Michigan Technology Law Review

Article 6

2021

Arms Control 2.0: Updating the Cyberweapon Arms Control Framework

Evan Mulbry
University of Michigan Law School

ARMS CONTROL 2.0: UPDATING THE CYBERWEAPON ARMS CONTROL FRAMEWORK

*Evan Mulbry**

ABSTRACT

This Note analyzes multiple problems with the existing arms control framework for cyberweapons as well as surveillance technology and calls for four specific areas of reform. First, the existing framework does not specifically enumerate the software controlled under existing arms control treaties, which can lead to gaps in international export control compliance. Cyberweapons should be enumerated with greater specificity to prevent confusing and disjointed implementation by states. Second, the divide between Wassenaar and Shanghai Cooperation Organization conceptions of what constitutes a cyberweapon reduces the effectiveness of international control because nations do not share an agreed upon cyberweapon definition. States should form a multilateral treaty utilizing a shared definition to ensure cyberweapon exports are regulated by a treaty and include a greater diversity of countries covering a larger share of this market. Third, the Wassenaar Arrangement, the current treaty regulating many cyberweapon exports, fails to impose strict controls on cyberweapons and surveillance technology. Under the Wassenaar Arrangement, cyberweapons and surveillance technology should be listed as "very sensitive items" and subject to additional control because exports can lead to derivative viruses, which multiply the harm of the original export. Finally, the existing framework is unclear in its differentiation between cyberweapons subject to strict control as weapons and those subject to less control as dual-use items. International control lists should include an addendum to the general rule assigning particular types of software to consistently implement each category across jurisdictions.

* J.D. Candidate, May 2022, University of Michigan Law School. I would like to extend my gratitude to Emma Macfarlane, Chaila Fraundorfer, as well as the members of the Volume 28 Notes Office, especially Alex Theodosakis, Narmada Murugan, Landen Haney, Briana Sooy, and Editor-in-Chief Kimberly Parry. Thank you also to my friends for always listening, and my partner for believing in me.

TABLE OF CONTENTS

INTRODUCTION

Imagine a catastrophe striking your community, without physical damage to major infrastructure. Water systems fail. Electricity, telephone, and wireless communication grids fail. All networks are down.[1] Rivers and water systems are contaminated because the computers controlling the chemical balance fail.[2] Critically ill patients begin to pass away as lifesaving machines fail to properly function.[3] This type of catastrophe is what cyberweapons can inflict on society by attacking critical infrastructure. Cyberweapons have evolved as one of the most significant threats to international peace and security since the invention of the atomic bomb.[4] Current analysis focuses on this threat in the context of their impact such as what constitutes an act of war, but with less attention paid to their

1. Beatrice Christofaro, *Cyberattacks Are the Newest Frontier of War and Can Strike Harder Than a Natural Disaster. Here's Why the US Could Struggle to Cope If It Got Hit.*, BUS. INSIDER (May 23, 2019, 5:50 AM), https://www.businessinsider.com/cyber-attack-us-struggle-taken-offline-power-grid-2019-4.

2. *See, e.g.*, *A Cyber-attack on an American Water Plant Rattles Nerves*, ECONOMIST (Feb. 9, 2021), https://www.economist.com/united-states/2021/02/09/a-cyber-attack-on-an-american-water-plant-rattles-nerves.

3. Shashank Joshi, *A Murderous Cyber-Attack Is Only a Matter of Time*, ECONOMIST (Nov. 17, 2020), https://www.economist.com/the-world-ahead/2020/11/17/a-murderous-cyber-attack-is-only-a-matter-of-time.

4. *See, e.g.*, *World Teeters on Cyber-War Brink*, ITWIRE (May 22, 2012, 3:27 PM), https://www.itwire.com/business-it-news/security/54797-world-teeters-on-cyber-war-brink.

acquisition.[5] The United Nations ("UN") stated cyberoperations are governed by international law,[6] but did not delineate the legal boundaries for cyberweapon transfer from government to private actors and transfers across borders from private actors to other governments.[7]

Issues regarding cyberweapon transfers are important because they enable actors with poor human rights records to access sophisticated cyberweapons and surveillance technology. For example, British Aerospace Engineering ("BAE") Systems sold sophisticated cyber technology under the current framework to states such as Saudi Arabia,[8] which has violated numerous human rights according to Amnesty International.[9] While it is impossible to determine whether BAE's software was responsible, this type of sophisticated surveillance software enabled some Gulf States, such as Saudi Arabia, to make social media activists "vanish" during the Arab Spring.[10] One former Saudi Air Force officer noted 90% of the most active campaigners in 2011 have now disappeared.[11] In defending against accusations of impropriety, BAE noted all of its software transfers were in accordance with Danish export laws,[12] which implement major international arms agreements such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (the "Wassenaar Arrangement").[13] However, current international agreements do not include strong enough restrictions that could have prevented this sale.

This example highlights a problem created in the international arms control framework: international controls on cyberweapons including surveillance technology do not accurately reflect the threat they pose to societies. Because surveillance software and other cyberweapons (for example, intrusion software) are controlled items generally,[14] but are not

5. *See, e.g.*, Stephanie Gosnell Handler, *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, 48 STAN. J. INT'L. L. 209, 215–25 (2012).

6. Detlov Wolter, *The UN Takes a Big Step Forward on Cybersecurity*, ARMS CONTROL ASS'N (2013), https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity#source.

7. *See* U.N. Secretary-General, *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/98 (June 24, 2013).

8. *How BAE Sold Cyber-Surveillance Tools to Arab States*, BBC (June 15, 2017), https://www.bbc.com/news/world-middle-east-40276568.

9. AMNESTY INT'L, AMNESTY INTERNATIONAL REPORT 2020/21: THE STATE OF THE WORLD'S HUMAN RIGHTS 309–13 (2021) (mentioning Saudi Arabia's repeat human rights violations, including invoking the Anti-Cyber Crime Law to silence critics).

10. *Id.*

11. *Id.*

12. *Id.*

13. *See About Us*, WASSENAAR ARRANGEMENT, https://www.wassenaar.org/about-us [hereinafter *About Wassenaar Agreement*] (last updated June 22, 2021).

14. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: List of Dual-Use Goods and Technologies and Munitions

escalated to the status of "very sensitive,"[15] their export is less restricted.[16] Implementing stronger controls in the Wassenaar Arrangement and ensuring proper execution by its parties may have blocked this transaction.

This Note argues cyberweapons pose a significant threat to international peace in the coming century and that countries should cooperate to supplement existing international agreements to restrict the cross-border transfer of cyberweapons to and from private actors as well as governments. In doing so, this Note discusses both offensive weapons and surveillance technology as cyber weapons because both fall within the cyber-arms industry.[17] Part I discusses the background of cyberweapon international arms control. Part II outlines the problematic gaps in the current international arms control framework related to cyberweapons. Part III provides solutions to address the unique concerns of cyberweapons and how the global community can take steps to reduce the cross-border transfers of cyberweapons. Part IV summarizes and concludes the Note.

I. BACKGROUND

Stuxnet was a computer virus that began infecting Iranian networks in 2007 and was the world's first identified cyberweapon.[18] American and Israeli operatives originally designed Stuxnet to attack Iranian nuclear infrastructure by infiltrating industrial computers and searching for the Siemens Step 7 software, an industrial software used to control nuclear manufacturing processes.[19] After identifying this software, Stuxnet would update it with code that hijacked different processes to damage nuclear production infrastructure while simultaneously sending updates to the operator that no issues were present.[20] The operator would not be aware there was a problem until the equipment began to self-destruct.[21] Despite Stuxnet's ultimate discovery by Iran, newer versions of the code continued

List, category 2, pt. 5, Dec. 5, 2019, WA-LIST (19) 1 [hereinafter Wassenaar Arrangement, List of Dual-Use Goods], https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf.

15. *See id.* at 178.

16. *See* Daryl Kimball, *The Wassenaar Arrangement at a Glance*, ARMS CONTROL ASS'N, https://www.armscontrol.org/factsheets/wassenaar (last reviewed Dec. 2017).

17. *See, e.g.*, Von Jacob Appelbaum et al., *NSA Preps America for Future Battle*, SPIEGEL INT'L (Jan. 17, 2015, 5:07 PM), https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html (describing the U.S. government as stockpiling cyber-arms including surveillance technology).

18. Joshua Alvarez, *Stuxnet: The World's First Cyber Weapon*, STAN. CTR. FOR INT'L SEC. AND COOP. (Feb. 3, 2015), https://cisac.fsi.stanford.edu/news/stuxnet.

19. *See What is Stuxnet?*, MCAFEE, https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html (last visited Nov. 26, 2021).

20. *Id.*

21. *Id.*

to damage Iranian nuclear infrastructure for several weeks after its initial discovery.[22]

A. *Characteristics of a Cyberweapon*

As one of the original cyberweapons, the Stuxnet example demonstrates three aspects of cyberweapons that differentiate them from conventional kinetic weapons such as bullets and bombs. First, cyberweapons can be designed to target a specific country's systems or infrastructure.[23] The Stuxnet virus was originally designed to only damage Iranian facilities,[24] a characteristic unique to cyberweapons, because when specifically designed, there should be little collateral damage apart from the intended target. It is estimated that the Stuxnet virus damaged 984 Iranian centrifuges at one nuclear facility alone.[25]

Second, once unleashed, a cyberweapon can create unintended derivative viruses. The designers of the Stuxnet virus intended for it to be inoperable after June 2012, but enterprising coders developed derivative viruses based on the Stuxnet design.[26] The computer security agency McAfee reports that at least six viruses have been designed based on Stuxnet's original code.[27] Derivative viruses have been used by non-state actors to attack critical infrastructure, such as power plants, water treatment facilities, and other public services. For example, in 2013, the Russian hacker group, "Energetic Bear," used a Stuxnet derivative (Havex) to access sensitive European critical infrastructure information.[28] Industroyer, another Stuxnet variant, is able to control power station infrastructure.[29] In 2015 and 2016, portions of the Ukrainian power grid were taken offline when the Industroyer virus was used to manipulate the Ukrainian power grid into overloading.[30] What makes the Industroyer virus a particularly potent

22. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

23. *Id.*

24. *Id.*

25. William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

26. *What is Stuxnet?*, *supra* note 19.

27. *Id.*

28. Eduard Kovacs, *Attackers Using Havex RAT Against Industrial Control Systems*, SEC. WEEK (June 24, 2014), https://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems.

29. *What is Stuxnet?*, *supra* note 19.

30. Anton Cherepanov & Robert Lipovsky, *Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet*, WELIVESECURITY (June 12, 2017, 2:00 PM), https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet.

variant of Stuxnet is that it can "speak" to legacy infrastructure and impair electricity infrastructure that was not designed with network security.[31]

Thirdly, cyberweapons make attributing a particular attack difficult. No state has officially taken responsibility for Stuxnet, and one of the only mentions of attribution occurred during an Israeli General's retirement party, where Stuxnet was mentioned as one of his successful operations.[32] Despite this lack of official acknowledgement, it is widely believed the United States and Israel were responsible for developing Stuxnet.[33] For traditional kinetic weapons, establishing the responsible actor is easier because one can usually trace the weapon back to its deployment. For example, if a bomb falls on a particular place, one can attribute the attack to a particular actor by seeing which planes dropped the bomb. Cyberattacks are more difficult to track.[34] Even though attacks, such as Stuxnet, always leave a trail, the work required to determine the ultimate culprit can take weeks or months.[35] One key aspect of attribution analysis requires investigating the malware used in the attack.[36] The current arms control framework creates a problem because this information is not widely shared since many cyberweapon and surveillance technology exporting countries are not a party to these multilateral regimes.[37]

B. *Current Arms Control Framework*

Despite the current regime's imperfections, efforts have been made to reduce the proliferation of cyberweapons. There are multiple arms control treaties, such as the Australia Group, addressing various facets of the international weapons market.[38] Within this multitude of different agreements, these new weapons would logically fall within the Wassenaar Arrangement.[39]

At the end of the Cold War, the international community was concerned about unrestricted access to weapons.[40] To prevent the unfettered spread of

---

31. *Id.*

32. *See* Josh Fruhlinger, *What Is Stuxnet, Who Created It And How Does It Work?*, CSO U.S. ONLINE (Aug. 22, 2017, 2:39 AM), https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

33. *Id.*

34. OFF. OF THE DIR. OF NAT'L INTEL., A GUIDE TO CYBER ATTRIBUTION 2 (2018).

35. *Id.*

36. *Id.* at 3.

37. For example, China and Israel are not a party to the Wassenaar Arrangement, which is a major part of the international arms control framework. *See About Wassenaar Arrangement*, *supra* note 13.

38. *E.g.*, Daryl Kimball, *The Australia Group at a Glance*, ARMS CONTROL ASS'N, https://www.armscontrol.org/factsheets/australiagroup (last reviewed Mar. 2021).

39. *See id.*; *Origins*, WASSENAAR ARRANGEMENT, https://www.wassenaar.org/about-us (click "Origins" tab) [hereinafter *Wassenaar Arrangement Origins*] (last updated June 22, 2021).

40. *Wassenaar Arrangement Origins*, *supra* note 39.

arms, a group of thirty-three countries founded a multilateral agreement requiring countries to individually implement export controls related to dual-use[41] and military technology.[42] This arrangement became known as the Wassenaar Arrangement[43] and governed dual-use military and non-military item transfer between governments and private actors.[44] The Wassenaar Arrangement advocates for a licensing[45] system at the national level where the government reviews individual transactions for illicit activities.[46]

When cyberweapons were being exported by Wassenaar Arrangement members, they incorporated these new weapons into the legacy regime instead of developing an overarching cyberweapon arms control treaty.[47] In December 2013, the Wassenaar Arrangement was amended to include intrusion software in response to exports of this software to countries with a history of human rights abuses such as Libya.[48]

This amendment received different industry responses in Europe and the United States. In Europe, adoption of the intrusion software update was implemented verbatim in October 2014.[49] However, in the United States there was opposition to the Commerce Control List[50] amendments because industry groups believed the agency's definition was too broad.[51] More than 264 comments were submitted by trade associations, affected companies, and even members of Congress.[52] For example, the Carnegie Mellon Software Engineering Institute believed the amendment to the regulations

41. A "dual-use" item is one that has civil applications as well as terrorism and military or weapons of mass destruction-related applications. 15 C.F.R. § 730.3 (2021). For example, a cell phone can be used for phone calls or to detonate a roadside bomb.

42. *Wassenaar Arrangement Origins*, *supra* note 39.

43. *Id.*

44. *About Wassenaar Arrangement*, *supra* note 13.

45. A license is an authorization from the government to engage in a particular export transaction(s). 15 C.F.R. § 772.1 (2021).

46. *See Guidelines & Procedures, including the Initial Elements*, *in* WASSENAAR ARRANGEMENT SECRETARIAT, WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES: FOUNDING DOCUMENTS 7 (2019), https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-Public-Docs-Vol-I-Founding-Documents.pdf.

47. *See* Wassenaar Arrangement, List of Dual-Use Goods, *supra* note 14, category 5, pt. 2.

48. Eva Galperin & Nate Cardozo, *What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?*, ELEC. FRONTIER FOUND. (May 28, 2015), https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation.

49. Commission Delegated Regulation 1382/2014, 2014 O.J. (L 371) 1–212, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R1382&from=EN.

50. The Commerce Control List details a list of items under the export control jurisdiction of the Bureau of Industry and Security, U.S. Department of Commerce, and generally includes dual-use non-military items. *See* 15 C.F.R. § 774 (2021).

51. *See* Galperin & Cardozo, *supra* note 48.

52. Roszel Thomsen & Philip Thomsen, *Export Controls on Intrusion and Surveillance Items: Noble Sentiments Meet the Law of Unintended Consequences . . .*, J. INTERNET L., Sept. 2015, at 22, 30.

would have a "chilling effect" on cyber research.[53] Other groups believed the drafting of the regulations was overly broad and would hurt the U.S. security research industry.[54] This initial opposition to the proposed rule led the U.S. government to implement an interim rule, and it went back to the Wassenaar Arrangement to renegotiate the scope and language of the rule.[55] In 2017, the Wassenaar Arrangement made significant changes that were proposed as final rules in the United States and will become effective on January 22, 2022.[56]

Other countries have taken a regional approach to addressing cyberweapon concerns. For example, the Shanghai Cooperation Organization ("SCO") concluded an agreement that sought to limit the proliferation of cyberweapons and "information terrorism."[57] The SCO includes countries such as China, India, Russia, and Pakistan.[58] Commentators believe the definition of "information war" as "mass psychologic[al] brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party" attempts to justify censorship.[59] The SCO agreement stands in opposition to the Wassenaar approach because it uses a more expansive definition of cyberweapons and their capabilities. It also encompasses countries, such as China, that are not parties to major existing international arms control treaties.[60]

The SCO approach includes not only programs that target areas such as critical infrastructure but also views cyberweapons from a political perspective.[61] This perspective was summarized by Sergei Korotkov in his discussion at a 2008 U.N. disarmament conference.[62] Korotkov defined aggression as "anytime a government promotes ideas on the internet with

53. ALLEN HOUSEHOLDER & ART MANION, CERT COORDINATION CENTER, COMMENTS ON BUREAU OF INDUSTRY AND SECURITY PROPOSED RULE: WASSENAAR ARRANGEMENT 2013 PLENARY AGREEMENTS IMPLEMENTATION: INTRUSION AND SURVEILLANCE ITEMS 4-6 (2015), https://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_442291.pdf.

54. *See, e.g.*, Galperin & Cardozo, *supra* note 48.

55. Information Security Controls: Cybersecurity Items, 86 Fed. Reg. 58205, 58206 (Jan. 19, 2022) (to be codified at 15 C.F.R. pts. 740, 772, 774).

56. *Id.*

57. Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, Annex 1, June 16, 2009 [hereinafter SCO Agreement], http://eng.sectsco.org/load/207508.

58. *Shanghai Cooperation Organization*, UNITED NATIONS: DEP'T OF POL. & PEACEBUILDING AFFS., https://dppa.un.org/en/shanghai-cooperation-organization (last visited Nov. 26, 2021).

59. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 825 (2012).

60. *See About Wassenaar Arrangement*, *supra* note 13.

61. Tom Gjelten, *Seeing the Internet as an 'Information Weapon,'* NPR (Sept. 23, 2010, 12:00 AM), https://www.npr.org/templates/story/story.php?storyId=130052701.

62. *Id.*

the goal of subverting another country's government."[63] This conception of aggression and cyberweapons as tools to subvert a foreign government's legitimacy is more expansive than the definition proscribed in the Wassenaar Arrangement.[64] The SCO's cyberweapon definition highlights a difference of opinion that must be bridged if countries seek to develop a cyberweapon framework that includes countries outside the Wassenaar Arrangement.

II. THE PROBLEM

Cyberweapons pose a significant threat to international peace and security. They have the potential to inflict significant harm on entire nations with minimal investment from the instigating country.[65] There are three problems that must be addressed in considering the regulation of cross-border transfers between governments and private entities or persons: defining a cyberweapon, the current gap in the arms control framework, and the level of control applied.

A. *Defining What Is a Cyberweapon*

Under the Wassenaar Arrangement's conception,[66] the current inclusion of intrusion software and software that defeats, weakens, or bypasses information security is vague and creates a risk of differing interpretations. For example, these categories may not include software taking control of computers in preparation for a Distributed Denial of Service ("DDoS") attack. A DDoS attack occurs when a hacker takes control of many computers then directs them to simultaneously and repeatedly access a website or server to overload the target.[67] The Wassenaar Arrangement's definition may not encompass this type of cyberweapon because, as discussed below, its definitions is defined based on the software's intent rather than its technical characteristics.[68] As a result, countries may differ in whether they regulate DDoS preparation software based on this provision of the Arrangement.

Additionally, the current approach by the Wassenaar Arrangement reacts to gaps in the cyberweapons framework rather than proactively including cyberweapons as they are developed. For example, the inclusion

63. *Id.*
64. *Id.*
65. *See* Phillip Pool, *War of the Cyber World: The Law of Cyber Warfare*, 47 INT'L L. 299, 303 (2013).
66. Wassenaar Arrangement, List of Dual-Use Goods, *supra* note 14, category 5, pt. 2.
67. *What Is a Distributed Denial of Service Attack (DDoS)?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack (last visited Nov. 26, 2021).
68. See discussion *infra* Section B.

of surveillance technology was in response to the transfer of surveillance and intrusion technology to governments with a history of human rights abuses.[69] Furthermore, changes made to the Wassenaar Arrangement's control lists were provided as a clarification, and not in recognition of cyberweapon's growing threat.[70] This reactive approach risks making the definition of cyberweapons not reflective of technological advancements.

Cyberweapons span a range of capabilities unlike conventional weapons that are clearly designed for military use and would have little value to a benevolent citizen (for example, a civilian would have little use for a heat seeking missile).[71] On one end of the spectrum, there are those cyberweapons Professors Thomas Rid and Peter McBurney describe as the generic cyberweapons. Generic cyberweapons are analogous to paintball guns—they look like a real weapon, but they do little damage, and it is obvious when someone was attacked.[72]

On the other end of the spectrum are specific cyberweapons, which are specially designed to execute a defined mission.[73] Under this framework, the previously discussed Stuxnet virus would logically fall closer to the end of "specifically designed" because it was developed over a period of time by the west to specifically target Iranian nuclear facilities. This description of cyberweapons by Professors Rid and McBurney is similar to the Wassenaar notions of a cyberweapon, which focus on attacking critical infrastructure by seeking to circumvent defenses.[74]

By contrast, an opposing definition of cyberweapons includes "informational terrorism," which more broadly encompasses activities excluded by the Wassenaar definition.[75] The SCO Agreement demonstrates a different conception of cyberweapons as including the ability to wage informational warfare.[76] Information warfare does not have a generally accepted definition, but has been defined as denying, corrupting, or

69. *See* Thomsen & Thomsen, *supra* note 52, at 22–23.

70. WASSENAAR ARRANGEMENT SECRETARIAT, WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES: BACKGROUND DOCUMENTS AND PLENARY-RELATED AND OTHER STATEMENTS 57 (2020), https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-IV-Background-Docs-and-Plenary-related-and-other-Statements-Dec.-2020.pdf.

71. Thomas Rid & Peter McBurney, *Cyber-Weapons*, RSUI J., Feb.–Mar. 2012, at 6, 6, https://doi.org/10.1080/03071847.2012.664354.

72. *Id.* at 6.

73. *Id.*

74. *Cf. id.* at 7 (describing cyberweapons in terms of harm from the psychological dimension such as the intent to cause harm to the target).

75. *See* SCO Agreement *supra* note 57, at 9–10 (defining "information terrorism" as "using information resources in the information space and/or influencing on them for terrorist purposes").

76. *Id.*

exploiting an enemy's information systems for military gain.[77] While this formulation is vague, it would include "psychological operations,"[78] which are defined by the Department of Defense as intended to "convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals" with the purpose of "induc[ing] or reinforc[ing] foreign attitudes and behavior favorable to the originator's objectives."[79] Since the SCO deliberately chose the term "terrorism" and focused on misinformation,[80] they emphasized, among other things, the psychological impact of cyberweapons in addition to the Wassenaar Arrangement's definition. This psychological concern would include "misinformation" being distributed in their territory through the internet.[81] When the SCO Agreement was passed in 2009, commentators did not raise concerns of misinformation distributed by foreign powers, but rather focused on the impact it would have on civil liberties.[82] Recent campaigns by foreign governments in places such as the United States and the United Kingdom may lead commentators to rethink this strict dismissal of information warfare.[83]

B. *Gaps in the Current Arms Control Framework*

Two areas create compliance gaps in the current arms control framework. First, existing arms control agreements are vague in identifying and controlling cyberweapons. Second, many cyberweapon exporters are not a party to these international arms control agreements.

As previously discussed, the Wassenaar Arrangement imposed controls on infiltration software focusing on programs that weaken, bypass, or defeat information security.[84] The vague language attached to this definition stands in contrast to the scientifically specific language used in other parts of the Wassenaar Arrangement for conventional kinetic weapons and dual-use

77. Col. Andrew Borden, *What Is Information Warfare?*, AIR UNIV. CHRONS. ONLINE J. (Nov. 2, 1999), https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf.

78. *Id*.

79. Steven Aftergood, *DoD "Clarifies" Doctrine on Psychological Operations*, FED' N OF AM. SCIENTISTS (Jan. 19, 2010), https://fas.org/blogs/secrecy/2010/01/psyop.

80. SCO Agreement *supra* note 57, at 9–10 (defining "information terrorism" as "using information resources in the information space and/or influencing on them for terrorist purposes").

81. *Id.*

82. Hathaway et al., *supra* note 59, at 825.

83. *See* BEN NIMMO ET AL., GRAPHIKA, SECONDARY INFEKTION (2020), https://secondaryinfektion.org/report/secondary-infektion-at-a-glance; Bobby Allyn, *Study Exposes Russia Disinformation Campaign That Operated In the Shadows for 6 Years,* NPR (June 16, 2020, 2:36 PM), https://www.npr.org/2020/06/16/878169027/study-exposes-russia-disinformation-campaign-that-operated-in-the-shadows-for-6-.

84. Wassenaar Arrangement, List of Dual-Use Goods, *supra* note 14, § 5.A.4.

items. For example, when defining what materials are controlled under Category One,[85] the Wassenaar Arrangement lists among other items "[m]aterials not transparent to visible light and specially designed for absorbing near-infrared radiation having a wavelength exceeding 810 nm but less than 2000 nm."[86] Under the category "Materials Processing," the Wassenaar Arrangement controls "[r]otary position feedback units specially designed for machine tools or angular displacement measuring instruments, having an angular position 'accuracy' equal to or less (better) than 0.9 second of arc."[87] This technical definition contrasts to the vague language of "[s]ystems, equipment and components for defeating, weakening or bypassing 'information security', as follows . . . Designed or modified to perform 'cryptanalytic functions.'"[88] This contrast in language highlights the difficulty of applying parameters to define cyberweapons in an international agreement,[89] which is likely a motivating factor behind the Wassenaar's approach. It is an attempt to use the software's intended capabilities rather than its technical characteristics. However, focusing on the narrow intent of "bypassing" or "defeating" information security raises many questions. For example, does the definition cover cyberweapons that seek to slow down the speed of a network connection to frustrate the user but are not intended to defeat or weaken its security? This control framework could be more specific and may potentially be underinclusive of these important capabilities that have been used by malicious actors to slow down government and nongovernment networks.[90]

Secondly, many of the arms control agreements, such as the Wassenaar Arrangement, do not include emerging cyberweapon developers such as China and Israel as parties.[91] Israel eased export restrictions for cyberweapons in 2018 despite international criticism.[92] China has also been an active exporter of surveillance technology, including its Sensetime

85. Category One includes "Special Materials and Related Equipment." *Id.* § 1.

86. *Id.* § 1.C.1.b.

87. *Id.* § 2.B.6.c.

88. *Id.* § 5.A.4.

89. *See* Trey Herr, *PrEP: A Framework for Malware & Cyber Weapons*, 13 J. INFO. WELFARE 87, 87 (2014).

90. For example, in 2013, a conflict between two organizations led to a worldwide slowdown of the internet when one organization engaged in a DDoS Attack against the other. Dave Lee, *Global Internet Slows After 'Biggest Attack in History'*, BBC NEWS (Mar. 27, 2013), https://www.bbc.com/news/technology-21954636.

91. *See About Wassenaar Arrangement*, *supra* note 13.

92. *See* Tova Cohen & Ari Rabinovitch, *Israel Eases Rules on Cyber Weapons Exports Despite Criticism*, REUTERS (Aug. 22, 2019, 5:50 AM), https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ.

software to Mongolia.[93] China's Sensetime software enables the user government to perform real-time identification of pedestrians and vehicles.[94] Since these countries are outside existing arms control agreements, cyberweapon exports are unregulated and make attributing a particular attack difficult.

An international approach towards controlling cyberweapons is critical because, unlike traditional kinetic weapons, cyberweapon attacks are difficult to accurately attribute to a particular actor.[95] Persons, organizations, and governments can obscure their identity in cyberspace by contracting with third parties, facilitating attribution of the attack to another party, or moving through other jurisdictions.[96] Thus, when attributing an attack to a malevolent actor, information sharing is important because the malware's origin plays an important part of drawing connections between the various facets of a cyberattack.[97] As a result, countries must work together to address these concerns. When significant cyberweapon exporting countries are not members of an international framework, they enable different actors to engage in these veiled attacks by equipping them with the necessary tools to accomplish their objectives.

C. *Current Level of Control*

The current level of control for cyberweapons treats certain software similar to other dual-use items such as material processing equipment rather than more sensitive technology.[98] The Wassenaar Arrangement is largely divided into two separate lists, first the dual-use control list for dual-use non-military items, and second the munitions list.[99] In an effort to increase transparency, the munitions list requires more exchanging of information

93. Steven Feldstein, *The Global Expansion of AI Surveillance* 1, app. at 26 (Carnegie Endowment for Int'l Peace, Working Paper, 2019), https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

94. Rob Schmitz, *Facial Recognition in China Is Big Business as Local Governments Boost Surveillance*, NPR (Apr. 3, 2018, 10:40 AM), https://www.npr.org/sections/parallels/2018/04/03/598012923/facial-recognition-in-china-is-big-business-as-local-governments-boost-surveilla.

95. *See* Christopher S. Chivvis & Cynthia Dion-Schwarz, *Why It's So Hard to Stop a Cyberattack—and Even Harder to Fight Back*, RAND BLOG (Mar. 30, 2017), https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html; Anu Narayanan & Jonathan Welburn, *Is DarkSide Really Sorry? Is It Even DarkSide?*, RAND BLOG (May 19, 2021), https://www.rand.org/blog/2021/05/is-darkside-really-sorry-is-it-even-darkside.html.

96. *See* Narayana & Welburn, *supra* note 95.

97. *See* OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 34, at 3.

98. *See* Wassenaar Arrangement, List of Dual-Use Goods, *supra* note 14, §§ 2.B.6.c, 5.A (failing to classify penetration software as "sensitive," similar to other dual-use items such as material processing equipment).

99. *Control Lists*, WASSENAAR ARRANGEMENT, https://www.wassenaar.org/control-lists (last updated June 22, 2021).

between the member states about licensed exports.[100] By contrast, the dual-use list divides items into two tiers: "Basic Items" and "Sensitive Items and its subset of Very Sensitive Items".[101] For Basic Items, countries must provide a list of transfers twice per year for licenses that were denied for transactions to non-member countries, whereas the Sensitive and Very Sensitive items have stricter requirements.[102] When an item is placed in the Sensitive or Very Sensitive list, countries must report an approved transaction within sixty days if another member denied an "essentially identical" transaction.[103] Furthermore, for Very Sensitive items, members are called on to "exert extreme vigilance."[104]

Currently, nothing in Category Five part two is listed as sensitive or very sensitive.[105] Category Five part two of the Wassenaar Arrangement dual-use list includes the previously mentioned software such as infiltration software.[106] When adopting these controls, the plenary communications for the 2015 meeting do not mention why the Wassenaar Arrangement elected not to classify this type of software as Sensitive or Very Sensitive items.[107] Given the opposition raised in the United States when the rules were ultimately implemented,[108] it is possible that the committee recognized that stricter control would raise the public's ire.

The Shanghai Cooperation Organization's agreement on cyberweapons provides high-level guidance to signatory states on monitoring and controlling cyberweapons.[109] The Shanghai Cooperation Organization's approach includes information sharing but is less specific about under what conditions transaction specific information should be shared.[110] These pledges were recently reaffirmed at a 2018 meeting.[111]

III. PROPOSED SOLUTION

Governments should further develop and agree on a cyberweapon definition, as well as upgrade the level of control assigned to cyberweapons.

---

100. Kimball, *supra* note 16.
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. Wassenaar Arrangement, List of Dual-Use Goods, *supra* note 14, at 170–172.
106. *Id.*, category 5, pt. 2.
107. *See* Wassenaar Arrangement, *Statement Issued by the Plenary Chair on 2015 Outcomes of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technology* (Dec. 3, 2015).
108. *See* Galperin & Cardozo, *supra* note 48.
109. *See* SCO Agreement, *supra* note 57.
110. *See id.* art. 5.
111. *Press Release on the Outcome of the 13th Meeting of the SCO National Security Council Secretaries*, SHANGHAI COOP. ORG. (May 22, 2018), http://eng.sectsco.org/news/20180522/431989.html.

Cyberweapons have destructive capabilities that can result in human casualties and take critical infrastructure offline.[112] First, governments should consider whether cyberweapons include software that disseminates certain messages such as those spreading misinformation. The Western experience concerning software that widely disseminates certain information has changed since the original definition was drafted in 2015[113] and control lists may need to be updated to reflect this change. Although decisions addressing misinformation while balancing civil rights concerns deserve additional discussion, analysis of this topic is beyond the scope of this Note. Second, a new treaty is necessary to bring together nations in the Wassenaar Arrangement with those states outside it to develop a truly global framework on cyberweapons. Third, the Wassenaar control lists for cyberweapons should be drafted with greater specificity to ensure a uniform regulatory framework. Finally, cyberweapons should be subject to greater control because of the growing secondary market.

A. *Cyberweapons Definition*

The division between the SCO and the Wassenaar Arrangement over defining a cyberweapon centers on, among other things, whether software disseminating certain information qualifies as a cyberweapon.[114] This type of software was recently highlighted in a RAND report.[115] The software in question robotically re-tweets government-sponsored messages to blanket the social media landscape and push their messages to the top of a user's newsfeed.[116] Similarly, another analysis found that 20% of the Russian News Network's most avid followers accounted for 75% of their re-tweets.[117]

Russia has been accused of interfering in the United Kingdom and United States elections through such use of social media.[118] In 2019, the European Union's Commissioner for Security stated "[w]inter isn't the only thing that's coming—so is the risk of interference in our elections,"[119]

112. Joshi, *supra* note 3.

113. See discussion *supra* Section II.A.

114. See discussion *supra* Section II.B.

115. TODD C. HELMUS ET. AL, RAND CORP., RUSSIAN SOCIAL MEDIA INFLUENCE: UNDERSTANDING RUSSIAN PROPAGANDA IN EASTERN EUROPE 24 (2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

116. *Id.*

117. *Id.* at 25.

118. *Theresa May Accuses Vladimir Putin of Election Meddling*, BBC (Nov. 14, 2017), https://www.bbc.com/news/uk-politics-41973043; Abigail Adams, *Here's What We Know So Far About Russia's 2016 Meddling*, TIME (Apr. 18, 2019, 8:20 AM), https://time.com/5565991/russia-influence-2016-election.

119. Marco Silva, *Is Russia Trying to Sway the European Elections?*, BBC (May 20, 2019), https://www.bbc.com/news/blogs-trending-48296557.

demonstrating the heightened risk of foreign interference in its elections through means such as social media. In the 2020 U.S. presidential election, this type of social media activity also led officials to determine foreign governments were attempting to undermine U.S. confidence in the electoral system.[120] These developments demonstrate these nations may want to revisit whether cyberweapons include software such as those disseminating misinformation—but in doing so, freedom of speech and civil liberties must remain protected.

With this backdrop, Western governments have already begun this discussion. In the United States, Congress held hearings with major social media CEOs to discuss each companies' role in online misinformation and extremism.[121] Parliament in the United Kingdom created a subcommittee on "Online Harms and Disinformation," which began investigating online disinformation and misinformation in the United Kingdom.[122] The European Parliament established the "Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation."[123] These government efforts demonstrate they may also wish to revisit the discussion of whether software distributing certain information qualifies as a cyberweapon.

B. *A New Cyber-Treaty*

There is no comprehensive global treaty governing transfers of cyberweapons between governments and private parties. For example, the Wassenaar Arrangement does not include cyberweapon exporting countries such as China and Israel.[124] At the same time, technological advances enable non-state actors to utilize cyberweapons and inflict harm on persons and critical infrastructure. Thus, there is an immediate need to develop a new cyber-arms control regime that encompasses the world's cyberweapon exporters. Furthermore, existing members of Cold War-era arms treaties should seek to develop a new framework for restricting transfers of cyberweapons between governments and private actors. First, a multilateral

120. NAT'L INTEL. COUNCIL., FOREIGN THREATS TO THE 2020 US FEDERAL ELECTION i (2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf ("We assess that Russian President Putin authorized . . . influence operations aimed at . . . undermining public confidence in the electoral process . . . .")

121. Gerrit De Vynck et al., *Big Tech CEOs Face Lawmakers in House Hearing on Social Media's Role in Extremism, Misinformation*, WASH. POST (Apr. 9, 2021, 3:20 PM), https://www.washingtonpost.com/technology/2021/03/25/facebook-google-twitter-house-hearing-live-updates.

122. *Online Harms and Disinformation*, U.K. PARLIAMENT, https://committees.parliament.uk/work/232/online-harms-and-disinformation (last visited Sept. 11, 2021).

123. *Special Committee on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation*, EUR. PARLIAMENT, https://www.europarl.europa.eu/committees/en/inge/home/highlights (last visited Nov. 26, 2021).

124. *See About Wassenaar Arrangement*, *supra* note 13.

treaty would address the growing secondary market for cyberweapon utilization by state and non-state actors to inflict harm on other nations and extract profits. Second, a multilateral treaty would enable cross-border sharing of information to facilitate faster attribution of cyberattacks. Third, when drafting this agreement, two key provisions should be adopted. The presumption of denial approach taken from another arms control treaty, the Missile Technology Control Regime,[125] should be utilized for cyberweapon export. Additionally, the control lists should follow the form utilized in the Wassenaar Arrangement but provide specific types of cyberweapons as a companion to clarify the control status of different software.

Having a comprehensive, global treaty is important to address the growing secondary market for cyberweapons, where criminals utilize cyberweapons purchased on the dark web with cryptocurrency to engage in illegal activity.[126] Previously, crimes such as bank robbery required someone with a gun to run inside a bank and hold up the teller. Now, the decentralized nature of the dark web enables cybercriminals to buy cyberweapons such as ransomware to engage in crime from afar.[127] The person engaging in the attack can buy the ransomware on the internet from the software's developer, which separates the developer from the perpetrator.[128] As a result, the decentralized nature of the internet allows these criminals to anonymously create and sell cyberweapons.

A multilateral treaty would create non-binding obligations on states to address this growing secondary market. Treaties such as the Wassenaar Arrangement create non-binding obligations on states to standardize how export controls are implemented at the member country level.[129] Adopting a multilateral regime with states taking corresponding domestic action would decrease the cross-border flow of cyberweapons and increase the difficulty of developing these weapons. Given the international nature of cybercrime, a multinational treaty would create a framework to identify these cybercriminals and allow states to bring them to justice.

Moreover, a multilateral treaty would address the problem of attributing cyberattacks to particular actors because countries would have records of cyberweapon transfers. As previously mentioned, the Wassenaar Arrangement requires information sharing for exports of certain arms and dual-use items.[130] If a multilateral regime were developed for cyberweapons,

125. Kelsey Davenport, *The Missile Technology Control Regime at a Glance*, ARMS CONTROL ASS'N, https://www.armscontrol.org/factsheets/mtcr (last reviewed Mar. 2021).

126. *New Technology Has Enabled Cyber-Crime on an Industrial Scale*, ECONOMIST (May 6, 2021), https://www.economist.com/international/2021/05/06/new-technology-has-enabled-cyber-crime-on-an-industrial-scale.

127. *Id.*

128. *Id.*

129. *See About Wassenaar Arrangement*, *supra* note 13.

130. *See* discussion *supra* Section II.C.

it should include a similar type of information sharing mechanism to facilitate the identification of malware used in cyberattacks. Since the type of malware plays an important role in attributing an attack to a particular actor,[131] sharing malware and other cyberweapon export information would enable faster attribution of an attack.

In drafting this framework, authors should incorporate two key concepts from existing arms control treaties. Firstly, for cyberweapons, a presumption of denial approach should be adopted to restrict the deployment of these technologies. Secondly, as discussed in the next section, specific control lists should be utilized as a companion to the broad control principles utilized in the Wassenaar Arrangement.

The presumption of denial approach, utilized in the Missile Technology Control Regime ("MTCR"), would create a "strong presumption of denial" for exports of cyberweapons designed to directly harm persons or critical infrastructure.[132] The strong presumption of denial requirement means the exporting government may authorize export of these items on rare occasions.[133] Given the threat posed by the proliferation of ballistic missiles, this strong approach seems appropriate. Similarly, cyberweapons pose a substantial threat because they can damage infrastructure and create an unlimited number of copies from a single source code. This destructive power was shown by the recent state of emergency declaration in the United States following the cyberattack on a Colonial Pipeline facility.[134] Moreover, as shown in the Stuxnet example, once a cyberweapon is deployed other derivative weapons can be developed based on the original source code.[135] The presumption of denial approach can prevent the initial release that could ultimately lead to untold proliferation of cyberweapons over the internet.

C. *Upgrading Cyberweapon Control Status*

Cyberweapons such as intrusion software and their underlying source code should be added to the Sensitive or Very Sensitive lists in the Wassenaar Arrangement to reflect their danger to international peace and security. Following the approach of Professors Thomas Rid and Peter

131. *See* OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 34, at 3.

132. *See* Davenport, *supra* note 125; *Frequently Asked Questions*, MISSILE TECH. CONTROL REGIME, https://mtcr.info/frequently-asked-questions-faqs (last visited Nov. 26, 2021).

133. *See Frequently Asked Questions*, *supra* note 132 ("Category I items are subject to an unconditional strong presumption of denial regardless of the purpose of the export and are licensed for export only on rare occasions.")

134. Mary-Ann Russon, *US Fuel Pipeline Hackers 'Didn't Mean to Create Problems'*, BBC NEWS (May 10, 2021), https://www.bbc.com/news/business-57050690.

135. *See* discussion *supra* Section I.A.

McBurney,[136] source code should be deemed "very sensitive" when it is specially designed for infiltration of specific computer networks, whereas other commercial software that has dual-use capabilities should be controlled in the sensitive category. This demarcation would align the control status for intrusion with its capabilities since software specifically designed for intrusion represents a substantial risk to a country's national security and foreign policy interests. As recent cyberattacks show, infiltration software poses a substantial risk because it allows malicious actors to access critical networks.[137]

Moreover, heightening the control status of infiltration software would reduce the ability for cybercriminals to use infiltration software to access computer networks and hold them for ransom. As the recent attack on Colonial Pipeline in the United States demonstrates, cybercriminals are willing and able to infiltrate a network then hold it for ransom.[138] Upgrading the control status of infiltration software would heighten the legal obligations of states to report these transfers and hopefully reduce criminals' ability to access this software.

Additionally, heightening the control status of infiltration software and other cyberweapons would further other sanctions programs. Many ransomware attacks benefit countries already under United Nations sanctions. For example, according to a United Nations report, North Korea generated $2 billion in revenue in 2019 from its ransomware program to fund its weapons of mass destruction capabilities.[139] Other nations subject to sanctions such as Iran have also been known to engage in ransomware attacks.[140] Heightening the restrictions on intrusion software and other cyberweapon exports should reduce the ability of these nations to access the valuable source code that enables their operations.

D. *Enumerating Specific Cyberweapon Capabilities*

Cyberweapons such as computer worms[141] should be specifically enumerated on the Wassenaar Arrangement's control lists as a companion to

136. *See* discussion *supra* Section II.A.

137. Russon, *supra* note 134.

138. *Id.*

139. Michelle Nichols, *North Korea Took $2 Billion in Cyberattacks to Fund Weapons Program: U.N. Report*, REUTERS (Aug. 5, 2019, 2:28 PM), https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX.

140. *E.g.*, Gwen Ackerman, *Ransomware Linked to Iran, Targets Industrial Controls*, BLOOMBERG (Jan. 28, 2020, 9:17 AM), https://www.bloomberg.com/news/articles/2020-01-28/-snake-ransomware-linked-to-iran-targets-industrial-controls.

141. A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage. *What Is a Computer Worm,*

the overarching principles defining them. As discussed above, the Wassenaar Arrangement's control lists typically include the specific capabilities of items subject to control.[142] The overarching definitions such as software designed to weaken or degrade encryption are helpful in determining what is a cyberweapon, but greater guidance on categorizing particular software is needed. Until the specific components of cyberweapons are described, the Wassenaar Arrangement should provide, as a supplement, greater detail on what constitutes a cyberweapon by categorizing specific types of software. Providing this level of specificity would clarify ambiguities in the division of this technology.

Cyberweapons appear on both the Wassenaar Arrangement's Munitions List, which details military items, and the dual-use control list, but the difference between the two definitions is unclear. Clearly delineating the difference is important because ambiguities may lead to differing implementations creating regulatory gaps where exports illegal in one country under the Wassenaar Arrangement are allowed in another. The Wassenaar Arrangement Munitions List includes "'[s]oftware' specifically designed or modified for the conduct of military offensive cyber operations."[143] "Cyberspace Offensive Operations" are defined by the U.S. military to include "operations intended to project power by the application of force in and through cyberspace."[144] Intrusion software would seemingly fit this category. It is software that is designed to infiltrate systems, which would project power against adversaries through cyberspace because infiltration is the first step of crippling an adversary's system. However, as detailed above, intrusion software is specifically enumerated on the dual-use control list, which is subject to less restrictions than the Munitions list.[145] This vagueness creates ambiguity on which types of intrusion software should be classified as military items and which software would qualify as dual-use. Moreover, different countries may implement the same treaty provision in different ways, but more concrete evidence of whether this is occurring is not available. Such a situation undermines the Wassenaar Arrangement's usefulness as a global platform for standardizing export controls. Categorizing cyberweapons under each list would alleviate this confusion because it would assign specific types of software to each category, which would harmonize control status between different countries.

And How Does It Work?, NORTON, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html (last visited Dec. 18, 2021).

142. *See* discussion *supra* Section II.B.

143. Wassenaar Arrangement, List of dual-Use Goods, *supra* note 14, § ML21.b.5.

144. DEP'T OF THE ARMY, FM 3-38: CYBER ELECTROMAGNETIC ACTIVITIES 3-2 (2014).

145. See discussion *supra* Section II.A.

CONCLUSION

Cyberweapons are a significant threat to international peace and security. The current framework does not adequately address identifying and controlling cyberweapons. However, a series of changes could begin to address the problem cyberweapons pose to international peace and security. First, states should develop a common definition of a cyberweapon. Second, states should form a multilateral treaty utilizing the shared definition to ensure cyberweapon exports are governed by a treaty and include a greater geographic diversity covering a larger share of this market. Third, under the Wassenaar Arrangement, cyberweapons should be subject to additional control because exports can lead to derivative viruses, which multiply the harm of the original export. Finally, cyberweapons should be listed with greater specificity to reduce the ambiguity associated with the current definition. These changes represent significant steps toward reducing the ability of cybercriminals to access these dangerous weapons. As a result, international cooperation can reduce the risk a cyberweapon will cause real harm to society.