119.pdf.

[13] *See* WORLD ECONOMIC FORUM, *supra* note 7, at 2-3 ("Risks of cyberattacks are starting to have a business impact. Controls put in place to protect information assets have at least a "moderate" impact on front-line employee productivity for nearly 90% of institutions [that were surveyed]. Moreover, security concerns are already making companies delay implementation of cloud and mobile technology capabilities. And while direct cyber resilience spend represents only a small share of total enterprise technology expenditure, some chief information officers (CIOs) and chief information security officers (CISOs) estimate that indirect or unaccounted security requirements drive as much as 20-30% of overall technology spending, crowding other projects that could create business value."). *See also* Jonathan Zittrain, *Intensifying Cyber Threats*, HUFFINGTON POST (Jan. 22, 2014, 12:36 PM), http://www.huffingtonpost.com/jonathan-zittrain/intensifying-cyber-threats_b_4645548.html ("[T]he Syrian Electronic Army, which supports Bashar al-Assad's regime, has successfully managed to temporarily cripple the online operations of companies like Twitter and The New York Times.").

[14] *See, e.g.*, Craig Newman & Daniel Stein, *Talking heads: why regulators are looking at cyber security*, FIN. TIMES (Sept. 1, 2013), http://www.ft.com/cms/s/0/53125dc0-00ec-11e3-8918-00144feab7de.html ("[T]he International Organization of Securities Commissions reports that 53 per cent of the world's

national scandal and diplomatic kerfuffle.[15] Indeed, cyber controversies play a consequential role in some bilateral relationships; between the United States and China, for instance, allegations and counter allegations of cyber espionage consistently threaten to mar ties between the two countries.[16] Some have convincingly argued that an actual war conducted on a cyber battlefield "is still more hype than hazard,"[17] but signs of the future are already visible. For instance, the use of cyber assaults by Russian forces against Georgia in 2008, illuminated—in the words of Professor John Arquilla—"the potential of cyberwar in a manner not unlike the way the Spanish Civil War foreshadowed the rising dominance of air power 75 years ago, offering a preview of World War II's deadly aerial bombings."[18] More bluntly, Professor Ty Cobb predicts that cyberspace will be the setting in which 21st century conflicts will be fought.[19]

¶3 Cyberspace is also an established arena for regulation. Many sovereign states address cyber issues in domestic legislation.[20] Politicians from a number of countries—including

securities exchanges were hit last year by cyber attacks, and that nearly every exchange recognises cyber crime as a significant, systematic risk…The annual worldwide cost of cyber crime has been estimated at $100bn, and studies have shown that financial services companies are among the most frequently affected.").

[15] *See, e.g.*, Brent Lang, *Obama Calls Sony Hack 'Cyber Vandalism,' Not Act of War*, VARIETY, (Dec. 21, 2014, 9:52 AM), http://variety.com/2014/film/news/obama-calls-sony-hack-cyber-vandalism-not-act-of-war-1201384777/ ("President Barack Obama told CNN that North Korea's hack attack on Sony Pictures Entertainment is an act of 'cyber-vandalism,' not an act of war."); Patrick Frater, *Sony Hacking Spells Diplomatic Farce as China Weighs in With Equivocal Position*, VARIETY (Dec. 21, 2014, 4:20 AM PT), http://variety.com/2014/film/news/sony-hacking-spells-diplomatic-farce-as-china-weighs-in-with-equivocal-position-1201384689/ ("The chorus of accusations over the hacking of Sony Pictures Entertainment this weekend developed into a bout of diplomatic baiting and back-biting.").

[16] *See, e.g.*, William Wan & Ellen Nakashima, *Report ties cyberattacks on U.S. computers to Chinese military*, WASH. POST (Feb. 19, 2013), http://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700228e-7a6a-11e2-9a75-dab0201670da_story.html (reporting that senior U.S. officials, including President Obama, have repeatedly raised the issue of Chinese cyber attacks on commercial targets with Chinese government officials); Eyder Peralta, *U.S. Files Criminal Charges Against Chinese Officials Over Cyberspying*, NPR (May 19, 2014, 9:42 AM), http://www.npr.org/blogs/thetwo-way/2014/05/19/313935588/reports-u-s-files-criminal-charges-against-chinese-officials-over-cyber-spying (describing the U.S. government's 2014 decision to file criminal charges against five Chinese military-affiliated hackers for stealing commercial secrets from American companies); Jonathan Kaiman, *China reacts furiously to US cyber-espionage charges*, GUARDIAN (May 20, 2014, 1:31 PM), http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges ("China's foreign ministry called the allegations preposterous and accused the US of double standards. The assistant foreign minister, Zheng Zeguang, summoned the US ambassador, Max Baucus, to lodge a formal complaint…China also accused the US of hypocrisy, tacitly recalling Edward Snowden's revelations last year that Washington had overseen the hacking of Chinese companies, including the Shenzhen-based telecommunications company Huawei.").

[17] Thomas Rid, *Think Again: Cyberwar*, FOREIGN POL'Y (Feb. 27, 2012), http://www.foreignpolicy.com/ articles/2012/02/27/cyberwar.

[18] John Arquilla, *Cyberwar Is Already Upon Us*, FOREIGN POL'Y (Feb. 27, 2012), http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us.

[19] Ty Cobb, *Cyber Warfare: Where the 21st Century Conflicts Will be Fought*, HARV. NAT'L SEC. J. (Mar. 5, 2012, 10:36 PM), http://harvardnsj.org/2012/03/cyber-warfare-where-the-21st-century-conflicts-will-be-fought/.

[20] *See, e.g.*, ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 52-61 (2013), http://www.fas.org/sgp/crs/natsec/R42114.pdf (listing U.S. laws with provisions related to cybersecurity); Pavan Duggal, Indian Cyber Law Developments 2013, ECON. TIMES (Dec. 26, 2013, 1:46 PM),

the United States—have been especially adamant about improving cyber security in the private sector.[21] Multilateral efforts to tackle cybercrime,[22] cyber crises,[23] and the export of cyber technology[24] illustrate the seriousness with which world leaders treat cyberspace.

B. Article Outline

¶4 Cyber menaces looming on the horizon pose grave risks for individuals, businesses, and sovereign members of the international community alike. Recognizing the multifaceted nature of cyber threats, this Article takes a single, discrete danger—the proliferation of certain potentially destabilizing cyber products—and analyzes a single, discrete action that the international community has collectively taken to address that danger. Thus, this Article concentrates on the Wassenaar Arrangement—a global export control regime that has been labeled "the only important multilateral arrangement that addresses the conventional arms trade and high-technology items with military applications"[25]—and a recent Wassenaar Arrangement amendment intended to regulate the trade of certain dual-use cyber technologies (i.e., technologies that have both civilian and military uses). Part II provides background information on the global system for regulating

---

http://blogs.economictimes.indiatimes.com/Cyberlawsintodaystimes/entry/indian-cyber-law-developments-2013 (describing recent developments in Indian cyberlaw); Michael Knigge, *German jitters over cyber attacks*, DEUTSCHE WELLE, Mar. 8, 2013, http://www.dw.de/german-jitters-over-cyber-attacks/a-16658040 ("This week Germany's Interior Ministry released a first draft of a new law aimed at 'raising the security of IT systems.'"); *Brazil aims to bring order to lawless cyberspace*, REUTERS (Feb. 26, 2013, 3:35 PM), http://uk.reuters.com/article/2013/02/26/brazil-cyberfraud-idUKL1N0BP52J20130226 ("Long seen as the Wild West of online fraud, Brazil is about to implement its first cyber-crimes law in an attempt to protect its rapidly expanding banking and e-commerce industries.").

[21] *See, e.g.*, *Remarks as Prepared for Delivery by Special Assistant to the President and White House Cybersecurity Coordinator Michael Daniel – 007 or DDoS: What is Real World Cyber?*, WHITEHOUSE.GOV (Feb. 28, 2013), http://www.whitehouse.gov/sites/default/files/docs/2013-02-28_final_rsa_speech.pdf ("One governmental role is clear and uncontroversial: the government should help you – private sector companies – help yourself, particularly in the area of prevention."); *South Africa launches National Cyber Security Advisory Council*, IT NEWS AFRICA (Oct. 15, 2013, http://www.itnewsafrica.com/2013/10/south-africa-launches-national-cyber-security-advisory-council/ (describing South Africa's "National Cyber Security Policy Framework," a statute that seeks to foster cooperation between the government, private sector, and civil society in the realm of cyber security); Kelly Ng, *Cyber Security Remains a Priority for Singapore Government*, FUTUREGOV (Jan. 29, 2014), http://www.futuregov.asia/articles/2014/jan/29/cyber-security-remains-priority-singapore-governme/ (summarizing the Singaporean government's strategy to improve cyber security in the country; embedded in the strategy are partnerships between the government and the Singaporean private sector).

[22] *See* Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[23] *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 141 (2014) (describing the "International Multilateral Partnership Against Cyber Threats," a comprehensive alliance against cyber threats that is tasked with providing cybersecurity assistance and support to the International Telecommunication Union's 192 member–states as well as to other United Nations organizations).

[24] *See infra* Part IV (providing background information on the Wassenaar Arrangement, a multilateral export regime that controls the export of, inter alia, cyber technology products).

[25] Michael Lipson, *The Reincarnation of CoCom: Explaining Post-Cold War Export Controls*, 6 NONPROLIFERATION REV. 33, 33 (quoting William W. Keller, *The Political Economy of Conventional Arms Proliferation*, 96 CURRENT HIST. 179 (1997)).

exports. Part III summarizes key elements of the Wassenaar Arrangement. Part IV examines the December 2013 amendment to the Wassenaar Arrangement. Part V argues that the Wassenaar Arrangement, even with the addition of the December 2013 amendment, is ill-equipped to stem the export of dangerous cyber technologies for historical, institutional, and theoretical reasons. Part VI concludes.

II. EXPORT CONTROLS AT A GLANCE

¶5 Also known as "export restraints" or "export restrictions," export controls are defined as "measures instituted by exporting countries to supervise export flows."[26] Governments utilize export controls to manage the flow of goods, services, and technologies across borders. Export controls are different from export bans in that the former give government regulators the legal authority to review, approve, and deny exports.[27] Generally, governments manage exports as a means of implementing any number of public policy objectives. Some products are controlled in order to support domestic industries.[28] Other products are controlled for the maintenance of the admittedly amorphous concept of "international security." Professor Philippe Achilleas explains international security in the following way:

> The protection of international security is based on three complementary techniques. Firstly, there is disarmament, which is aimed at eliminating one category of weapon. Secondly, there is arms control, which is aimed at reducing the risk of war, making it less destructive when war starts, and reducing defense costs through the signing of agreements between countries. These agreements are aimed at reducing, limiting or regulating the use of certain weapons. Finally, non-proliferation is aimed at preventing the development and sale of particular weapons.[29]

¶6 Although export control regimes do not contribute to the first technique described above, which is better represented by initiatives like disarmament treaties,[30] multilateral

---

[26] Joanna Bonarriva, Michelle Koscielski, & Edward Wilson, *Export Controls: An Overview of Their Use, Economic Effects, and Treatment in the Global Trading System* 1 (Office of Industries, U.S. Int'l Trade Commission, Working Paper No. ID-23, 2009), *available at* www.usitc.gov/publications/332/working_papers/ID-23.pdf (citation and internal quotation marks omitted).

[27] Tim Maurer, *Exporting the Right to Privacy*, SLATE (May 15, 2014, 7:54 AM), http://www.slate.com/articles/technology/future_tense/2014/05/wassenaar_arrangement_u_s_export_control_reform_keeping_surveillance_tech.html.

[28] *See, e.g.*, Michael William Lochmann, *The Japanese Voluntary Restraint on Automobile Exports: An Abandonment of the Free Trade Principles of the GATT and the Free Market Principles of United States Antitrust Laws*, 27 HARV. INT'L L. J. 99, 99 (1986) ("In May of 1981, the Japanese government announced that it would restrict the number of automobiles its car manufacturers exported to the United States market during the following three years. This restriction was the apparent result of intense political pressure by domestic industry and labor organizations.").

[29] Philippe Achilleas, *International Regimes*, *in* EXPORT CONTROL LAW AND REGULATIONS HANDBOOK 20 (Yann Aubin & Arnaud Idiart eds., 2007).

[30] Disarmament treaties generally take three forms: security disarmament treaties, humanitarian disarmament treaties, and hybrid disarmament treaties. Bonnie Docherty, *Ending Civilian Suffering: The Purpose, Provisions, and Promise of Humanitarian Disarmament Law*, 15 AUSTRIAN REV. INT'L & EUR. L. 7, 12 (2010). Security disarmament treaties "focus on the elimination of certain weapons of war." *Id.*

export controls geared towards controlling the spread of potentially dangerous cutting-edge technologies—the subject of this Article—function as part of the latter two techniques. That is, these types of export controls aim to both moderate the destructiveness of cyber conflicts (arms control) and preemptively forestall the transfer of weaponizable technologies (non-proliferation). Countries are incentivized to participate in export control agreements for essentially the same reasons. Indeed, Professors Ron Smith and Bernard Udis posit that a state might participate in an export control regime to, inter alia, stop the spread of weapons that "may prolong a war," avert both "an expensive arms race" and "pre-emptive aggression," and "prevent the sale of weapons to a potential enemy."[31]

¶7 Modern export controls emerged during the Cold War. After receiving reports detailing the Soviet Union's acquisition of Western technology for military purposes, the United States and its allies "worried that, as Lenin had predicted, the Capitalist West would sell the Communist East the rope with which to hang it."[32] In response, Western Bloc powers formed the Coordinating Committee for the Control of Multinational Trade (CoCom) to prevent the transfer of arms, nuclear-related items, and dual-use technologies to the Eastern Bloc.[33] Following the end of the Cold War, CoCom was disbanded and replaced by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, a regime that embraced many former Eastern Bloc countries as "parties rather than adversaries."[34]

¶8 Commonly known as "the Wassenaar Arrangement" or "the Arrangement," the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is but one element of today's multilateral export control system; that system comprises four "separate and almost wholly independent" regimes.[35] Aside from

---

Humanitarian disarmament treaties focus on "reduc[ing] the suffering of individuals in times of war." *Id.* at 16. Hybrid disarmament treaties "represent a blend of elements characteristic of security disarmament and humanitarian disarmament, while moving increasingly toward the latter." *Id.* at 13.

[31] Ron Smith & Bernard Udis, *New Challenges to Arms Export Control: Whither Wassenaar?*, 8 NONPROLIFERATION REV. 81, 82 (2001).

[32] 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, 450 (2003). *See also* Robert Y. Stebbings, *Export Controls: Extraterritorial Conflict—The Dilemma of the Host Country Employee*, 19 CASE W. RES. J. INT'L L. 303, 313 (1987) ("According to U.S. intelligence sources, the Soviet KGB is directing a massive campaign to acquire Western technology, coordinated at the highest levels of the Soviet government. Although deficient in military manpower and perhaps even firepower, the NATO countries have maintained a technological advantage over Warsaw Pact countries. Therefore, defense experts wish to assure the maintenance of technological "lead time" by restricting exports and reexports of the most advanced technology and goods which can be used militarily, as well as commercially, or from which the technology can be gleaned.") (citation omitted).

[33] *See* Corr, *supra* note 32, at 450-51. *See also* Stebbings, *supra* note 32, at 312 ("The main purpose of COCOM is to implement a system of multilateral control of various commodities and technical data that may affect the national security of a given member nation. COCOM member countries agree to monitor all imports and exports as they may affect each country's national security. Reexportation from a COCOM member country to a "controlled country" is not allowed without consent from the original exporting member and requires a unanimous vote of COCOM members. Controlled countries include almost all communist nations, the interests of which are deemed inimical to the interests of the COCOM member nations. These nations are: Cuba, Vietnam, Kampuchea, Angola, Tibet, North Korea, South Africa, Libya, Nicaragua, Albania, Laos, Outer Mongolia, Namibia, the U.S.S.R. and the Warsaw Pact nations.").

[34] Charles B. Shotwell, *Export Controls: A Clash of Imperatives*, *in* 1 THE GLOBAL CENTURY: GLOBALIZATION AND NATIONAL SECURITY 335, 455 (2001).

[35] Daniel H. Joyner, *Restructuring the multilateral export control regime system*, 9 J. CONFLICT & SEC.

the Wassenaar Arrangement, which is intended to "contribute to regional and international security and stability by promoting transparency and greater responsibility" in the global trade of munitions and dual-use products, the other three regimes are the Nuclear Suppliers Group, the Australia Group, the Missile Technology Control Regime.[36] The Nuclear Suppliers Group is made up of countries that have been working together to restrict the proliferation of nuclear weapons since 1992.[37] The Australia Group focused only on "international export controls on chemical weapons precursor chemicals" when it was first formed in 1985, but eventually the organization "expanded its focus to include chemical production equipment and technologies and measures to prevent the proliferation of biological weapons."[38] Created in 1987, the Missile Technology Control Regime includes "member countries that have agreed to coordinate their national export controls to stem missile proliferation."[39] The principal aim of all four regimes is to control exports of certain items via the coordination and harmonization of member states' nonproliferation policies.[40]

III. THE WASSENAAR ARRANGEMENT

¶9 In July 1996, representatives of 33 countries met in Vienna, Austria and agreed to go forward with the Wassenaar Arrangement.[41] To implement the agreement, the founding members of the Arrangement placed export controls on items enumerated in two lists: the Munitions List and the List of Dual-Use Goods and Technologies.[42] "Munitions" are easy to conceptualize as they are basically synonymous with military weapons; munitions that are regulated by the Arrangement include bombs, torpedoes, and grenades.[43] "Dual-use goods and technologies" are best explained by way of illustration:

> A personal computer (PC) is the quintessential example of an item that has both military and commercial purposes. John Q. Citizen in America uses his Apple Powerbook laptop to keep his financial house in order, a commercial use of a PC. However, an underground terrorist organization in a dark corner of the world could use that same Powerbook to build a dirty bomb, using the laptop for weapons

---

L. 181, 183 (2004).

[36] *Multilateral Export Control Regimes*, BUREAU OF INDUSTRY AND SECURITY, UNITED STATES DEPARTMENT OF COMMERCE, http://www.bis.doc.gov/index.php/policy-guidance/multilateral-export-control-regimes (last visited Sept. 8, 2015).

[37] *Id*.

[38] *Id.*

[39] *Id.*

[40] *See* Joyner, *supra* note 35, at 184-85.

[41] *See Press Statement*, THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES (July 12, 1996), http://www.wassenaar.org/publicdocuments/1996/press120796.html. The 33 countries were Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. *Id.*

[42] *See id.*

[43] *List of Dual-Use Goods and Technologies and Munitions List*, THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES 170 (2013), http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/WA-LIST%20%2813%29%201.pdf.

> proliferation. Therefore, the laptop is a "dual use" item - it has both commercial and military applications.[44]

¶10 In setting up the Arrangement, members of the group had four primary goals. First, members sought to promote "transparency and greater responsibility with regard to transfers of conventional arms and dual-use goods and technologies" and thereby forestall "destabilizing accumulations" of those items.[45] Second, members aspired to use domestic policies to ensure that transfers of conventional arms and dual-use goods and technologies would not contribute to the development of military capabilities.[46] Third, members wanted to complement and reinforce "the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognized measures designed to promote transparency and greater responsibility."[47] Fourth, members were interested in "enhancing cooperation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behavior of a state is, or becomes, a cause for serious concern."[48] To achieve these collective goals, the founding members of the Wassenaar Arrangement committed to sharing information, controlling the distribution of items on the munitions and dual-use lists, and notifying one another of transfers and denials of listed items to non-members.[49]

¶11 The declared goals of the Wassenaar Arrangement, lofty as they may be, have always been subject to institutional realities. The earnest commitments made by member states are not really enforceable.[50] Those enforcement issues are only worsened by the Arrangement's notification mechanisms.[51] Funding for the Arrangement is far from transparent and only mentioned once in its guiding documents.[52] And reforming any of the Arrangement's flaws is a tough row to hoe because all decisions need to be "reached by consensus of the Participating States."[53] Consensus-based decision-making plainly becomes harder as the number of decision-makers grows. Decision-making proved difficult with the thirty-three original members; with new additions Croatia, Estonia, Latvia, Lithuania, Malta, Mexico, Slovenia, and South Africa, the organization now embraces forty-one member states.[54] Technically, the Arrangement could become even

---

[44] Jordan Collins, *Same Laws, Different Century: The Bureau of Industry & Security's Role in Global Trade & National Security*, 15 CURRENTS INT'L L. J. 108, 110 (2006).

[45] *See Press Statement*, *supra* note 41.

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *See* Jamil Jaffer, *Strengthening the Wassenaar Export Control Regime*, 3 CHI. J. INT'L L. 519, 520 (2002) ("The Wassenaar Arrangement attempts to control proliferation of dual-use technologies through a variety of mechanisms, including controls on distribution, information-sharing among member states, and notification of transfers or denials of dual-use goods to non-member states.") (citation omitted).

[50] *See infra* Part V.B.1 (describing the Wassenaar Arrangement's enforceability problems).

[51] *See infra* Part V.B.2 (describing the Wassenaar Arrangement's counterproductive notification provisions).

[52] *Guidelines & Procedures, including the Initial Elements*, THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES 6 (2014), http://www.wassenaar.org/guidelines/docs/Guidelines%20and%20procedures%20including%20the%20Initial%20Elements.pdf ("Financial needs of the Arrangement will be covered under annual budgets, to be adopted by Plenary Meetings.").

[53] *Id.*

[54] *Participating States*, THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL

more unwieldy in the future; more countries could theoretically join the Arrangement provided they fulfill the "agreed membership criteria," which include adherence to the other three multilateral export control regimes and maintenance of both "adequate" export controls and "responsible" policies towards countries that threaten international peace and security.[55]

IV. THE CYBER AMENDMENT TO THE WASSENAAR ARRANGEMENT

¶12 The Wassenaar Arrangement's control lists are not static; members agreed from the beginning that the lists would "be reviewed regularly to reflect technological developments and experience gained by Participating States."[56] With a cyber menace looming on the horizon[57] and no single international agency or body with the mandate to deal with cyber-security, the Wassenaar Arrangement eventually sprang into action. Growing calls for action on matters of cybersecurity came to fruition during a December 2013 meeting.[58] Following that meeting, the Arrangement issued a public statement proclaiming that member states had agreed on new export controls for technologies that "under certain conditions, may be detrimental to international and regional security and stability."[59] Daniel Reisner and Doron Hindin suggest that these new export controls, which effectively constituted a "cyber amendment," were a bid "to curtail the proliferation of 'active' or 'offensive' cyber technologies [that are] used to initiate offensive cyber attacks or actively mine and analyze protected data."[60]

ARMS AND DUAL-USE GOODS AND TECHNOLOGIES, http://www.wassenaar.org/participants/index.html (last visited Sept. 8, 2015).

[55] *See* RICHARD F. GRIMMETT, CONG. RESEARCH SERV., RS20517, MILITARY TECHNOLOGY AND CONVENTIONAL WEAPONS EXPORT CONTROLS: THE WASSENAAR ARRANGEMENTS 3 (2006), http://www.fas.org/sgp/crs/weapons/RS20517.pdf.

[56] *Guidelines & Procedures, including the Initial Elements*, *supra* note 52, at 4.

[57] *See supra* Part I (explaining the dangers emanating from cyberspace).

[58] *See* Sam Jones, *Arms deal sets limits on cyber technologies*, FIN. TIMES, Dec. 15, 2013, http://www.ft.com/cms/s/0/d4653c82-641d-11e3-98e2-00144feabdc0.html (explaining that leaders of Wassenaar Arrangement member states were particularly concerned about "the notion that technologies may end up in the hands of terrorist groups or hostile organisations and be used to thwart western surveillance operations or mount cyber attacks."). *See also* Willie Jones, *Treaty Limiting Weapons Exports Updated to Include Cyberweapons*, IEEE SPECTRUM, Dec. 6, 2013, http://spectrum.ieee.org/riskfactor/telecom/security/treaty-limiting-weapons-exports-updated-to-include-cyberweapons ("Diplomats representing several Western governments are huddling in Vienna this week in the hopes of finalizing new, Internet-related additions to the Wassenaar Arrangement. That pact—under which the United States, Russia, Japan, France, Germany and dozens of other signatories agree to strictly limit exports of certain weapons—is being updated in order to control access to complex surveillance and hacking software and cryptography. These countries hope to keep sophisticated cyberweapons out of what they consider to be the wrong hands despite explosive growth (pun intended) in the cybersnooping market.").

[59] *Plenary Statement: 2013 Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES 1 (2013), http://www.wassenaar.org/publicdocuments/2013/WA%20Plenary%20Public%20Statement%202013.pdf.

[60] Daniel Reisner & Doron Hindin, *Caught by surprise: Israel's export control regime and cyber technologies*, WORLDECR, 29 (2014). *See also* Sam Jones, *Cyber war technology to be controlled in same way as arms*, FIN. TIMES, Dec. 4, 2013, http://www.ft.com/cms/s/0/2903d504-5c18-11e3-931e-00144feabdc0.html (describing the December 2013 Wassenaar Arrangement meeting as one in which

¶13 The cyber amendment was manifested in a number of changes to the Wassenaar Arrangement's control list of dual-use goods and technologies; two changes called for member states to apply new export controls to software.[61] One such change was the addition of category 5.A.1.j, which mandates export controls on certain forms of software and associated goods, specifically "IP network communications surveillance systems or equipment, and specially designed components therefor."[62] The technology in question must perform certain functions on a "carrier class IP Network" and be "specifically designed" to carry out specified processes.[63] The former requires "[a]nalysis at the application layer," "[e]xtraction of selected metadata and application content," and the "indexing" of this extracted data.[64] The latter requires that the technology was designed either for the "[e]xecution of searches on the basis of 'hard selectors'" or for "[m]apping of the relational network of an individual or of a group of people."[65]

¶14 The other change was the addition of category 4.A.5, which calls on member states to apply export controls to "[s]ystems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, 'intrusion software.'"[66] The Arrangement defines "intrusion software" as:

> "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.[67]

---

member states were trying to reach "an agreement to put sensitive cyber security technologies on the same footing as regular armaments").

[61] Sam Jones, *supra* note 58 (explaining that the cyber amendment called on Wassenaar Arrangement members to place controls on "sales of internet communications surveillance systems and intrusion software").

[62] *List of Dual-Use Goods and Technologies and Munitions List*, THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES 81 (2013), http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/WA-LIST%20%2813%29%201.pdf.

[63] *Id.* Category 5.A.l.j reads in full:

> IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:
>
> 1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone): a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
>
> b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
>
> c. Indexing of extracted data; and
>
> 2. Being specially designed to carry out all of the following:
>
> a. Execution of searches on the basis of 'hard selectors'; and
>
> b. Mapping of the relational network of an individual or of a group of people.

[64] *Id.*

[65] *Id.*

[66] *Id.* at 73.

[67] *Id.* at 209.

The Arrangement defines the term "software" as "[a] collection of one or more 'programmes' or 'microprogrammes' fixed in any tangible medium of expression."[68]

¶15 Both additions to the Wassenaar Arrangement are meant to address threats posed by cyber technology, focusing primarily on software that facilitates data mining and analysis. Software qualifying under the Arrangement's revised rubric is now subject to export controls.

V. THE PROBLEMATIC NATURE OF THE 2013 CYBER AMENDMENT

¶16 Despite the hoopla surrounding the changes made at the Wassenaar Arrangement's December 2013 meeting, the cyber amendment may prove to be ineffective in controlling the proliferation of dangerous cyber technologies for historical, institutional, and theoretical reasons.

A. Historical Argument

¶17 Attempts to control the flow of technology across borders have not always been successful. The most relevant failure in recent memory is the U.S.-sponsored effort to restrict the export of encryption technology via the Wassenaar Arrangement in the late 1990s.

¶18 An encryption program generally encodes information in "an unintelligible form"[69] and thereby ensures the "confidentiality of communications."[70] More technically:

> Encryption permits transformation of passwords or messages into a form that cannot be understood without access to special information necessary to decode the password or message. Messages are scrambled by application of a mathematical algorithm. The algorithm allows the user to select a key. The key allows the user to decrypt messages. Encryption strength increases with the length of the key. Key length is generally measured in bits.[71]

Encryption technology is dual-use in that it can be used to, for instance, protect consumer data[72] (a civilian purpose) and intercept enemy communications during armed conflict and prevent terrorist attacks[73] (military purposes).

---

[68] *Id.* at 218. The term "programme" is given the following definition: "A sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer." *Id.* at 214. A "microprogramme" is defined as "[a] sequence of elementary instructions maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction register." *Id.* at 211.

[69] Mark T. Pasko, *Re-Defining National Security in the Technology Age: The Encryption Export Debate*, 26 J. LEGIS. 337, 337 (2000).

[70] Corr, *supra* note 32, at 484.

[71] *Id.* at 484 n.174 (quoting Bernadette Barnard, *Leveraging Worldwide Encryption Standards via U.S. Export Controls: The U.S. Government's Authority to "Safeguard" the Global Information Infrastructure*, 1997 COLUM. BUS. L. REV. 429, 433-35 (1997)).

[72] *See, e.g.*, Sophie Curtis, *Small businesses urged to encrypt data after London sole trader fined £5,000*, TELEGRAPH, Sept. 26, 2014, http://www.telegraph.co.uk/technology/internet-security/10336836/Small-businesses-urged-to-encrypt-data-after-London-sole-trader-fined-5000.html.

[73] *See* Thinh Nguyen, *Cryptography, Export Controls, and the First Amendment in Bernstein v. United States Department of State*, 10 HARV. J.L. & TECH. 667, 668-69 (1997) ("For millennia, people have

¶19 The potential for encryption programs to be exploited by criminal elements galvanized many jurisdictions—including the European Union[74] and the United States[75]—to regulate encryption technology exports to varying degrees. The U.S. government has long had an exceptional interest in controlling cryptographic exports because of the role that encryption plays in the U.S. economy[76] and the U.S. law enforcement system.[77] Thus, Washington has long imposed severe restrictions on exports of encryption technology.[78] The U.S. lobbied to extend those restrictions beyond its borders at a 1998 Wassenaar Arrangement meeting and was successful. As a result, the Arrangement placed encryption technology on the dual-use list and Arrangement members specifically agreed to restrict the export of encryption software with numerical keys above 64 bits in length.[79]

---

employed cryptography as a tool for securing communications, and for equally as long, other people have tried to decode those messages. During World War II, the Allies were able to break a secret German code, called Enigma. With this capability, they were able to locate and sink large numbers of German U-boats and obtain advanced information about German military operations that was critical to the campaign in Europe. Similar code-breaking ability also allowed the United States Navy to intercept the Japanese fleet in one of the most decisive battles in the Pacific—the Battle of Midway. During the Cold War, signals intelligence provided information about the Soviet Union's military capabilities, the downing of Korean Airlines Flight 007, and Libyan involvement in the bombing of the La Belle Discotheque in West Berlin. More recently, intercepted communications have been used to reveal unfair trading practices by competing nations, monitor proliferation of weapons of mass destruction, enforce international sanctions, identify conventional military threats, and prevent terrorism.") (citations omitted).

[74] Nathan Saper, *International Cryptography Regulation and the Global Information Economy*, 11 NW. J. TECH. & INTELL. PROP. 673, 682 (2013) ("Cryptography in the European Union (EU), like in the U.S., is free to use domestically, but faces restriction on its export.").

[75] *See, e.g.*, Pasko, *supra* note 69 ("While encryption offers American industry a tremendous advantage in conducting its business by ensuring that transactions and industrial secrets are kept safe, encryption also offers many opportunities for misuse. Criminal activities that use encryption technology to their advantage, such as terrorism, organized crime, and industrial espionage have prompted the federal government to enact strong laws regulating encryption in order to prevent such misuse."); Saper, *supra* note 74, at 677 ("The United States pioneered the efforts to regulate encryption during the Cold War.").

[76] *See* Shotwell, *supra* note 34, at 339 (explaining that some financial transactions in the United States are protected by encryption technology).

[77] *See* Karim K. Shehadeh, *The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests*, 15 AM. U. INT'L L. REV. 271, 283-84 (1999) ("Essentially, law enforcement advocates argue that widespread use of encryption would hamper intelligence gathering and undermine the ability of law enforcement to prevent crime. A recently published Federal Bureau of Investigation ("FBI") report states that '[e]ncryption can also be used to conceal criminal activity and thwart law enforcement efforts to collect critical evidence needed to prevent, solve and prosecute serious and often violent criminal activities, including illegal drug trafficking, organized crime, child pornography, and terrorism.' For instance, law enforcement officials cite examples where strong encryption frustrated court-authorized crime interdiction efforts. Recent terrorist incidents also heighten fears that strong encryption has already become a vital tool used by terrorists and drug cartels to evade detection by law enforcement officials.") (citations omitted).

[78] *See* Ioannis Iglezakis, *Regulation of Cryptography and Other Dual-use Goods*, *in* CYBER LAW IN GREECE 67, 71 (Dimitrios Maniotis, Michail-Theodoros Marinos, Apostolos Anthimos, Ioannis Iglezakis, & George Nouskalis, eds., 2011) ("The USA has imposed severe restrictions on cryptography exports. The export of cryptographic products was subject to the International Traffic in Arms Regulation (ITAR) until 1996 and then exports were transferred to the Department of Commerce under the Export Administration Regulations (EAR). ITAR restricted export of 'dual-use' cryptography, which was included in the munitions list.").

[79] *See* Shehadeh, *supra* note 77, at 298.

¶20 A mere month after the meeting, however, the Arrangement's consensus on encryption technology began to break. The French government, citing "its desire to improve the ability of its citizens to protect their confidential communications and its wish to remove obstacles to the growth of e-commerce," announced that it would drop "all controls on encryption technology up to 128-bits."[80] Other Arrangement members, namely Germany and Finland, opposed any restrictions whatsoever on the export of encryption software.[81] And, further undermining the Arrangement's consensus, non-members with fewer controls on encryption technology ended up benefitting from the Arrangement's restrictions. Switzerland, for instance, quickly became a thriving center for encryption-software production.[82]

¶21 Finally, because of the widespread use of the Internet, export controls on encryption technology eventually "lost any effect."[83] Professor Ioannis Iglezakis explains, "[S]ince encryption programs can be downloaded from everywhere in seconds . . . it seems impossible for countries to limit dissemination of such programs."[84] Eventually, the ineffectiveness of these export controls forced the United States "to rethink its encryption priorities and develop a new strategy."[85]

¶22 The cyber amendment appears strikingly similar to the encryption-related amendment passed in the late 1990s. That is, analogous to encryption technologies, many of the cyber technology programs added by the recent amendment are dual-use, software-based products. For this reason, the failure of the Wassenaar Arrangement to control the export of encryption software lends support to the theory that the cyber amendment will also likely fail.

B. Institutional Argument

¶23 The Wassenaar Arrangement's effectiveness is seriously hindered by inadequate enforcement rules and the lack of a ban on undercutting; both defects are rooted in the Wassenaar Arrangement's written guidelines. These organizational weaknesses stymie the Arrangement's ability to control the cross-border flow of cyber technologies.

1. Lack of Binding Enforcement Provisions

¶24 The Wassenaar Arrangement is *multilateral* in scope. Nevertheless, each Arrangement member must take two distinct *unilateral* steps for the regime to function properly: refrain from thwarting the enactment of collectively beneficial regulations and refrain from disregarding collectively beneficial regulations that have already been enacted. The Arrangement's guiding documents contain no provisions for persuading

[80] Pasko, *supra* note 69, at 351.

[81] Shotwell, *supra* note 34, at 339.

[82] Iglezakis, *supra* note 78 ("[S]ome countries (e.g., Switzerland) have benefitted from this situation by promoting the lack of controls in their territory.). *See also* Shehadeh, *supra* note 77, at 275 ("[W]hile United States encryption exporters were frustrated by domestic export policies that remained more restrictive than Wassenaar, foreign manufacturers were operating in less restrictive environments.").

[83] Iglezakis, *supra* note 78.

[84] *Id.* In an interconnected and globalized world, controlling the export of intangible products, including encryption programs, is inherently difficult. *See infra* Part V.C.

[85] Pasko, *supra* note 69, at 351.

member states that are obstinate during the enactment process or for punishing member states that refuse to abide by Arrangement regulations. Thus, the regime can be rendered ineffectual with regard to cyber technology if (1) any member states refuse to add previously unregulated forms of cyber technology to the Wassenaar Arrangement's control list of dual-use goods and technologies or (2) any member states fail to abide by the strictures of the cyber amendment or any other Wassenaar Arrangement regulation.

¶25 Because the Wassenaar Arrangement operates on the principle that all decisions must be supported by all members, the first unilateral step that every member state must take is to abstain from obstructing the regime's consensuses on controlled items and controlled destinations.[86] In theory, the consensus-based system protects each state's individual interests; at the same time, the system elevates a single state's individual interests above the group's collective interests. This is problematic when conflicting interests arise among Arrangement members. The incentive to sell certain goods to certain customers, for instance, might compel countries to act against collective interests.[87] Even the North Atlantic Treaty Organization—which has a system of collective defense that forces at least some alignment in the political and security interests of member states—is not immune to individual economic motivations taking precedence over other considerations; the French government's initial reluctance to cancel its €1.2 billion contract to sell helicopter assault ships to Russia, despite pleas from France's NATO allies following the downing of Malaysia Airlines Flight 17 by Russian-backed separatists in Ukraine,[88] was only the latest and most high-profile example of this incentive in action.

¶26 The second unilateral step that every Wassenaar Arrangement member takes is to put the regime's consensus-based, collectively agreed-upon control lists into action. Much like the prior step, this is ultimately a matter of discretion. That is, the Arrangement's guiding documents guarantee that "[t]he decision to transfer or deny transfer of any item will be the sole responsibility of each Participating State. . . . All measures undertaken . . . will be in accordance with national legislation and policies and will be implemented on the basis of national discretion."[89] But since the Arrangement's written guidelines do not include any enforcement mechanisms, the Arrangement imposes "no obligation on its signatories to enact domestic legislation consistent with its provisions."[90] Furthermore, even if a member state chooses to pass laws that effectuate the purposes of the Arrangement, that member state faces no penalty from the Arrangement for failing to enforce those laws. This point is encapsulated by the following conversation between Connecticut Senator Joseph Lieberman and the U.S. State Department's Senior Advisor for Arms Control and International Security John Holum during a congressional hearing on the Wassenaar Arrangement:

---

[86] *See supra* Part III (explaining the Wassenaar Arrangement's consensus-based decision-making system).

[87] *See infra* Part V.C.1 (discussing the economic incentives underlying state behavior).

[88] *See* Hugh Carnegy & Peter Spiegel, *Row erupts over French warship ahead of European sanctions talks*, FIN. TIMES (July 22, 2014), http://www.ft.com/intl/cms/s/0/36d15660-1163-11e4-a17a-00144feabdc0.html. Note that France decided to suspend delivery of the helicopter assault ships in late 2014 when the situation in Ukraine worsened. *See* Stacy Meichtry & Gregory L. White, *France Suspends Delivery of Warship to Russia*, WALL ST. J. (Nov. 25, 2014), http://www.wsj.com/articles/france-halts-plans-to-deliver-warship-to-russia-1416919199.

[89] *Guidelines & Procedures, including the Initial Elements*, *supra* note 52, at 3.

[90] Shehadeh, *supra* note 77, at 297.

> Senator Lieberman[:] Help me understand. When a nation, when a member Nation of Wassenaar violates the agreement by exporting an item on the agreed upon list, what are the sanctions that are possible?
>
> Mr. Holum[:] Well, there are no sanctions because ultimately the decision making belongs to the countries.[91]

¶27 With member states free to choose whether to enact controls on listed items and free to choose whether to enforce any enacted controls, reaching a consensus on controlled items and controlled destinations—the first unilateral action described above—turns out to be of little consequence. By virtue of their membership in the Wassenaar Arrangement, members are not bound to do anything at all. In this light, the Arrangement is nothing more than an organization for sharing information about export controls *without* the institutional teeth to actually control exports.

2. Lack of a Rule Forbidding Undercutting

¶28 *a) Undercutting Explained.*—Unlike the other three multilateral export control regimes, the guidelines governing the Wassenaar Arrangement do not incorporate a rule forbidding undercutting, or a "no undercut rule,"[92] which would prohibit members of an export control regime from exporting "any listed item or items that had been officially denied an export license by another member."[93] Professor Daniel Joyner explains the importance of such a rule:

> When a denial of an export license for an item on a control list is made at the national level, member states under this rule are to notify the regime. This is a *crucial* element in ensuring member states that the restrictive policies of the regime will not be abrogated to the financial gain of one or a few members, to the corresponding loss of the remainder of member states whose positions have thereby been undercut and to the mooting of regime principles.[94]

¶29 In lieu of a proper no undercut rule for dual-use goods like cyber technology, the Wassenaar Arrangement provides for notification procedures. These procedures are primarily described in three paragraphs: paragraph 4 of section II and paragraphs 1 and 2 of section V. Paragraph 4 of section II spells out the steps that member states must take in notifying other members about denials of export requests:

---

[91] *The Wassenaar Arrangement and the Future of Multilateral Export Controls: Hearing before the United States Senate Committee on Governmental Affairs*, 106th Cong. (2000), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-106shrg64899/html/CHRG-106shrg64899.htm.

[92] Joyner, *supra* note 35, at 185 n.8 ("The Wassenaar Arrangement is the only one of the [four multilateral export control] regimes without these denial notification/no undercut policies.").

[93] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-1095, EXPORT CONTROLS: CHALLENGES WITH COMMERCE'S VALIDATED END-USER PROGRAM MAY LIMIT ITS ABILITY TO ENSURE THAT SEMICONDUCTOR EQUIPMENT EXPORTED TO CHINA IS USED AS INTENDED 10 (2008).

[94] Joyner, *supra* note 35, at 185 (emphasis added).

> 4. In accordance with the provisions of this Arrangement, Participating States agree to notify transfers and denials. These notifications will apply to all nonparticipating states. However, in the light of the general and specific information exchange, the scope of these notifications, as well as their relevance for the purposes of the Arrangement, will be reviewed. Notification of a denial will not impose an obligation on other Participating States to deny similar transfers. However, a Participating State will notify, preferably within 30 days, but no later than within 60 days, all other Participating States of an approval of a licence which has been denied by another Participating State for an essentially identical transaction during the last three years.[95]

Paragraphs 1 and 2 of section V provide additional procedural instructions regarding notifications:

> 1. Participating States will notify licences denied to non-participants with respect to items on the List of Dual-Use Goods and Technologies, where the reasons for denial are relevant to the purposes of the Arrangement.
>
> 2. For the Dual-Use List, Participating States will notify all licences denied relevant to the purposes of the Arrangement to non-participating states, on an aggregate basis, twice per year.[96]

Conspicuously missing from the three cited paragraphs is a rule forbidding member states from exporting dual-use items to a recipient after receiving notification that a fellow Arrangement member denied that recipient an export license. The closest the guidelines come to such a rule is the "essentially identical transaction" provision in paragraph 4 of section II, and that provision is extremely limited in nature: it only applies to sensitive items and it only mandates notification—not denial—within a maximum of 60 days after a license approval.[97]

¶30 *b. Undercutting in Action.*—A no undercut rule's impact is illustrated best via hypothetical. Suppose a multilateral export control regime called the "Lumber Control Regime" is created to control the export of lumber. Suppose further that a type of lumber called "olivewood" falls within a category of the Lumber Control Regime's control list. Finally, suppose the countries of "Woodland" and "Timberstan" are founding members of

---

[95] *Guidelines & Procedures, including the Initial Elements*, *supra* note 52, at 3.

[96] *Id.* at 5.

[97] *See* GRIMMETT, *supra* note 55, at 5 ("The Arrangement does not prohibit a participating country from making an export to a particular destination that has been denied by another participant (this practice is called 'undercutting'). But participants are required to notify other participants within 60 days, and preferably within 30 days, after they approve a license for an export of sensitive dual-use goods that are essentially identical to those that have been denied by another participant during the previous three years."). *See also* Jaffer, *supra* note 49, at 521-522 ("[T]he Wassenaar Arrangement contains only the weakest of provisions to assist member nations in ensuring that their export license denials are not undercut by other member nations. The no undercut provisions contained in the Wassenaar Arrangement require member nations to provide information about exports they deny, as well as notification when a member transfers technology or goods that are essentially identical to products denied by other members.") (citations and internal quotation marks omitted).

the Lumber Control Regime but the country of "Pariahguay" is deliberately excluded from membership because it is widely considered to be a state sponsor of terrorism. When a Woodland company applies to the Woodland government for a license to export olivewood to Pariahguay and the Woodland government rejects the company's application, the existence of a no undercut rule matters a great deal. *With* a no undercut rule in place, Woodland's subsequent notification of the rejection forbids all members of the Lumber Control Regime from exporting olivewood to Pariahguay. *Without* a no undercut rule, however, Woodland's notification becomes a notification—if not an advertisement—that Pariahguayan companies seek to import olivewood. Most importantly, nothing precludes Timberstani political leaders from approving the applications of Timberstani companies eager to export olivewood to Pariahguay. Woodland's rejection of an export license could thereby facilitate the derogation of the Lumber Control Regime's principles.

¶31 As demonstrated in the above hypothetical, the absence of a no undercut rule works against the Wassenaar Arrangement because "[a] country denying an export license essentially notifies all other members of a sales opportunity."[98] Accordingly, this situation "may actually create a perverse incentive for the denying member to decline to report the denial because of the concern that it will simply be providing other members with an export opportunity."[99] No wonder the Arrangement currently receives "scant attention from the policy community" and "ridicule from the arms lobby."[100]

C. Theoretical Argument

¶32 There are three theoretical reasons that the cyber amendment to the Wassenaar Arrangement will fail to stifle the dissemination of destabilizing cyber products. First, member states and companies in those member states are incentivized to sell exports—such as cyber products—to as many buyers as possible. Second, keeping cyber technology within a nation or group of nations will be problematic as advances in the technology are made in an increasingly borderless world. Third, the intangibility inherent in software products makes it well-nigh impossible to control their flow across borders.

1. Economic Incentives Motivate Governments and Private Actors to Ignore the Cyber Amendment

¶33 The Wassenaar Arrangement's unenforceability[101] renders it dependent on the voluntary compliance of governments and businesses.[102] The private sector did not always

---

[98] Michael D. Klaus, *Dual-Use Free Trade Agreements: The Contemporary Alternative to High-Tech Export Controls*, 32 DENV. J. INT'L L. & POL'Y 105, 115 (2003) (citation omitted).

[99] Jaffer, *supra* note 49, at 522.

[100] William W. Keller & Janne E. Nolan, *Proliferation of Advanced Weaponry: Threat to Stability*, *in* THE GLOBAL CENTURY: GLOBALIZATION AND NATIONAL SECURITY 785, 800-01 (Richard L. Kugler & Ellen L. Frost eds., 2002).

[101] *See supra* Part V.B.1 (describing the Wassenaar Arrangement's enforceability problems).

[102] *See* Heinz Gartner, *The Wassenaar Arrangement (WA): How it is Broken and Needs to be Fixed*, 24 DEF. & SEC. ANALYSIS 53, 54 (2008) ("The WA is not a traditional arms control and disarmament agreement, as it is not legally binding on the state parties. Enforcement relies on co-operation and voluntary compliance, with governments and industries representing the two most important actors in the agreement's dynamics.").

play a significant role in dual-use technology innovation, as Professors William Keller and Janne Nolan explain:

> From the 1950s at least through the 1970s, the lead investor in communications, computers, and semiconductors in the United States was the Department of Defense. Pentagon research and development accounted for some of the most significant technical advances, such as supercomputers, geosynchronous satellites, and integrated circuitry. Strict government controls over research and development minimized unregulated technological diffusion and formed the basis for restrictive instruments such as export controls and supplier cartels. Today, this situation is reversed.[103]

Concerning this reversal, Professor Joyner further explains:

> [P]roduction of dual use technologies has shifted in large degree to elements of the private sector, as national governments have found that higher quality and lower prices are available 'off the shelf' in private markets. This shift has had the result of significantly decentralizing the production of sensitive items and requiring increased coordination between the private and public spheres.[104]

As both government institutions and private sector institutions are integrally involved in the development of dual-use technology, their collaboration is a sine qua non for controlling exports of that technology. In other words, for an export control regime like the Wassenaar Arrangement to work, companies seeking to export certain items must apply to their national governments for export licenses and only proceed with sales upon receiving licenses. However, controlling exports this way is extraordinarily difficult because impeding sales in foreign markets runs counter to the interests of all of all parties involved, especially private sector businesses. That is, Wassenaar Arrangement member states—which are individually responsible for controlling exports but are themselves incentivized to violate the Agreement and allow as many exports as possible—must rely on the cooperation of profit-seeking private sector companies with essentially unbalanced incentives to sidestep the Agreement.

¶34 The mostly democratic and mostly capitalist members of the Wassenaar Arrangement face a strategic trade-off when it comes to export controls. On the one hand, national leaders are motivated to protect their nations' security by curtailing the movement of potentially dangerous technologies. On the other hand, national leaders are motivated to minimize regulations that hamper the economic activities of tax-paying companies that employ members of their electorates.[105] These two conflicting incentives are apparent in

---

[103] Keller & Nolan, *supra* note 100, at 786.

[104] Joyner, *supra* note 35, at 186.

[105] *See, e.g.*, Collins, *supra* note 44, at 108 ("Export controls, through the implementation of domestic policy and by participation in international agreements, evoke the importance of a nation's most delicate balancing act: national security vs. economic competitiveness."). Note that there may not necessarily be a contradiction between a country pursuing its security interests and its economic interests simultaneously when exporting defense and dual-use items. *See* Michael Hirsh, *The Great Technology Giveaway?*,

the actions taken by Arrangement members, who claim that they are "willing to support general WA [Wassenaar Arrangement] guidelines that address the concerns of all countries" but nevertheless "consistently and simultaneously oppose specific controls that might negatively impact their own export policies and decisions."[106]

¶35 That same strategic trade-off does not apply to businesses, which have no need to appeal to a security-sensitive electorate. Instead, for-profit enterprises generally seek to earn money for the benefit of owners or shareholders.[107] Private sector prioritization of profits is intuitive, has been borne out innumerable times by the actions of businesses,[108] and is especially true now that the existential threat posed by the Cold War heating up has vanished.[109] In fact, businesses are subject to such compelling economic incentives that, when faced with regulations akin to the cyber amendment, many might simply relocate to jurisdictions with fewer regulations. Due to globalization, businesses "set up shop wherever capital, labor, and market destinations make the most economic sense."[110]

¶36 Software companies that produce dual-use cyber technology can easily exploit the fact that programs can be sent to customers from any place with a functional Internet connection. Moreover, a software company's only two indispensable factors of production are computers and qualified personnel; since neither factor is inordinately difficult to move across borders, software companies face relatively low transfer costs. These companies are

---

FOREIGN AFFAIRS, Sept./Oct. 1998, http://www.foreignaffairs.com/articles/54383/michael-hirsh/the-great-technology-giveaway ("The idea that national security and commercial interests trade off—that every time you sell a satellite overseas, you make a profit but lose a little bit of your military edge—harks back to a time when CIA bean counters worried over every uptick in Soviet technology, and when the U.S. defense industry was sequestered in top-secret grandeur, spending untold billions on weapons designed exclusively for the Pentagon, with older generation models going to America's Cold War allies. Today the situation could not be more different.") Some have even argued that an exporting country's security interests and economic interests go hand in hand. *See* Corr, *supra* note 32, at 444 n.3 ("Many in the Clinton Administration, including the Defense Department, recognized that the military increasingly relies on technological superiority, and that the civilian commercial sector, not the military industrial sector, drives technology. That sector, in turn, is increasingly dependent on exports. It is therefore tautological that for export control purposes you cannot at once strangle and promote the source of your technological superiority.") (citations omitted).

[106] Gartner, *supra* note 102, at 55.

[107] *See, e.g.*, *id.* ("Although the WA export control list could provide guidelines for future export decisions and export conduct for both state and non-state actors, it has little impact on specific export decisions. These remain largely driven by profit, growth, and investment opportunities. The main private actors involved in the WA—the exporting companies—remain vehemently opposed to the strict enforcement of effective export control measures.").

[108] *See, e.g.*, Jing-Dong Yuan, *The Future of Export Controls: Developing New Strategies for Nonproliferation*, 39 INT'L POLICY 131, 142 (2002) ("In certain cases, companies may simply disregard the implications of their technology transfers and, indeed, may cheat to obtain export licenses that allow a business advantage over potential competitors. For instance, in the late 1980s, a number of West German companies were found guilty of illegal exports of nuclear, chemical, and rocket items and relevant technologies to Middle Eastern countries, including Libya.") (citation omitted).

[109] *See, e.g.*, Hirsh, *supra* note 105 (describing how, in the post-Cold War era, American exporters such as Hughes Electronics, AT&T, Loral Space & Communications, and United Technologies carried out "intense corporate lobbying" to pressure the U.S. government to reclassify certain munitions as dual-use items and thereby simplify and expedite the export process for those items); Keller & Nolan, *supra* note 100, at 797 (noting that, following the Cold War, the desire of businesses "to sell into international markets has slowly but irresistibly taken precedence [over concerns about the diffusion of advanced technology].").

[110] Yuan, *supra* note 108, at 141; *see also infra* Part V.C.2 (describing the behavior of companies in an increasingly globalized world).

therefore well positioned to conduct regulatory arbitrage by moving their operations whenever they reassess their regulatory cost-benefit analyses.[111] In fact, this is precisely what happened when the Wassenaar Arrangement placed strict controls on dual-use encryption technologies; over time, production of encryption software "thrived in countries with fewer controls."[112]

¶37 Thus, the two actors tasked with carrying out the directives of the Wassenaar Arrangement—the governments of Arrangement members and the private sector actors doing business in member states—are subject to strong incentives to disregard those directives. And, in practice, "aggressive and effective lobbying" by export-oriented companies has made member states progressively more tolerant of the fact that those companies openly flout many of the Arrangement's regulations.[113]

2. Innovations in Cyber Technology Will Occur in a Globalized World

¶38 *a. Whither Borders?*—All export control regimes presuppose the existence of borders; the term "export" is meaningless in a borderless world. Consequently, as borders shrink in terms of significance, export control regimes like the Wassenaar Arrangement will likewise shrink in terms of significance. And borders are indeed shrinking; the world economy is currently characterized by, inter alia, the "globalization of business" and "rapid technological innovation."[114] These two phenomena mutually and continually reinforce one another: technological innovations fuel increased globalization, increased globalization fuels yet more technological innovations, and so on. The speed and extent of technological innovation, most notably in the realm of communication, has transformed the global economy. Only historical comparison elucidates the sheer magnitude of technology's impact:

> In 1830, for instance, it would have cost around $2,000 of today's money to transmit one letter from London to India, and it could have taken up to six months to reach its destination. Today, a letter can be shipped internationally for $3 and reach its destination in only a few days. Going beyond that, the world is flush with near-instantaneous communication of all kinds, from tweets to SMS texts, and from instant messenger software to

---

[111] Note that seemingly immovable factors of production, such as factories, may also be moved across borders with relative ease. Jan Clenski, *Moving with the times: Factory relocation forms basis for business model*, FIN. TIMES, Nov. 16, 2010, http://www.ft.com/cms/s/0/645e407c-f05e-11df-88db-00144feab49a.html. Nevertheless, a company that does not rely on any immovable assets is at least theoretically freer to relocate abroad than a company that does rely on immovable assets because the former literally has fewer things to transport.

[112] Iglezakis, *supra* note 78; *see also* Shehadeh, *supra* note 77, at 300-01 ("[S]tringent United States laws have led to a significant increase in the amount of encryption products that are available from foreign manufacturers. For instance, The Arrangement does not require members to control the intangible export of encryption software in cyberspace. In the United States, however, current regulations restrict the distribution of encryption software via the Internet. The foregoing has allowed software manufacturers from newly emerging countries to make their encryption software available over the Internet, and establish a reputation for security that United States-exported products cannot match in foreign markets.").

[113] Gartner, *supra* note 102, at 55.

[114] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-03-43, NONPROLIFERATION: STRATEGY NEEDED TO STRENGTHEN MULTILATERAL EXPORT CONTROL REGIMES 24 (2002).

> calls via VoIP (voice-over Internet protocol). Technological change means not only that most types of global flows are growing in volume but also that global networks of flows are evolving more rapidly. As a result, the world is increasingly connected and dynamic—and potentially more volatile.[115]

The connectedness, dynamism, and potential volatility described above apply to cyber technologies, which, as a result of innovation and globalization, can currently be exported in myriad ways. For instance, technologies may be "exported" by shipping data storage devices abroad, traveling with data storage devices, transmitting data via the Internet, allowing foreigners access to data *inside* of the exporting country, and allowing foreigners and non-foreigners access to data *outside* of the exporting country.[116] Since controlling exports is naturally harder when the exporting process takes so many forms, globalization presents a formidable procedural challenge to export controls. On a more fundamental level, however, globalization poses a conceptual challenge to export controls. With borders becoming "porous" and technologies and information become "more transportable," the inevitable result is that the "the underlying assumptions of programs to stem the flow of dual-use technologies and commodities come under question."[117]

¶39 *b. Multinational Companies and Multinational Teams*—Multinationalism has long been the order of the day for many tech companies in terms of producing and selling products and services. In recent years, research and development in high tech has likewise become a global affair. It is hardly news that companies like Sweden's Ericsson, France's Alcatel-Lucent, South Korea's Samsung, America's Motorola, and Germany's Siemens outsource manufacture operations to places like China, India, Israel, Malaysia, Mexico, and Thailand.[118] Relatively unknown, however, is the fact that businesses use foreign countries as sites for innovation too; all five companies mentioned, for instance, have research campuses in China.[119] San Jose-based eBay has an innovation hub in Tel Aviv.[120] Microsoft, a company headquartered in Redmond, Washington, boasts a research laboratory in Bangalore.[121] To inspire Google employees to be innovative no matter where they sit, the company provides perks like "ski gondolas in the Zurich office, a pub-like

---

[115] MCKINSEY GLOBAL INSTITUTE, GLOBAL FLOWS IN A DIGITAL AGE: HOW TRADE, FINANCE, PEOPLE, AND DATA CONNECT THE WORLD ECONOMY 20 (2014), http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights/Globalization/Global%20flows%20in%20a%20digital%20age/MGI_Global_flows_in_a_digial_age_Full_report.ashx (citations omitted).

[116] *See* Corr, *supra* note 32, at 472-73. *See also* Keller & Nolan, *supra* note 100, at 785 ("Technological change is transforming the context of international security and commerce. The rapid expansion of cross-border trade and the free flow of intellectual as well as financial capital brought on by technological advances have made our national borders porous.").

[117] Shotwell, *supra* note 34, at 336.

[118] *See* THEODORE MORAN, DEALING WITH CYBERSECURITY THREATS POSED BY GLOBALIZED INFORMATION TECHNOLOGY SUPPLIERS 3 (2013), http://www.iie.com/publications/pb/pb13-11.pdf.

[119] *See id.*

[120] *Improving the Customer Experience*, LEADERS, http://www.leadersmag.com/issues/2014.3_Jul/Entrepreneurship/LEADERS-Dafan-Gura-Goldenberg-Parnes-Matalon-Schory-eBay.html (last visited Sept. 8, 2015) ("The Israel Innovation Center (IIC) is a self-contained, off-platform team based in Tel Aviv, Israel…The IIC is part of the newly formed Innovation and New Ventures group, created to act as the center of innovation, which includes creating new businesses, and supporting the eBay Marketplaces businesses and eBay Inc. at a corporate level.").

[121] Dinesh C. Sharma, *Microsoft Research goes to Bangalore*, CNET NEWS, Jan. 12, 2005, http://news.cnet.com/Microsoft-Research-goes-to-Bangalore/2100-1008_3-5533395.html.

meeting room in Dublin, and [a] sidewalk cafe in Istanbul."[122] When innovation occurs transnationally, as it now apparently does, it is hard to pin down the nation to which the fruits of innovators' labors belong. Should source code written in the Lima office of a London-based company be considered a Peruvian or British export?

¶40 At first blush, "rules of origin" offer a tempting solution to the above question because those rules are often used to investigate trade issues, such as "whether a shipment falls within a quota limitation, qualifies for a tariff preference or is affected by an anti-dumping duty."[123] In the Wassenaar Arrangement context, however, rules of origin provide less guidance because the rules "vary from country to country."[124] Given the Wassenaar Arrangement's focus on national discretion, each of the forty-one members is presumably responsible for classifying a given product for export control purposes pursuant to that country's rules of origin. Using this approach to determine the origin of a product that originates from more than one country, however, "can be very complex, sometimes subjective, and time-consuming."[125]

¶41 The process becomes all the more complex, subjective, and time-consuming when the teams that produce an item are themselves multinational. Ever-improving technology allows companies like eBay, Microsoft, and Google to "pick the best brains from anywhere in a global organisation and set them working together in cyberspace."[126] Multinational teams add an additional layer of complexity to export issues because a product is sometimes considered to have been exported to a foreign country the moment that a foreign national is given access to it. This type of export, called a "deemed export," is a "legal fiction" that is "based on the assumption that conveying information to a foreign national will result in the information being relayed to that national's home country."[127] The deemed export rule can be activated in a variety of settings:

> [The settings] range from allowing a foreign national to inspect a product or technical data, to having a conversation with a foreign national. However, the [deemed export] rule applies not only to actual releases, but also to possible releases: if a foreign employee can access a controlled commodity, software, or technology, it could qualify as a deemed export regardless of whether the employee actually accessed the information.[128]

Given the "intangible, amorphous nature of deemed transfers," exporting countries with an operational deemed export rule face "special hazards and difficulties" due to the "increasing use of internal company e-mail servers, or intranets, where proprietary data is

---

[122] *Inside Google workplaces, from perks to nap pods*, CBS NEWS, Jan. 22, 2013, http://www.cbsnews.com/news/inside-google-workplaces-from-perks-to-nap-pods/.

[123] WTO.COM, *Glossary, Rules of Origin,* https://www.wto.org/english/thewto_e/glossary_e/rules_of_origin_e.htm.

[124] *Id.*

[125] VIVIAN C. JONES & MICHAEL F. MARTIN, CONG. RESEARCH SERV., RL34524, INTERNATIONAL TRADE: RULES OF ORIGIN 1 (2012), https://www.fas.org/sgp/crs/row/RL34524.pdf.

[126] Alicia Clegg, *Tactics for remote teamwork*, FIN. TIMES, Feb. 13, 2012, http://www.ft.com/cms/s/0/77c904b6-51b1-11e1-a99d-00144feabdc0.html.

[127] Joseph A. Schoorl, *Clicking the "Export" Button: Cloud Data Storage and U.S. Dual-Use Export Controls*, 80 GEO. WASH. L. REV. 632, 640-41 (2012).

[128] *Id.* (citations and internal quotation marks omitted).

shared among employees, and broad company computer networks where a foreign national may gain access to controlled data and files."[129] Although the rule is not in place in all jurisdictions, it is a factor in certain large export markets such as the United States.[130] Describing the challenges U.S.-based technology companies face because of the deemed export rule, Professors Ron Smith and Bernard Udis write:

> It is now common for U.S. software engineers to work on a program during the day, beam it by satellite to India, Israel, or Russia, where another team works on it during the U.S. night and passes it back the next morning. Controlling such technology transfer raises obvious difficulties for traditional export control mechanisms.[131]

¶42 As increasingly multinational teams in multiple offices of multinational firms collaborate on high-tech products like cyber technology, determining a country of origin for those products—or even figuring out the precise moment that those products have been exported if the deemed export rule applies—will become arbitrary if not altogether impossible. Suppose a source code is written by a team of Canadian, Kenyan, and Japanese nationals working together in the Lima office of a London-based company. If the Canadian writes the code, and then asks his Japanese colleague to review it, and the Japanese colleague subsequently shows the code to their Kenyan teammate, how many times has the code been exported and which country's export rules apply? Is the answer different if the three of them jointly generate the code instead of passing it to one another for editing? A rule that assigns the finished source code to one or another of the five countries would require so much willful ignorance of the other four de facto origins as to be irredeemable.

¶43 *c. Mass Collaboration*—Cross-border collaborations are not limited to the private sector; in more informal environments, people from all over the world use the Internet to collectively generate a variety of things, including software. Professor Yochai Benkler teaches that despite the enduring belief that rational individuals act out of narrowly-defined self-interests, the advent of open-source software in recent years has shown that thousands of volunteers collaborating on a "complex economic project" are capable of "beat[ing] the largest and best-financed business enterprises in the world at their own game."[132] Increased

---

[129] Corr, *supra* note 32, at 475.

[130] Collins, *supra* note 44, at 110 ("In addition to regulating the more traditional exportation of tangible goods, the EAR [Export Administration Regulations] encompasses the more abstract concept of intangible technology releases through the Deemed Export Rule (DER). Despite no formal recognition until 1996, releases of controlled technology to foreign nationals working inside U.S. borders are subject to DER export controls. The DER is not supported by legislative language, a fact recognized in the Congressional debates over reauthorization. The DER stands for the proposition that a legal, foreign worker in the U.S. exposed to controlled technology subject to the EAR has imported that technology to his or her home country solely by virtue of their exposure.") (citations and internal quotation marks omitted). *See also* Corr, *supra* note 32, at 473 ("U.S. companies should be aware that controlled transactions may occur when they hire foreign nationals and allow them access to controlled technology. This type of transfer is termed a "deemed export" because the foreigner's access to the controlled technology is deemed to be a restricted transfer to the foreigner's country of citizenship.").

[131] Smith & Udis, *supra* note 31, at 87.

[132] Yochai Benkler, *Coase's Penguin, or, Linux and The Nature of the Firm*, 112 YALE L. J. 369, 371 (2002). *See also* MCKINSEY GLOBAL INSTITUTE, *supra* note 115, at 42 ("Open-source software projects are an example of the power of online collaboration tools to enable complex collaboration among participants

connectivity, made possible by computer communications networks that have become "faster, cheaper, and more ubiquitous," has brought about "a dramatic change in the scope, scale, and efficacy of peer production."[133] The era of mass collaboration, it seems, has arrived.

¶44 It is difficult to grasp the concept of mass collaboration without an example. The McKinsey Global Institute offers Apache as a case study in which "open-source collaborators are distributed around the globe and rarely, if ever, work in person."[134] According to McKinsey, a single Apache project in which "nearly 400 people provided code and identified close to 3,000 bugs" is evidence of "the immense sophistication and potential of online collaboration tools."[135] McKinsey also notes that Apache is "the most widely deployed web server."[136] Putting aside the laudable sophistication and significant potential value of these types of projects, the hundreds of geographically dispersed collaborators behind a piece of open-source software like Apache make meaningful country of origin identification—let alone export control—into an exercise in futility.

¶45 Admittedly, the dual-use technologies targeted by the cyber amendment, such as intrusion software, do not include web servers like Apache. In principle, however, source code for an intrusion program can just as easily be created, shared, and jointly improved upon as source code for a program like Apache. Any attempt to control the export of an intrusion program—or any controlled cyber technology—would need to comprehensively address the fact that when a single item is the product of individuals located in hundreds of places, it is more the product of our borderless planet than the product of any given country.

¶46 *d. Cloud Computing*—The complications generated by transnational collaborative teams are exponentially compounded by cloud computing, which is already considered "vital to the success of billions of individuals, businesses and entire economies."[137] The "cloud" consists of "a vast network of large computers called servers"[138] that can be located "anywhere in the world with adequate electricity and Internet connectivity."[139] Purchasing cloud services does not entail purchasing a set of physical servers; rather, consumers purchase a "virtual machine" that "behaves like a physical computer but actually utilizes resources from numerous interconnected servers."[140] Crucially, information in the cloud "is automatically allocated to different servers based on a number of factors, and these allocations generally occur without the knowledge of providers or users."[141] The cloud "can be accessed through any Internet-enabled computer" and "it can also be hacked into from anywhere."[142]

---

in multiple locations.")

[133] Benkler, *supra* note 132, at 383.

[134] MCKINSEY GLOBAL INSTITUTE, *supra* note 115, at 42 (citation omitted).

[135] *Id.*

[136] *Id.*

[137] THE NATIONAL FOREIGN TRADE COUNCIL, PROMOTING CROSS-BORDER DATA FLOWS: PRIORITIES FOR THE BUSINESS COMMUNITY 2 (2011), http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf.

[138] Schoorl, *supra* note 127, at 635.

[139] *Id.* at 645.

[140] *Id.*

[141] *Id.* at 635.

[142] *Id.* at 637.

¶47 Perpetually and imperceptibly moving data in the cloud turns the entire current export control paradigm on its head. With electricity and Internet access spreading to every corner of the globe and with users and providers of cloud services mostly unaware of server locations or data movements, data in the cloud will eventually become functionally omnipresent. Imagine if the Canadian, Kenyan, and Japanese programmers in that Lima office of a London-based company store their source code in the cloud. If the source code is a multinational product that exists everywhere at once, what impact could the cyber amendment to the Wassenaar Arrangement possibly have on that code's ultimate destination?

3. Cyber Technology's Intangibility Makes Control Especially Challenging

¶48 The cyber amendment added two types of software to the Wassenaar Arrangement control list.[143] Since software is defined by the Arrangement as an expression of instructions that direct the actions of a computer,[144] the cyber amendment put export controls over a specific type of information. The problems inherent in controlling information make the cyber amendment particularly unlikely to be effective.

¶49 As a preliminary matter, cyber technology is based on data and is therefore completely unlike the scores of tangible dual-use products that the Wassenaar Arrangement controls. The latter can be physically inspected at a border. The former comprises knowledge and speech in the form of strings of numbers and letters; these intangible technologies can be transferred via intangible mediums of transfer such as telephone calls, emails, and face-to-face conversations between individuals holding disparate passports. Designed to manage tangible exports, conventional methods of export control can do little to prevent the spread of information from one person to another.

¶50 In particular, the advent of modern technology has decimated the odds of information remaining confidential over time. Steven Levy, a journalist who focuses on privacy and technology, explains why:

> The telegraph, telephone, radio, and especially the computer have put everyone on the globe within earshot—at the price of our privacy. It may feel like we're performing an intimate act when, sequestered in our rooms and cubicles, we casually use our cell phones and computers to transmit our thoughts, confidences, business plans, and even our money. But clever eavesdroppers, and sometimes even not-so-clever ones, can hear it all. We think we're whispering, but we're really broadcasting.[145]

Levy may be referring to the difficulties modernity has created for those wishing to keep personal data private, but his insights are applicable to secrets of any nature, including source code. Put simply: efforts to hold back the dissemination of sought-after information inevitably founder. For instance, despite the millions of dollars that the Kremlin poured

[143] *See supra* Part IV (describing the two types of software that the cyber amendment added to the Wassenaar Arrangement).

[144] *See supra* Part IV (providing the Wassenaar Arrangement's definitions of "software," "programme," and "microprogramme").

[145] STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT SAVING PRIVACY IN THE DIGITAL AGE 1 (2001).

into its efforts to silence foreign—especially Western—radio broadcasts in the Soviet Union,[146] the masses invariably obtained access to news from beyond the Iron Curtain. In 1967, Soviet Jews famously found ways to bypass government jamming and ended up "glued to their radios" as they listened to BBC and Voice of America broadcasts about Israel's victory in the Six-Day War.[147] Just as the Union of Soviet Socialist Republics failed to stop information from penetrating its borders in the 1960s, so too the Islamic Republic of Iran failed to keep information from escaping its borders in the 2000s. Following Iran's disputed 2009 presidential election, Tehran's army of cyber-censors could not hide facts, images, or even videos about the regime's gruesome crackdown on protesters from the rest of the world.[148] Not even the legendary Iranian Internet blockade[149] could stand in the way of information speeding down the information superhighway. But data need not be controversial or momentous to be infectious; the numbers and letters behind software programs are as shareable as any news story. After all, packets of computer code are a form of knowledge and, as *The Economist* rightly posits, "[a]ttempting to stop people from generating and spreading knowledge is futile."[150]

VI. CONCLUSION

¶51 Flawed as it may be, the December 2013 amendment to the Wassenaar Arrangement leaves room for measured optimism for at least three reasons.

¶52 First, the Wassenaar Arrangement's successes and failures must be understood in context. The Wassenaar Arrangement is merely an arrangement; it is not and has never been a binding treaty. The Arrangement's non-binding characteristics put it closer to "soft law" than "hard law" on the spectrum of international legalization, and it was precisely this softness that facilitated the compromises that were required to bring the Arrangement into existence in the first place.[151]

---

[146] George W. Woodard, Cold War Radio Jamming, *in* COLD WAR BROADCASTING: IMPACT ON THE SOVIET UNION AND EASTERN EUROPE 51, 53 (A. Ross Johnson & R. Eugene Parta eds., 2010) ("In 1948, the Soviet Union commenced significant jamming of VOA and BBC broadcasts. This jamming had increased almost tenfold by the time jamming ended in 1988. Approximately 200 local and distant (sky-wave) jamming transmitters, with a total output power of approximately three-four megawatts in 1952, had grown by 1988 to approximately 1700 transmitters with an estimated total output power of 45 megawatts […] Operating these transmitters 24 hours per day at an estimated electrical cost of $0.06 per kilowatt-hour amounted to an operational cost of $48 million per year for electricity alone (assuming 50% transmitter efficiency), not including operational and maintenance labor costs, or capital costs. What started in 1948 as jamming of only VOA and BBC had grown by 1988 to include…Deutsche Welle, Kol Israel, Radio Korea, Radio Vatican, Radio Netherlands, and others.").

[147] Yaacov Ro'i, *The Soviet Jewish Reaction to the Six Day War*, *in* THE SOVIET UNION AND THE JUNE 1967 SIX DAY WAR 251, 254 (Yaacov Ro'i & Boris Morozov eds., 2008).

[148] *See* Brian Stetler & Brad Stone, *Web Pries Lid of Iranian Censorship*, N.Y. TIMES, June 22, 2009, http://www.nytimes.com/2009/06/23/world/middleeast/23censor.html.

[149] *See* Declan McCullagh, *Iranians find ways to bypass Net censors*, CNET NEWS, June 18, 2009, http://www.cnet.com/news/iranians-find-ways-to-bypass-net-censors/.

[150] *Cyber-security: The digital arms trade*, THE ECONOMIST, Mar. 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade.

[151] *See* Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54 INT'L ORG. 421, 445 (2000). Professors Abbott and Snidal explain:

> The 1996 Wassenaar Arrangement for national controls on exports of conventional

¶53 Second, the multilateral dialogue that the Arrangement stimulates is no small fry. Cyber threats know no borders and, accordingly, any effort to defend against them within national boundaries simply makes no sense. Export control regimes like the Wassenaar Arrangement are "important promulgators of multilateral norms."[152] These norms are an invaluable tool for pressuring both members and non-members into complying with regime regulations. Indeed, nonproliferation experts praise multilateral export control regimes for "helping set international standards for limiting exports of sensitive items and helping stem proliferation in particular countries of concern."[153]

¶54 Finally, expectations about the Wassenaar Arrangement are so low—the former head of the Wassenaar Secretariat once declared that although the Arrangement has not yielded any "spectacular results," the situation would be worse without it[154]—that there is little chance that the Arrangement has duped or will dupe anybody into a false sense of security.

¶55 For these reasons, the striking mismatch between the cyber dangers we are facing and the limited potential of the December 2013 amendment to protect us should not be a cause for alarm.[155] It should be a call to action. Notwithstanding the lessons of history, not all forms of cyber technology are doomed to go the way of encryption programs. Collective action by members of the international community created the Wassenaar Arrangement in the first place; with still more collective action, the Arrangement's organizational shortcomings can be remedied. Even theoretical challenges, ever a thorn in the side of regulatory schemes, can be managed—to some extent at least—with sufficient creativity. Boundless determination, rather than hopeless fatalism, is the only option we have to protect ourselves. The cyber amendment was a step in the right direction. Having an umbrella in a hurricane is better than having nothing at all.

> weapons and dual-use technologies illustrates the use of soft legalization to facilitate compromise….The United States pressed for a new institution to address post–Cold War security threats like terrorism, regional conflicts, and arms buildups by rogue nations like Iraq. But it faced several barriers to agreement: nearly twice as many nations would have to take part; the 'common enemy' of the Cold War no longer existed; the participating nations had very different attitudes toward particular countries and conflicts; the economic costs of export controls would fall unevenly across countries; and some states were more technically prepared than others to operate a sophisticated export control system. The nonbinding 'arrangement' overcame these barriers by incorporating substantial flexibility in all three elements of legalization.

Id. (citations omitted). Additionally, Professors Abbott and Snidal posit that, besides its tendency to enable compromise between states, soft law is superior to hard law because it "offers more effective ways to deal with uncertainty, especially when it initiates processes that allow actors to learn about the impact of agreements over time." *Id.* at 423.

[152] Joyner, *supra* note 35, at 184-85.

[153] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 93, at 7.

[154] *Id.* at 8.

[155] Indeed, although cyber threats should not be underestimated, it is vital not to overstate the imminence or magnitude of those threats. Scaremongering helps no one. *See generally* Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SEC. J. 39 (2011).