UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Managing Commercial Spyware Through Export Controls

LESSONS LEARNED FROM THE WASSENAAR EXPERIENCE

ELAINE KORZAK, PHD, LLM

CLTC WHITE PAPER SERIES

Managing Commercial Spyware Through Export Controls

LESSONS LEARNED FROM THE WASSENAAR EXPERIENCE

ELAINE KORZAK, PHD, LLM

Research Scholar, Berkeley Risk and Security Lab (BRSL)

Research Affiliate, Center for Long-Term Cybersecurity (CLTC)

UC Berkeley

March 2025

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

The proliferation and misuse of commercial spyware technologies present an international policy problem. A burgeoning industry of commercial spyware providers has emerged that markets a range of technologies with the ability to covertly access and/or monitor communications data of individuals and groups. Governments and non-governmental stakeholders across the globe have sought to address human rights harms, and more recently national security and nonproliferation risks, associated with the misuse of commercial spyware technologies.

This white paper examines the most significant multilateral effort that has been made to date to constrain commercial spyware: the use of multilateral export controls under the Wassenaar Arrangement. Following revelations of human rights violations in the aftermath of the Arab Spring, Wassenaar participating states placed a specific set of commercial spyware technologies on the Wassenaar dual-use control list in 2013. These changes, which represented the first international effort to directly regulate commercial spyware technologies, proved highly controversial, particularly in the United States. An impasse in international regulation efforts followed for several years.

This examination of Wassenaar controls identifies three lessons that have been learned with regard to the regulation of commercial spyware through multilateral export controls, based on analysis of their implementation in two key jurisdictions: the European Union (EU) and the US.

First, export control decisions have been compounded by the need to balance new and additional equities. In addition to economic interests and national security concerns, states need to engage with human rights as well as cybersecurity considerations in the context of export controls. This multitude of considerations requires individual states to wrestle with their own prioritization among these equities in order to effectively engage in and shape export controls, as well as other international regulation efforts.

Second, Wassenaar export controls were contentious, and this has had a lasting effect on the Wassenaar Arrangement and its members, led to questions about the utility of export controls, and impeded international progress on the issue. Rather than focusing on one regulatory mechanism, stakeholders should pursue a web of national and international measures to address commercial spyware. This, in turn, requires systematic mapping and examination of potential measures.

Third, there are inherent limitations to Wassenaar controls, and to export controls more generally, that need to be identified and acknowledged. Given that the Wassenaar controls target only a very small subset of commercial spyware technologies, the effectiveness of export controls is naturally limited. The Wassenaar experience provides an opportunity to assess and improve the efficacy of controls, but to conduct such assessments, data regarding export applications, approvals, and denials needs to be systematically gathered, collated, and analyzed.

Recent initiatives, in particular the Pall Mall process, indicate renewed interest and growing political momentum among states to tackle the question of commercial spyware and its international regulation. The lessons identified in this paper provide valuable insights for stakeholders seeking to improve upon existing export controls, as well as to explore other mechanisms and measures to address the proliferation and misuse of commercial spyware technologies.

Introduction

On 10 August 2016, Ahmed Mansoor, a prominent human rights activist in the United Arab Emirates (UAE), started to receive suspicious text messages on his phone.[1] Rather than click on the messages, which claimed to contain information about the torture of UAE citizens, Mansoor forwarded them to researchers at the Citizen Lab, a research center at the University of Toronto.[2] A few days later, Apple urged iPhone users across the globe to download an updated version of its iOS mobile operating system that patched important security flaws.[3] As the first of its kind, Apple's emergency update was widely covered in the press at the time.[4]

In the meantime, researchers discovered that Mansoor's phone had been targeted by NSO Group's Pegasus — sophisticated intrusion and monitoring software. Notably, the attempt to compromise Mansoor's phone took advantage of three previously unknown vulnerabilities in the iOS operating system, so-called "zero days" that allow a remote user to take complete control of an iPhone with just one click.[5] Once a device is compromised, Pegasus software "can read text messages and emails and track calls and contacts. It can even record sounds, collect passwords and trace the whereabouts of the phone user."[6] Had the action succeeded, Mansoor's digital security would have been compromised, allowing his attackers to comprehensively surveil his communications and activities.

1 Nicole Perlroth, "IPhone Users Urged to Update Software After Security Flaws Are Found," *The New York Times*, 25 August 2016, available at https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html.

2 Ibid.

3 Ibid.

4 See, for instance, Dan Tynan and agencies, "Apple issues global iOS update after attempt to use spyware on activist´s iPhone," *The Guardian*, 25 August 2016, available at https://www.theguardian.com/technology/2016/aug/25/apple-ios-update-arab-activists-iphone-spyware; Nicole Perlroth, "IPhone Users Urged to Update Software After Security Flaws Are Found," *The New York Times*, 25 August 2016, available at https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html; and SecurityWeek News, "Apple Issues Emergency Fix for iOS Zero-Days: What You Need to Know," *Security Week*, 26 August 2016, available at https://www.securityweek.com/apple-issues-emergency-fix-ios-zero-days-what-you-need-know/.

5 Tom Spring, "Emergency iOS Update Patches Zero Days Used by Government Spyware," *Threatpost*, 25 August, 2016, available at https://threatpost.com/emergency-ios-update-patches-zero-days-used-by-government-spyware/120158/. See also Bill Marczak and John Scott-Railton, '*The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*,' Report, The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto, 24 August 2016, available at https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/. Since then, NSO Group's software has evolved from so-called "one-click" to "zero-click" tools, which do not require any action on the part of the user to be infected. See, for instance, Gordon Kelly, "New iPhone iMessage Flaw Enables 'Zero Click' Hack," *Forbes*, 25 August 2021, available at https://www.forbes.com/sites/gordonkelly/2021/08/25/apple-iphone-warning-pegasus-hack-upgrade-ios-14-security/.

6 Nicole Perlroth, "IPhone Users Urged to Update Software After Security Flaws Are Found," *The New York Times*, 25 August 2016, available at https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html.

Ahmed Mansoor's case is not an isolated incident. He is one of many activists, journalists, lawyers, and politicians worldwide that have been targeted and compromised by commercial spyware technologies. Countless accounts have been published by researchers, advocacy groups, and investigative journalists detailing an array of human rights abuses by (repressive) governments using commercial spyware. NSO Group, the Israel-based company offering the Pegasus software used to target Ahmed Mansoor, is only one of many companies developing and selling sophisticated monitoring and intrusion software used by law enforcement and intelligence agencies worldwide.[7] Yet NSO Group has been regularly featured in the news for several years and has gained such notoriety that its name has become somewhat synonymous with the global spyware technology industry.[8] While this has put NSO Group at the center of many international campaigns highlighting human rights violations resulting from the use of surveillance technologies, a burgeoning market for commercial spyware technologies has developed beyond this single company.

As a result, the proliferation and (mis)use of commercial spyware technologies have emerged as global policy problems. In response, various national and international efforts have sought to address the human rights abuses aided by the provision of commercial spyware — with varying degrees of success.

Advocacy groups and United Nations (UN) experts have called for bans or moratoriums on the development, sale, and use of commercial spyware.[9] Private-sector companies, including Meta and Microsoft, have issued policy recommendations related to these technologies.[10] In high-profile litigation cases, Apple and WhatsApp have sued NSO Group for breaching their

7 See, for instance, Jen Roberts et al., *Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights*, Report, Atlantic Council, 4 September 2024, available at https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.

8 For instance, in the summer of 2021, an international network of journalists and media outlets uncovered the use of NSO software targeting more than 1,000 individuals in over 50 countries, including human rights activists, journalists, business executives, politicians, and government officials. See Washington Post Staff, "Takeaways from the Pegasus Project," *The Washington Post*, 2 August 2021, updated 2 February 2022, available at https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

9 See, for instance, United Nations Office of the High Commissioner for Human Rights, "Spyware scandal: UN experts call for moratorium on sale for 'life threatening' surveillance tech," Press release, 12 August 2021, available at https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

10 David Agranovich and Eneken Tikk, *Meta Policy Recommendations for Tackling the Surveillance-for-Hire Industry*, Policy Paper, Meta, 15 December 2022, available at https://about.fb.com/wp-content/uploads/2022/12/Meta-Policy-Recommendations-for-Tackling-the-Surveillance-for-Hire-Industry.pdf; Microsoft, "Standing up for democratic values and protecting stability of cyberspace: Principles to limit the threats posed by cyber mercenaries," *Microsoft blog post*, 11 April 2023, available at https://blogs.microsoft.com/on-the-issues/2023/04/11/cyber-mercenaries-cybersecurity-tech-accord/.

operating systems and applications.[11] Following revelations that EU member states had used NSO Group's products, the European Parliament established a committee of inquiry, the PEGA Committee, to investigate any alleged misuse of commercial spyware in the region.[12] The US Government implemented a series of policy measures to mitigate human rights harms, including placing spyware providers on its sanctions list, and issuing visa restrictions for individuals working in the spyware industry.[13] The US government also issued an executive order banning federal agencies from using commercial spyware that could pose security risks to the US or that had been misused by foreign actors.[14] Most recently, in 2024, renewed interest and political momentum in the international regulation of commercial spyware technologies has surfaced with the Pall Mall Process, a multistakeholder process initiated by the governments of France and the United Kingdom aimed at tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities.[15]

Against this backdrop, this paper examines one of the most significant multilateral efforts that has been made to date to constrain commercial spyware technologies, namely the use of multilateral export controls under the Wassenaar Arrangement. The issue of human rights harms resulting from the use of commercial spyware technologies first surfaced during the early 2010s. The aftermath of the Arab Spring revealed a pattern of human rights abuses aided by the provision of commercial spyware technologies from Western companies such as Gamma International, Amesys, and Hacking Team. A human rights campaign followed, calling for the

11 See, for instance, Ryan Naraine, "Apple Suddenly Drops NSO Group Spyware Lawsuit," *Security Week*, 13 September 2024, available at https://www.securityweek.com/apple-suddenly-drops-nso-group-spyware-lawsuit/, Reuters, "US judge finds Israel's NSO Group liable for hacking in WhatsApp lawsuit," *Reuters*, 23 December 2024, available at https://www.reuters.com/technology/cybersecurity/us-judge-finds-israels-nso-group-liable-hacking-whatsapp-lawsuit-2024-12-21/. For commentary, see Asaf Lubin, "Unpacking WhatsApp's Legal Triumph Over NSO Group," *Lawfare*, 7 January 2025, available at https://www.lawfaremedia.org/article/unpacking-whatsapp-s-legal-triumph-over-nso-group, and Allie Schiele, "Spyware Company NSO Group Faces Setbacks in Attempts to Avoid US Lawsuits," *Just Security*, 17 January 2025, available at https://www.justsecurity.org/106536/nso-whatsapp-lawsuit/.

12 For an introductory overview, see Eugenia Lostri, "PEGA Committee Votes on Spyware Recommendations," *Lawfare*, 17 May 2023, available at https://www.lawfaremedia.org/article/pega-committee-votes-on-spyware-recommendations. For the report of the PEGA Committee, see "Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware," A9-0189/2023, 22 May 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html#_section3

13 Brian Fung, "Biden administration sanctions makers of commercial spyware used to surveil US," *CNN*, 5 March 2024, available at https://www.cnn.com/2024/03/05/business/biden-administration-sanction-commercial-spyware/index.html; Stephanie Kirchgaessner, "US announces new restrictions to curb global spyware industry," *The Guardian*, 5 February 2024, available at https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions.

14 Executive Order 14093, Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security, 27 March 2023, available at https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to.

15 See announcement of the UK Government, "The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities," 6 February 2024, available at https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

international regulation of these technologies, particularly through restrictions on their sale and export. In response, certain items were added in 2013 to the export control regulations of the Wassenaar Arrangement, a multilateral coordination mechanism for the export of conventional weapons and dual-use items. These changes, which represented the first international effort to directly regulate commercial spyware technologies, have proved highly controversial. Following the Wassenaar controls, international regulation did not significantly progress for several years.

This study provides an in-depth analysis of the Wassenaar export controls by examining their implementation in the European Union (EU) and the US. It identifies lessons learned with regard to the regulation of commercial spyware through export controls of the Wassenaar Arrangement. The goals are to take stock of developments in the field, and to identify challenges and limitations associated with the first multilateral attempt to address the misuse of commercial spyware technologies. The identified lessons learned offer insight into the utility of export controls as a regulatory mechanism. Beyond that, they also hold valuable pointers for future regulatory efforts by states and non-governmental stakeholders. A look at past efforts, their effectiveness, and their challenges is a crucial step for effectively driving new international regulatory efforts forward. With renewed interest and political momentum for multilateral regulation evident in the Pall Mall Process, the experience of Wassenaar export controls holds valuable lessons for stakeholders seeking to address the proliferation and misuse of commercial spyware technologies.

To that end, Part I of the study introduces and defines commercial spyware technologies and the burgeoning international market that has fueled their proliferation. Part I also maps the use of commercial spyware technologies — from legitimate use to their misuse that has been consistently cataloged. While human rights harms resulting from the misuse of commercial spyware have dominated international discussions for years, national security and nonproliferation risks have been raised more recently.

Parts II and III examine the use of export controls under the Wassenaar Arrangement to regulate commercial spyware technologies. Part II describes in depth the developments in the Wassenaar Arrangement that designated certain surveillance and intrusion tools as dual-use items subject to multilateral export controls. This section also introduces the Wassenaar Arrangement, and explains the human rights context for the changes that were made before outlining those changes in detail.

Part III of the study analyzes the implementation of relevant export controls in the European Union and the United States. The experiences in both geographies reveal important differences. Whereas implementation in the US has been fraught with difficulties at first, delaying and calling into question US commitment in this area, the EU has embraced the Wassenaar changes and a human rights-oriented approach in its export control regime. In particular, Part III outlines how the implementation difficulties in the US have contributed to Wassenaar controls being seen as a contentious policy instrument.

Part IV surveys other international or multilateral efforts relevant for the regulation of commercial spyware technologies. While important policies and measures have been taken by various stakeholders, including national governments, the focus in this part is on international efforts that could complement the Wassenaar controls. These include calls for international moratoriums and bans, the recently launched Pall Mall Process, and developments in various UN bodies. These efforts target different aspects of commercial spyware regulation and, more importantly, highlight venues for potential future regulation.

Lastly, Part V identifies three lessons learned from the effort of applying export controls to regulate commercial spyware technologies. This section fleshes out the limits and challenges to the regulation of commercial spyware through export controls. Concluding thoughts summarize the findings and place them in the broader context of efforts to advance international efforts to regulate spyware.

PART I
Commercial Spyware

1. DEFINING COMMERCIAL SPYWARE

While civil society organizations, academics, industry representatives, and policymakers have been discussing commercial spyware for years, there is no agreed-upon definition of the term.[16] Spyware is often described as software that facilitates unauthorized remote access to an internet-enabled device for purposes of surveillance or data extraction.[17] However, depending on individual or institutional preferences, a plethora of other terms are also frequently used in international debates, including "cyber surveillance technology,"[18] "hacker-for-hire,"[19] "cyber mercenaries,"[20] or, more recently, "commercial cyber intrusion capabilities."[21] Definitions of all these terms vary across different government and non-governmental stakeholders.[22]

This paper uses the terms "commercial spyware" or "commercial spyware technology" to describe a set of surveillance goods and technologies that are commercially available. More specifically, it defines commercially available spyware broadly to cover hardware, software, and expertise used to covertly monitor, exploit, and/or analyze data that is stored, processed, and transferred through information and communication technologies (ICTs).[23] The defining feature of commercial spyware is its ability to covertly access and/or monitor communications data, whether at rest or in transit. ICTs can include devices, such as computers and mobile phones, or telecommunications networks as a whole.[24]

16 Heejin Kim, "Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue," *International and Comparative Law Quarterly*, Vol. 70, April 2021, pp. 379–415.
17 See, for instance, Jen Roberts et al. (note 7).
18 See Heejin Kim (note 16).
19 See David Agranovich and Eneken Tikk (note 10).
20 See Microsoft (note 10).
21 See UK Government (note 15).
22 Despite any variances, the term "spyware" is more often than not used as a practical shorthand in discussions. See also Jen Roberts et al. (note 7).
23 Heejin Kim (note 16).
24 Mark Bromley, *Export Controls, Human Security and Cyber-Surveillance Technology. Examining the Proposed Changes to the EU Dual-Use Regulation*, Stockholm International Peace Research Institute, December 2017, available at https://www.sipri.org/publications/2017/other-publications/export-controls-human-security-and-cyber-surveillance-technology-examining-proposed-changes-eu-dual.

Examples of spyware include tools that remotely monitor and control devices such as computers or phones without detection (intrusion software).[25] Other technologies remotely track, identify, intercept, and record mobile and satellite phone calls (mobile telecommunications interception equipment or IMSI Catchers); intercept, collect, and analyze data that passes through an IP network (IP network surveillance systems); or retrieve and analyze communications data that is stored on networks, computers, and mobile devices (digital forensics systems).[26] Broadly speaking, these types of tools enable government entities to identify and monitor individuals or groups.

Due to these capabilities, commercial spyware technologies are considered dual-use items.[27] They can be used to enhance military capabilities as well as to support civilian applications, due to the technologies' "ostensibly legitimate use such as law enforcement and computer security projects."[28] The following analysis focuses on the use and regulation of civilian applications of commercial spyware technologies and excludes their use in the military context.

In addition to the variety of terms used to describe commercial spyware technologies, the term "cyber weapon" has also been used, particularly by mainstream media outlets.[29] The notion of "cyber weapon" has become a popular shorthand to describe a variety of malicious uses of information and communication technologies. As one scholar observes, cyber weapon is "a term often used loosely and without analytical rigour. . . . 'Cyberweapon' has become a catch-all term for diverse forms of malicious software (malware) for which an extraordinary range of capabilities is claimed."[30] However, "cyber weapon" refers to a narrow set of software that can cause physically destructive effects such as death, injury, or damage.[31] Given this understanding, commercial spyware technologies do not qualify as cyber weapons, and their characterization as such has not aided analytical clarity in international governance debates, particularly in the context of dual-use export controls.

25 Ibid. See also Mark Bromley et al., "ICT surveillance systems: trade policy and the application of human security concerns," *Strategic Trade Review*, Vol. 2(2), 2016, pp. 37–52.

26 Mark Bromley (note 24).

27 Ibid. See also Jen Roberts et al. (note 7).

28 Heejin Kim (note 16).

29 See, for example, Ronen Bergman and Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon," *The New York Times*, 28 January 2022, updated 15 June 2023, available at https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

30 Tim Stevens, "Cyberweapons: an emerging global governance architecture," *Palgrave Communications*, Vol. 3, 2017.

31 Bill Boothby, "Cyber weapons: Oxymoron or a real world phenomenon to be regulated?," In Karsten Friis and Jens Ringsmose (eds.), *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (Routledge: Abingdon, UK, 2016), pp. 165–174. Along these lines, Rid and McBurney have advanced a definition of cyberweapons as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings." Thomas Rid and Peter McBurney, "Cyber-weapons," *The RUSI Journal*, Vol. 157 (1), 2012, pp. 6–13.

2. THE USE AND MISUSE OF COMMERCIAL SPYWARE

The demand for commercial spyware technologies is in part fueled by novel challenges that rapid advances in technology have created for states. Individuals generate and exchange a growing amount of data through online communication tools. The proliferation and diversification of online messaging services with default end-to-end encryption has presented a particular challenge for states, which have found traditional intelligence-gathering and interception methods increasingly ineffective.[32]

In response to technological advances, states have sought to establish regulatory frameworks to enable and guarantee access to data for government entities under certain conditions and for certain purposes.[33] Device manufacturers, service providers, and network operators may be requested to cooperate with government authorities in various ways; for example, manufacturers may be required to decrypt encrypted data on a user's device pursuant to a judicial or administrative order.[34]

In addition to compelling business actors to provide access, nation-states have also pursued surveillance capabilities that would ensure government access to relevant communication data. While many states have sought to build these capabilities in-house, an increasing number of governments have turned to the private sector for surveillance capabilities. As Kim explains, "as many countries lack home-grown technological capabilities and telecommunications infrastructure required for extensive surveillance operations, companies find lucrative business opportunities in assisting these States to realise their ambitions for technologically-enabled intelligence and law enforcement."[35] In the end, many states, including European and North American nations, use a variety of spyware technologies, whether natively developed or commercially procured, for intelligence gathering and law enforcement purposes.[36]

The result has been a burgeoning industry and the proliferation of commercially available spyware technologies worldwide. According to one account in 2023, at least 80 out of 193 UN

32 Heejin Kim (note 16). This is often referred to as the "going dark" problem or debate. For an overview, see Jonathan Zittrain, et al., "Don't Panic: Making Progress on the 'Going Dark' Debate," *Berkman Center for Internet & Society at Harvard Law School*, 1 February 2016, available at https://dash.harvard.edu/entities/publication/73120379-2a25-6bd4-e053-0100007fdf3b.

33 Perhaps the best-known framework is that of lawful interception (LI), which describes the process by which a network operator is required to provide communication data to law enforcement or intelligence agencies on the basis of judicial or administrative orders. Most states have laws in place that require compliance by network operators. Regulations also provide for measures to oversee and control the activities of law enforcement and intelligence agencies. See Mark Bromley (note 24).

34 Heejin Kim (note 16).

35 Ibid.

36 Mark Bromley (note 24).

member states are known to have purchased spyware from commercial providers.[37] While the annual revenue generated by this industry is not known and is subject to speculation, it appears to be non-trivial, with estimates of billions of US dollars in revenue.[38]

The companies developing spyware are diverse in terms of their size and portfolio of products, ranging from large military contractors (such as Thales) to large ICT companies (such as Nokia), to smaller ICT companies that specialize in the provision of particular surveillance technologies (such as NSO Group).[39] While publicly available data about providers of commercial spyware technologies is extremely limited, a study from 2024 identified a concentration of companies in three countries: Italy, India, and Israel.[40] Earlier accounts identified leading producers of commercial spyware technologies in the EU, the US, Israel, and, increasingly, China.[41]

However, the spyware industry, including its main suppliers, products, and customers, is characterized by a high degree of opaqueness. More often than not, information about the commercial spyware industry and its technologies has come to light mostly through investigative journalism, civil society research, and high-profile incidents where the use or transfer of certain capabilities was revealed. In addition, discourse has centered around a handful of well-known (or even notorious) firms.[42] Thus, the information about commercial spyware that has been documented so far likely constitutes only a fraction of activities. The lack of transparency in this field has important ramifications for international policymaking. As others have pointed out, "the market for spyware lacks public data that is consistent, reliable, and clearly sourced. . . . Researchers, journalists, and policymakers alike must scrape through a variety of different resources just to scratch the surface of this market that has cloaked itself in secrecy, making it difficult for policy action."[43]

While commercial spyware technologies can be used by law enforcement and intelligence agencies in their exercise of legitimate state functions, repeated revelations of misuse have highlighted the harmful effects these technologies can have for human rights. Misuse has been documented in how certain governments have used these technologies against their citizens, in violation of human rights standards. Following the Arab Spring (in the early 2010s), revelations illustrated the potential uses of commercial spyware technologies to identify and monitor a range of individuals and

37 Alexander Martin, "More than 80 Countries have Purchased Spyware, British Cyber Agency Warns," *The Record*, 19 April 2023, available at https://therecord.media/spyware-purchased-by-eighty-countries-gchq-warns.

38 There are only a few publicly available revenue estimates and their veracity has been questioned. See, for instance, Jen Roberts et al. (note 7).

39 Mark Bromley (note 24).

40 Jen Roberts et al. (note 7).

41 Mark Bromley (note 24). On China, see Heejin Kim (note 16).

42 Jen Roberts et al. (note 7).

43 Ibid.

groups, including opposition politicians, human rights activists, journalists, and others.[44] Spyware tools were used to compromise individuals' devices and to monitor and track activities and communications, resulting or assisting in a range of human rights violations.[45] Since then, reports of human rights abuses have continued unabated, including through investigative journalism initiatives such as the Pegasus Project of 2021, which published numerous accounts of governments using spyware against journalists, opposition politicians, activists, and lawyers.[46] In particular, the targeting of 14 heads of state or government with spyware was widely reported in the news.[47]

In addition to human rights harms, which have dominated the international discourse for years, national security and nonproliferation risks have recently come into focus as well. Commercially available spyware technologies are increasingly seen as a risk to national and international security as they enable an increasing number of states to acquire and build capabilities for various cyber operations, including cyber espionage for commercial or intelligence purposes.[48]

In the end, states have shown an undeniable interest in commercial spyware technologies, which arguably have legitimate uses by law enforcement and intelligence agencies. However, human rights harms — and, more recently, national security risks — have highlighted significant concerns with the use and misuse of these technologies, resulting in repeated calls for national and international regulation.

• • •

In summary, a range of different terms are used by stakeholders to discuss what this paper describes as "commercial spyware," a set of commercially marketed technologies with the ability to covertly access and/or monitor communications data of individuals and groups. Terminology and understanding are far from settled in this space. Nonetheless, given the rapid technological advances and changing needs of government agencies, a burgeoning industry of commercial spyware technology providers has developed. This industry caters to legitimate uses of these technologies by law enforcement and intelligence agencies to gain and maintain access to communication data. The value of commercial spyware technologies, however, has been counterbalanced by frequent and sustained revelations of the technologies' misuse by governments, resulting in a range of human rights violations.

44 See Part II, Section 4 of this paper for an extended discussion.

45 Investigations into the trade and use of cyber tools were undertaken by two major news outlets, the *Wall Street Journal* and *Bloomberg*. In addition, many individual reports were released by civil society groups and research outlets such as Privacy International and the Citizen Lab at the University of Toronto.

46 See Washington Post Staff, "Takeaways from the Pegasus Project," *The Washington Post*, 2 August 2021, updated 2 February 2022, available at https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

47 See, for instance, BBC, "Pegasus spyware: French President Macron changes phone after hack reports," *BBC News*, 22 July 2021, available at https://www.bbc.com/news/world-europe-57937867.

48 Jen Roberts et al. (note 7).

PART II
Regulating Commercial Spyware Through Export Controls
The Wassenaar Arrangement

3. OVERVIEW OF THE WASSENAAR ARRANGEMENT

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, often referred to as the "Wassenaar Arrangement," was established in 1996.[49] As its name suggests, the Arrangement's focus is on conventional weapons and dual-use items. It forms an important part of the current multilateral export control system that contains separate regulations for weapons of mass destruction and their delivery systems.[50] The overarching goal underlying these regulations is to control the spread of certain items or technologies through a harmonization and coordination of individual states' export control policies. Thus, the Wassenaar Arrangement targets only the transfer of certain items, and not their development, production, possession, or use.

The goals of the Wassenaar regime are framed in distinctly international security and stability terms. Wassenaar's participating states seek to "contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies" in order to prevent "destabilizing accumulations."[51] The Arrangement's transfer policy aims to reinforce existing export control regimes for weapons of mass destruction and their delivery systems, and also includes measures aimed at preventing terrorists or terrorist groups from acquiring conventional weapons and dual-use items.[52]

49 The basic documents of the Wassenaar Arrangement have been compiled by the Arrangement's Secretariat as *Public Documents Volume I: Founding Documents* and are available at https://www.wassenaar.org/app/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf.

50 The other regimes are the Nuclear Suppliers Group (working to restrict the proliferation of nuclear weapons), the Australia Group (focused on chemical weapons and biological weapons production equipment), and the Missile Technology Control Regime (seeking to control missile proliferation).

51 See Wassenaar Arrangement, *Guidelines and Procedures, including the Initial Elements*, February 2017, contained in https://www.wassenaar.org/app/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf.

52 Ibid.

It is important to note that Wassenaar, as an export control mechanism, does not constitute an outright ban on the transfer of conventional weapons and dual-use items. Its scope is much more limited. Essentially, participating states commit to coordination and harmonization of their national export control policies. The Wassenaar Arrangement maintains two control lists: the Munitions List, which covers conventional weaponry, and the List of Dual-Use Goods and Technologies.[53] Participating states commit to control all items on either of those lists through their national export regulations.[54] The transfer of items placed on Wassenaar's control lists is not necessarily prohibited. Rather, items can still be exported but become subject to national export licensing procedures (and relevant licensing outcomes). In this sense, the Wassenaar Arrangement does not prohibit the transfer of conventional weapons or dual-use items, but functions as a mechanism to control the distribution or flow of items. The control lists are reviewed and updated regularly, and any decisions are taken by consensus.[55] While the two control lists form the core of the Arrangement, participating states also commit to sharing information and notifying members of transfers or denials of dual-use items to non-member states.[56] Members of the Arrangement undertake their discussions privately, and issue few public statements to provide insight into their decisions.[57]

Once the membership of the Arrangement decides to place a certain item on one of its control lists, the implementation is left entirely to participating states. Changes have to be implemented and applied on a national level to become effective, and a great deal of discretion is left to individual states. As Wassenaar's guiding document lays out, "[t]he decision to transfer or deny transfer of any item will be the sole responsibility of each Participating State. All measures undertaken with respect to the Arrangement will be in accordance with national legislation and policies and will be implemented on the basis of national discretion."[58] In addition, the Arrangement's guiding documents do not provide for any sanction or enforcement mechanisms if a state fails to transpose changes to Wassenaar's control lists into its domestic legislation.[59]

Lastly, the Wassenaar Arrangement is not a universal international instrument; its membership is limited and its regulatory reach, by definition, does not extend beyond its members. As of

53 Current and former lists are available at https://www.wassenaar.org/control-lists/.

54 See Wassenaar Arrangement, *Guidelines and Procedures, including the Initial Elements*, February 2017, contained in https://www.wassenaar.org/app/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf.

55 Ibid.

56 Ibid.

57 Ibid.

58 Ibid.

59 For a discussion of this point, see Innokenty Pyetranker, "An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement," *Northwestern Journal of Technology and Intellectual Property*, Vol. 13(2), 2015, pp. 153–180.

2025, Wassenaar's membership extends to 42 states, covering mainly OECD member states, as well as Ukraine, the Russian Federation, and South Africa.[60] In 2017, India was welcomed as the newest member to the Arrangement.[61] Although its membership includes most major industrialized nations and leaders in technological innovation, the Arrangement currently excludes important states, such as Israel and China. This limits the potential effectiveness of Wassenaar's multilateral export control efforts.

4. HUMAN RIGHTS CONTEXT OF WASSENAAR CONTROLS ON COMMERCIAL SPYWARE

The members of the Wassenaar Arrangement added a number of commercial spyware tools to their dual-use control list in 2013. As detailed below, this move proved to be a significant and controversial multilateral effort to regulate commercial spyware. The Arrangement covered a particular set of technologies, namely surveillance and intrusion tools. These types of tools became the focus of multilateral efforts following a string of revelations in the aftermath of the Arab Spring in 2011. Various surveillance or spyware technologies had been linked to repressive practices by authoritarian governments. Human rights considerations helped motivate the regulation of commercial spyware technologies by Wassenaar, and were seen by many as the main reason for the additions of 2013.

For years, media and NGO reports have linked the export of surveillance systems and intrusion software to violations of human rights.[62] The use of commercially marketed surveillance technology by authoritarian governments has been described as a "global policy problem."[63] The issue first gained broader coverage following the 2011 Arab Spring and its aftermath, when the use of surveillance technologies in countries such as Libya, Syria, and Bahrain was revealed.[64] In the case of Libya, French company Amesys was reported to have provided an internet monitor-

60 The full list of participating states includes: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and the United States.

61 See Wassenaar Arrangement, *India Becomes 42nd WA Participating State*, 8 December 2017, available at https://www.wassenaar.org/india-becomes-42nd-wa-participating-state-8-dec-2017/.

62 In an early instance from 2009, it was revealed that Nokia Siemens Networks had supplied one of the main mobile phone operators in Iran with technologies enabling the interception and collection of communications data. Reportedly, the information collected by the government was used in efforts to identify and monitor activists, who were ultimately detained and tortured. See Mark Bromley (note 24).

63 UNHCR, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Surveillance and Human Rights*, A/HRC/41/35, 28 May 2019.

64 For an excellent overview, see research and analysis by Citizen Lab and Access now.

ing system to the Gaddafi regime that was deployed against political dissidents, human rights advocates, and journalists.[65] A lawsuit alleging Amesys' complicity in acts of torture committed by the Gaddafi regime followed.[66] British-German company Gamma International was criticized for its FinFisher intrusion system, which was used by the government of Bahrain to monitor high-profile dissidents by remotely accessing devices, copying files, intercepting calls, and logging keystrokes.[67] Later, the infamous hack of Italian company Hacking Team revealed technology sales to countries such as Bahrain, Egypt, Ethiopia, Kazakhstan, Nigeria, Sudan, and Saudi Arabia.[68]

The (mis)use of spyware technologies has been linked with a range of human rights violations. The "most concrete examples"[69] involve the right to privacy, as any interception of communications or collection of personal data may constitute an interference with that right. However, as civil society groups and other actors have argued, these technologies enable a range of human rights infringements and violations:

> [T]he private text messages of activists are read out to them as they are tortured; . . . political refugees find their computers have been hacked and their digital life stolen. Surveillance technologies are used by governments to target opponents, journalists and lawyers, crack down on dissent, harass human rights defenders, intimidate populations, discourage whistle-blowers, chill expression and destroy the possibility of private life . . . In short, they are often part of a broader state apparatus of oppression, facilitating a wide variety of human rights violations including unlawful interrogation practices, torture and extrajudicial executions.[70]

The Arab Spring revelations generated widespread attention on the issue of human rights violations and the role of commercial spyware technologies. In April 2014, several non-governmental organizations formed the Coalition Against Unlawful Surveillance Exports (CAUSE).[71] Human Rights Watch, Privacy International, Reporters Without Borders, and others involved in the campaign called for the effective regulation of surveillance technologies. According to the coa-

65 Margaret Coker and Paul Sonne, "Life Under the Gaze of Gadhafi's Spies," *The Wall Street Journal*, 14 December 2011, available at https://www.wsj.com/articles/SB10001424052970203764804577056230832805896.

66 Business and Human Rights Resource Centre, *Amesys lawsuit (re Libya)*, available at https://www.business-humanrights.org/en/amesys-lawsuit-re-libya-0?page=1.

67 Vernon Silver, "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma," *Bloomberg*, 25 July 2012, available at https://www.bloomberg.com/news/articles/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.

68 Andy Greenberg, "Hacking Team Breach Shows a Global Spying Firm Run Amok," *Wired*, 6 July 2015, available at https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/.

69 Mark Bromley (note 24).

70 Privacy International, *BIS Submission*, available at https://privacyinternational.org/sites/default/files/2018-02/Privacy%20International%20BIS%20submission.pdf.

71 CAUSE members are: Amnesty International, Human Rights Watch, FIDH, Privacy International, Reporters Without Borders, Digitale Gesellschaft, and the Open Technology Institute.

lition's members, "[t] he unchecked development, sale and export of these technologies is not justifiable. Governments must swiftly take action to prevent these technologies spreading into dangerous hands."[72] CAUSE member organizations documented global export flows of technology, along with patterns of human rights violations in countries such as Bahrain, Morocco, Turkmenistan, Ethiopia, the United Arab Emirates, Egypt, and Nigeria.[73]

These developments provided the context in which the Wassenaar changes of December 2013 emerged. The relevant additions — IP surveillance systems and items related to intrusion software — had figured prominently in reports of human rights violations. In light of the commercial market for these types of technologies, the use of export controls appeared to be a promising avenue to address human rights violations. As Kim pointed out, "[b]y restricting the supply side of cyber surveillance goods and technologies, export control mechanisms can provide one of the few options to effectively regulate its availability and transfer."[74] In the end, human rights considerations were reportedly "at least in part" a clear motivating factor for the two states that submitted the proposals for the 2013 changes, namely France and the United Kingdom.[75]

Despite media revelations and human rights campaigns advocating for export restrictions of specific technologies, the official statement of the Wassenaar Arrangement in 2013 avoided any human rights references, and simply stated that the newly-added provisions included systems and tools that "under certain conditions, may be detrimental to international and regional security and stability."[76] This wording focused on international security ramifications, in line with Wassenaar's goals and rationale. Perhaps unsurprisingly, given Wassenaar's focus on conventional and dual-use items, the additions of 2013 were described in terms of weapons. *The Financial Times* referred to the decisions of Wassenaar as "[c]yber war technology to be controlled in same way as arms."[77] Some commentators equated surveillance systems and

72 Heini Järvinen, *Human rights orgs form coalition against surveillance exports*, European Digital Rights, 9 April 2014, available at https://edri.org/human-rights-orgs-form-coalition-against-surveillance-exports/.

73 See, for example, the list in Reporters Without Borders, *New global coalition urges governments to keep surveillance technologies in check*, 4 April 2014, available at https://rsf.org/en/new-global-coalition-urges-governments-keep-surveillance-technologies-check.

74 Heejin Kim (note 16).

75 Privacy International (note 70).

76 The 2013 Public Statement is available in Wassenaar Arrangement, *Public Documents Volume IV: Background Documents and Plenary-related and Other Documents*, December 2017, available at https://www.wassenaar.org/app/uploads/2017/12/WA_Public_Docs_Vol_IV_Background_Docs_and_Plenary-related_and_other_Statements.pdf.

77 Sam Jones, "Cyber war technology to be controlled in same way as arms," *Financial Times*, 4 December 2013. Available at https://www.ft.com/content/2903d504-5c18-11e3-931e-00144feabdc0.

intrusion software to "sophisticated cyberweapons,"[78] while others characterized the changes as an effort to "curtail the proliferation of 'active' or 'offensive' cyber technologies used to initiate offensive cyber attacks or actively mine and analyze protected data."[79]

While the 2013 changes to the Wassenaar dual-use list emerged in the context of human rights concerns, and were at least partially driven by a political desire to address human rights violations, controversy around surveillance and intrusion tools has not dissipated. On the contrary, in the years since, there has been continued coverage of the use of commercial spyware technology by government entities all around the world in ways that appear to violate human rights obligations. Israeli company NSO Group has become infamous for, and perhaps synonymous with, the continued export and use of spyware technology in ways that raise human rights concerns.[80] At the same time, advocacy and research groups have continued to push for national and international measures to restrict the transfer of certain cyber capabilities beyond the 2013 additions to the Wassenaar Arrangement.

5. OVERVIEW OF WASSENAAR CONTROLS ON COMMERCIAL SPYWARE

At its annual review meeting in December 2013, the participating states of the Wassenaar Arrangement added two entries to its List of Dual-Use Goods and Technologies: *IP network surveillance systems* and *items related to intrusion software*. The specific definitions used in the list have been criticized by a range of stakeholders,[81] and have generated considerable controversy with regard to the Arrangement's utility in regulating cyber tools more broadly.[82] Both additions are described in detail below.

78 Willie Jones, "Treaty Limiting Weapons Exports Updated to Include Cyberweapons," *IEEE Spectrum*, 6 December 2013, available at https://spectrum.ieee.org/riskfactor/telecom/security/treaty-limiting-weapons-exports-updated-to-include-cyberweapons.

79 Daniel Reisner and Doron Hindin quoted in Innokenty Pyetranker (note 59).

80 See, for example, Andrew Blake, "Israeli spyware found on phones in 45 countries, U.S. included," *The Washington Times*, 18 September 2018, available at https://www.washingtontimes.com/news/2018/sep/18/israeli-spyware-found-phones-45-countries-us-inclu/.

81 Part III, Section 7 in this paper, Implementation of Wassenaar Controls in the United States, offers a detailed description of relevant criticism.

82 Despite the notoriety of the 2013 additions, this may not have been the first time that the Wassenaar Arrangement had sought to control the transfer of systems relevant to cybersecurity. Since the 1990s, the Arrangement has controlled certain systems on its Dual-Use List due to the standard of encryption they contained. With these encryption controls, even before the changes in 2013, some surveillance tools were arguably covered by the Arrangement's controls due to their cryptographic components. However, the additions in 2013 were novel in that they subjected a certain set of cyber tools to export controls irrespective of their cryptographic characteristics.

The first entry added to the Dual-Use control list in 2013 comprised *IP network surveillance systems*. A new category — Category 5.A.1.j. — was added to a section covering "Telecommunications." The scope of this provision is narrow, targeting only systems that can operate on a nationwide level to intercept internet traffic and conduct high-performance analysis of communications data.[83] A number of requirements need to be met, indicating that "the clear intention is to cover [only] those technologies used for so-called mass surveillance."[84]

According to Category 5.A.1.j., "IP network communications surveillance systems or equipment, and specially designed components therefor" are placed under export controls if they satisfy a number of conditions. First, they need to be able to perform all of the following functions on a "carrier class IP network," such as a 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.

Second, these systems or equipment need to be "specially designed" to carry out all of the following activities:

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.[85]

Taken together, these requirements ensured that only a narrow segment of network surveillance systems would be covered by the Wassenaar restrictions. The requirement for the mapping of relational networks was especially key in this regard, as it is "a highly sophisticated function that is used only in limited kinds of surveillance products such as the products specifically marketed for intelligence activities."[86] The limited scope of the provision on IP network

83 Heejin Kim (note 16). See also Jukka Ruohonen and Kai K. Kimppa, "Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity," *Journal of Information Technology & Politics*, Vol. 16, 2019, pp. 169–195.
84 Jukka Ruohonen and Kai Kimppa (note 85).
85 See Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (15) 1 Corr. 1 of 4 April 2016, p. 80, available at https://www.wassenaar.org/app/uploads/2016/04/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf.
86 Heejin Kim (note 16).

surveillance systems has been criticized for being overly restrictive, and for excluding other types of network surveillance systems that have been used by repressive regimes.[87]

However, the second entry added to the Dual-Use control list in 2013 — *items related to intrusion software* — proved to be far more controversial than the first. The items in question were added to Category 4 of the Dual-Use list, which covers "Computers" and were meant to address tools used to surreptitiously gain access to (or hack) devices in order to obtain information or spy on individuals. The additions did not seek to control intrusion software per se, but specific items used to generate and operate such software. This delineation is intended to restrict the infrastructure used to generate, install, and control intrusion tools, i.e. the components that remain with the purchaser, but not any component that would end up on the device of a targeted user.[88]

Specifically, controls were added for "systems, equipment, and components" (Category 4.A.5.) as well as "software" (Category 4.D.4.) that is "specially designed or modified for the generation, operation or delivery of, or communication with, 'intrusion software'".[89] Controls were also added for "technology" used "for the 'development' of 'intrusion software'" (Category 4.E.1.c.).[90] The meaning of "development" is fairly broad and captures numerous activities, including design, design research, assembly, testing of prototypes, and technical assistance, such as training and instruction.[91] Thus, specific types of equipment, software, and technology related to intrusion software, rather than intrusion software itself, are covered by the 2013 additions. To operationalize these provisions, the Wassenaar Arrangement defines *intrusion software* essentially as software capable of performing one of two specific functions. Intrusion software is described 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 use 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.[92]

87 Ibid.

88 Fabian Bohnenberger, "The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls," *Strategic Trade Review*, Vol. 3(4), 2017, pp. 81–102.

89 See Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, pp. 72–73 (note 87).

90 Ibid, p. 73.

91 Heejin Kim (note 16).

92 See Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, p. 210 (note 77).

In light of these definitions, the scope of the controls on items related to intrusion software was criticized by a range of stakeholders as being overly broad, capturing not only intended hacking tools but also a number of essential cybersecurity processes.[93] As described further below, the US private-sector and security research communities voiced serious concerns and lobbied the US government to ultimately seek changes to the language of the 2013 Wassenaar additions. This resulted in a number of adjustments to the original 2013 provisions in subsequent years. The US made proposals to narrow the scope of controls on items related to intrusion software that led to changes in 2016 and 2017.

While the 2016 meeting of Wassenaar members produced only minor adjustments,[94] the decisions in 2017 carved out important exemptions. In essence, the scope of provisions related to intrusion software was narrowed by adding a number of exemptions for key cybersecurity practices and activities. A note appended to the controls on "software" (Category 4.D.4) created an exception for software updates or upgrades that operate "only with the authorization of the owner or administrator of the system receiving it."[95] More prominently, exemptions for "vulnerability disclosure" and "cyber incident response" were added to the controls on "technology" used for the development of intrusion software (Category 4.E.1.c.).[96] Vulnerability disclosure is defined as "the process of identifying, reporting, or communicating a vulnerability to, or analyzing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability."[97] Cyber incident response covers "the process of exchanging necessary information on a cyber security incident with individuals or organizations responsible for conducting or coordinating remediation to address the cyber security incident."[98]

With these changes, the members of the Wassenaar Arrangement sought to exclude "essential cyber security tools that inappropriately fell within the meaning of [the] initial cyber amendment."[99] The exemptions were welcomed by US government officials, private sector, and

93 See Part III, Section 7 Implementation of Wassenaar Controls in the United States for a detailed discussion.

94 See Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (16) 1 Corr. 1 of 17 February 2017, p. 74, available at https://www.wassenaar.org/app/uploads/2016/12/List-of-Dual-Use-Goods-and-Technologies-and-Munitions-List-Corr.pdf.

95 See Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (17) 1 of 7 December 2017, p. 78, available at https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf.

96 Ibid., p. 79.

97 Ibid.

98 Ibid.

99 Heejin Kim (note 16).

research community representatives, who had voiced criticism at the initial 2013 additions.[100] Since then, only minor editorial adjustments have been made.[101]

Overall, export controls on IP surveillance systems and items related to intrusion software that were added in 2013 have remained on Wassenaar's Dual-Use list. Relevant criticism was addressed in 2017 by narrowing the scope of controls on items related to intrusion software, most notably through a number of exemptions for vulnerability disclosure and cyber incident response. It remains to be seen whether these changes will be further amended to include more exemptions, or even to factor in a more substantial review of the initial control provisions. Similarly, it is unclear whether other types of commercial spyware tools, beyond IP surveillance and intrusion technologies, will be considered for inclusion in the Arrangement in the future.[102] In light of the discussions surrounding the 2013 additions, and the changed geopolitical landscape, it appears doubtful that participating states will introduce additional controls in this area.

• • •

In summary, the 2013 additions to the Wassenaar Arrangement represented the first significant multilateral effort to regulate commercial spyware technologies. Yet these efforts are limited in scope. Since the Wassenaar Arrangement is a multilateral instrument for the harmonization of export controls, the additions seek to regulate the transfer or flow of technologies, not their development, possession, or use. In addition, the original 2013 changes and subsequent amendments target a narrow set of commercial spyware technologies: IP surveillance systems, and items related to intrusion software.

The 2013 additions were reportedly introduced by the United Kingdom and France, amidst criticism of human rights violations connected with the use of these systems by repressive regimes. Although Wassenaar's mandate does not mention human rights concerns, the changes intro-

100 See, for example, Tom Cross, "New Changes to Wassenaar Arrangement Export Controls Will Benefit Cybersecurity," *Forbes*, 16 January 2018, available at https://www.forbes.com/sites/forbestechcouncil/2018/01/16/new-changes-to-wassenaar-arrangement-export-controls-will-benefit-cybersecurity/#4b9915615ed6.

101 The definitions for "vulnerability disclosure" and "cyber incident response" were moved from the local to the global definitions section. This changed their place in the Wassenaar Dual-Use List. The definitions themselves remained the same.

102 While no further changes have been made to the Dual-Use List, controls were added to the Munitions List in December 2019, namely for software designed or modified for the "conduct of military offensive cyber operations." See Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (19) 1 of 5 December 2019, p. 212, available at https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-19.pdf.

duced these considerations — at least to some extent — into the export control debate.[103] Human rights advocates sought to address commercial spyware tools used to infiltrate and track individuals' devices, as well as systems that can carry out large-scale analysis of networks. The 2013 additions to the Agreement applied export control restrictions to IP surveillance systems and items related to intrusion software. However, the regulation of these and other tools remains a pressing issue, as cases of misuse and abuse continue unabated.

In contrast, the 2016 and 2017 changes to Wassenaar's control lists were proposed by the United States. The changes sought to narrow the scope of the provisions on items related to intrusion software. These provisions were criticized by the private sector and the cybersecurity research community in the US for being overly broad. It remains to be seen whether members of the Wassenaar Arrangement will further amend existing provisions or place additional technologies on the dual-use control list in the future. Prospects for further controls are in part influenced by the experiences of different nations in implementing the changes to date, as detailed in the following section.

103 Particularly in the case of the United Kingdom, it remains unclear whether human rights were the sole motivating factor for the proposed additions. According to some, the UK proposal was aimed at controlling "Advanced Persistent Threat Software and related equipment (offensive cyber tools)." See Privacy International, *International Agreement Reached Controlling Export of Mass and Intrusive Surveillance Technology*, 8 December 2013, available at https://privacyinternational.org/blog/1218/international-agreement-reached-controlling-export-mass-and-intrusive-surveillance.

PART III

Regulating Commercial Spyware Through Export Controls

Implementation in the EU and the US

6. IMPLEMENTATION OF WASSENAAR CONTROLS IN THE EUROPEAN UNION

The prominence of European companies in the early revelations about human rights abuses and the export of commercial spyware technologies has resulted in significant attention being paid to this issue among stakeholders in the European Union and its member states. Relevant additions and changes agreed to in the Wassenaar Arrangement were swiftly implemented by the EU. More importantly, the need to address the proliferation of cyber surveillance technology has been a driving force for a broader revision of the EU's export control regime that has been underway for several years.

The EU provides a common legal framework for its membership, centralizing the regulation of dual-use export controls. This framework establishes the free transfer of dual-use items within the EU single market while restricting the export, brokering, transit, and transfer of dual-use items to destinations outside of the Union. The EU's mandate in dual-use export controls is rooted in the "common commercial policy," an area where the EU has "exclusive" competence.[104] EU regulations are legally binding and directly applicable in member states, but their implementation and enforcement are left to national authorities. This means that decisions related to the granting or denial of export licenses are made at the national level. Council Regulation 428/2009, adopted in May 2009, formed the legal basis for the Union's common policy on dual-use export controls during the 2013 Wassenaar additions and their subsequent changes.[105] This regulation was replaced in September 2021 with the "recast" Dual-

104 Areas of "exclusive" competence give the EU the ability to legislate alone, except where member states have been specifically empowered to do so. Measures adopted by the EU are legally binding and directly applicable throughout EU member states.

105 See Council Regulation (EC) No 428/2009 of 5 May 2009, setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. The text is available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0428&from=EN.

Use Regulation (Regulation 2021/821), which was the result of a reform process that had been underway since 2011.[106]

Following the 2013 additions to the Wassenaar Arrangement, the EU moved to add the relevant items to its dual-use control list in December 2014.[107] The subsequent changes to controls on items related to intrusion software were likewise incorporated into the EU control lists.[108] The 2014 implementation by the EU generated some initial controversy around the scope of controls on intrusion software, as cybersecurity researchers warned of unintended consequences for essential cybersecurity practices and activities.[109] However, early guidance from governments seemed to alleviate at least some of the initial concerns, suggesting that the controls were not geared toward legitimate cybersecurity activities, if properly applied.[110] Attention thus quickly shifted away from the scope of the controls to their actual implementation by EU member states.

Following the implementation of Wassenaar controls in 2014, the effectiveness of EU export controls has been questioned on the basis that member states have not uniformly or consistently applied the mandated controls. For instance, Denmark's reported approval for the export of IP surveillance systems to Qatar highlighted concerns that states had not taken a restrictive approach when it comes to approving export licenses.[111] Similarly, the types of export licenses for which exporting companies were required to apply have varied considerably. Germany, for instance, appears to have controlled exports involving intrusion software by requiring individual licenses for every export, while Italy has issued global or general licenses that enabled multiple exports that were valid for multiple years and destinations.[112] However, it has been difficult to

106 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, and transit and transfer of dual-use items (recast). The text is available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=EN.

107 Dual-use exports were regulated through Regulation 428/2009, but in order to avoid delays, the Commission delegated authority to update the control list pursuant to Regulation 599/2014.

108 Commission, Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009, COM (2019) 562 final (2019).

109 See, for example, Sergey Bratus et al., *Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense at Risk — And How To Fix It*, 9 October 2014, available at https://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf. In contrast, the provision on IP surveillance systems was seen as too narrow by some. See, for example, Privacy International (note 103).

110 See, for example, Colin Anderson, *Considerations on Wassenaar Arrangement Control List Additions For Surveillance Technologies*, Access, March 2015, available at https://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf.

111 Mark Bromley (note 24).

112 Ibid.

assess licensing policies and their restrictiveness due to a lack of comparable and comprehensive data regarding approvals and denials of license applications across EU member states.[113]

More importantly, the regulation of commercial spyware technologies has played a prominent role in the lengthy review of the EU dual-use export control regime that concluded in 2021. Revelations implicating EU-based technology companies following the uprisings of the Arab Spring were an important impetus for comprehensive reform efforts.[114] Due to this context, human rights concerns shaped the reform process in fundamental ways. The EU's approach has been described as "rights-based export controls."[115] Reform proposals unequivocally emphasized human rights considerations in order to restrict exports of surveillance systems and intrusion software. As the impact assessment for the proposed reform stated, changes to the existing regime "appear[s] indispensable to achieve the objective to prevent human rights violations caused by the lack of appropriate controls of cyber-surveillance technology."[116]

In the end, the final text of the recast Dual-Use Regulation did not embrace all the proposed policy changes. However, controversy centered not around whether human rights should play a role in regulating export controls of commercial spyware tools, but rather to what extent they should be strengthened in the export control process. Thus, the reform of the EU export control regime has brought about a greater human rights orientation, though not one as ambitious as previously thought. The review of the EU's export control regime, which had begun in 2011, aimed to modernize the existing legal framework, chiefly to replace the 2009 Dual-Use Regulation. In September 2016, the European Commission proposed a draft regulation that would "recast" the existing Dual-Use Regulation.[117] The proposal was subject to the ordinary legislative procedure of the European Union, which means that it had to go through a process involving the European Commission, the Council, and the European Parliament.[118] In January

113 Ibid. A notable development to partly address this issue is the publication of the first annual report on the implementation of EU export controls in January 2025. The report is mandated by the recast EU Dual-use Regulation and contains aggregated data regarding EU member states' export control decisions. See Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, COM(2025) 19 final, 30 January 2025, available at https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2025)19&lang=en.

114 Heejin Kim (note 16).

115 Ibid.

116 European Commission, Report on the EU Export Control Policy Review — Executive Summary of the Impact Assessment (Accompanying the Proposal, 28 September 2016, available at http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf.

117 This followed a process involving several proposals, assessments, and consultations. European Commission, Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast), COM(2016) 616 final, 28 September 2016, available at https://eur-lex.europa.eu/resource.html?uri=cellar:1b8f930e-8648-11e6-b076-01aa75ed71a1.0013.02/DOC_1&format=PDF.

118 For a detailed overview of the process, see Mark Bromley (note 24).

2018, the European Parliament commented on the Commission's draft, submitting a set of amendments that largely endorsed the main components.[119] However, the Council's negotiating mandate and response, adopted in July 2019, was markedly different, dismissing key proposals with regard to spyware technologies.[120] Extensive negotiations among all three institutions followed that culminated in a "final compromise text" in November 2020.[121] The resulting recast Dual-Use Regulation (Regulation 2021/821) formally went into effect on September 9, 2021.[122]

On the one hand, the Commission proposal placed significant emphasis on the issue of commercial spyware, expanding controls over surveillance and other tools while enhancing the role of human rights concerns in the export control process. For example, the proposal created a new control category dedicated to "cyber-surveillance technology," with a list of items identified under this new category.[123] This "autonomous" EU list would have enabled the Commission to add items if "necessary due to risks that the export of cyber surveillance items may pose as regards the commission of serious violations of human rights or international humanitarian law."[124] This meant that additional cyber tools could be added by the Commission independent of changes within the Wassenaar Arrangement, and on the basis of human rights concerns. According to Bromley, "[t]his would for the first time, create an EU control list for dual-use items that is not drawn from one of the multilateral export control regimes, and give the Commission the ability to take the lead on adding items to the EU dual-use list."[125] Two such items that were initially included were monitoring centers and data retention systems.[126]

Another example of the enhanced role of human rights in the Commission's proposal (as amended by the Parliament) was the creation of a so-called "catch-all" control for the export of non-listed items that applies in certain situations. Accordingly, cyber surveillance items not listed in the EU Dual-Use Regulation can still be subjected to export controls if they are used "in connection with violations of international human rights law or international humanitarian law

119 Draft European Parliament Legislative Resolution in: European Parliament, Report on the Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items, European Parliament, Committee on International Trade, Report 2016/0295 (COD), 19 December 2017, available at https://www.europarl.europa.eu/doceo/document/A-8-2017-0390_EN.html

120 See EPRS, *Briefing: EU Legislation in Progress, Review of Dual-Use Export Controls*, November 2019.

121 See Heejin Kim (note 16).

122 Regulation (EU) 2021/821 (recast) (note 106).

123 The proposal explicitly expanded the EU's definition of "dual-use items" to include "cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law, or can pose a threat to international security or the essential security interests of the Union and its Member States." See European Commission (note 117).

124 Ibid.

125 Mark Bromley (note 24).

126 Ibid.

in countries where serious violations of human rights have been identified by the competent bodies of the UN, the Council of Europe and the Union or national competent authorities."[127]

On the other hand, the Council signaled a more reserved stance, seeking to limit the prominence of human rights considerations in export controls of spyware technologies. It rejected both the creation of an autonomous EU list for cyber surveillance items and the incorporation of a "catch-all" provision.[128] Several EU member states expressed concerns that the expansion of controls for commercial spyware beyond those agreed to within Wassenaar would lead to the EU working "in isolation".[129] Moreover, states warned that stricter export controls could negatively impact the economic competitiveness of EU-based companies, particularly vis-à-vis the US and China, and that the proposed provisions would undermine innovation and disrupt industry supply chains.[130]

In the end, the compromise reached reflected the intense debate among industry, civil society organizations, European institutions, and national governments.[131] It recognizes the need to curb the flow of commercial spyware technologies and strengthen human rights considerations, though not to the extent envisioned by the Commission and the Parliament. The recast Dual-Use Regulation does not, for example, provide for an autonomous control list for cyber surveillance items. In other words, the EU does not go beyond its commitments in the Wassenaar Arrangement. This also means that monitoring centers and data retention systems (as proposed by the Commission and Parliament) have not been added to the dual-use control list. The "catch-all" clause for cyber surveillance items, however, did become part of the recast Dual-Use Regulation. Cyber surveillance items that are not listed by the EU can still fall under export controls if "the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law."[132]

All in all, the EU's implementation of Wassenaar's additions of surveillance and intrusion tools has been relatively swift, with attention shifting to the operationalization of export controls by EU member states. In addition, the prominence of EU-based companies in the surveillance industry was an important driver for a broader review of EU export control policy, resulting in

127 European Commission (note 117).
128 Heejin Kim (note 16).
129 Ibid.
130 Ibid.
131 For an in-depth discussion of stakeholder reactions, see Mark Bromley (note 24) and Fabian Bohnenberger (note 88).
132 Regulation (EU) 2021/821 (recast) (note 106).

a new, recast Dual-Use Regulation. This updated regulation reflects the ambition of EU member states to restrict the flow of various spyware technologies and to place greater emphasis on human rights in the export control process. While many provisions from the initial reform proposal did not materialize due to economic and political concerns, the recast Dual-Use Regulation still advances an EU export control policy that is markedly oriented toward human rights.

7. IMPLEMENTATION OF WASSENAAR CONTROLS IN THE UNITED STATES

After the EU's implementation of Wassenaar's cyber controls, the US sought to implement the additions of surveillance and intrusion tools in 2015. Relevant US agencies proposed guidance that was criticized by industry, security researchers, and non-governmental organizations for being overly broad. As a result, and in contrast to developments in the EU, the government announced its decision not to go through with the proposed implementation, as well as its intent to return to negotiations within Wassenaar to amend the original additions of 2013. This led to the changes of 2016 and 2017 described above. Only in 2021 — several years after the initial Wassenaar provisions were introduced — did the US return to the issue and implement the amended controls. Together with other efforts, such as the Export Controls and Human Rights Initiative, the implementation, although belated, signaled a greater US engagement in the regulation of surveillance technologies and related human rights concerns by the Biden Administration. Broader reforms of the US export control regime may also enable controls for an increasing number of commercial spyware technologies in the future. However, these reform efforts have been driven by increasing economic and technological competition between the US and China.

The US set out to implement the 2013 Wassenaar additions involving surveillance and intrusion tools in 2015. Dual-use items are subjected to export controls through the so-called Commerce Control List (CCL), which is a list of items, as well as foreign persons and end-uses, "that are determined to be a threat to the national security and foreign policy of the United States."[133] The main legal framework for the CCL is the Export Administration Regulations (EAR).[134] The CCL is maintained by the Bureau of Industry and Security (BIS), within the Department of Commerce (DOC). The BIS is also responsible for export licensing and enforcement functions. In May 2015, the Bureau of Industry and Security issued proposed regulations to implement the 2013 additions to the Wassenaar Arrangement. The proposed rule was followed by a period

133 Heejin Kim (note 16).
134 See Export Administration Regulations (EAR), 15 CFR.

for public comments. The Bureau also published an extensive list of frequently asked questions (FAQs) that was meant to supplement the proposed rule and clarify how the controls apply. During and after the comment period, a broad coalition of stakeholders voiced substantial criticism, including human rights organizations that had advocated for the imposition of export controls in Wassenaar. Whereas the provisions regarding IP surveillance systems did not seem problematic, the proposed rules regarding intrusion software proved extremely controversial.

Criticism of the proposed rule was mainly based on its perceived detrimental effect on cybersecurity business and research. While controls on items related to intrusion software were aimed at tools used in connection with human rights violations, many argued that they could unintentionally undermine everyday activities involved in the defense of networks and devices, such as penetration testing or vulnerability disclosure. As Katie Moussouris explained,

> "[f]or human rights advocates, software . . . that bypasses security protections, hides from anti-virus and other malware detection tools, and spies on the victim, represent a threat to human life when used by repressive regimes. But for security researchers, the same offense techniques that are developed to bypass existing computer security measures are used in research to highlight weaknesses in order to fix the vulnerable software." [135]

Critics thus argued that the proposed rule would unduly affect cybersecurity researchers and companies, thereby undermining the cybersecurity of digital networks broadly. As individual researchers, small companies, and even large vendors would be affected, "the entire Internet ecosystem and everyone who uses technology will suffer the chilling effect on research and advances in defense."[136] These concerns illustrate the essence of the dual-use problem and the difficulty in avoiding unintentional consequences of regulations.

More specific criticism was pointed at the proposed US implementation rule, the original Wassenaar provisions, and the implementation challenges for companies. First, researchers, industry, and civil society organizations argued that the rule proposed by the US in 2015 was even broader than the 2013 Wassenaar language relating to intrusion software, thus capturing a range of cybersecurity items, including "many of the common and perfectly legitimate

135 Katie Moussouris, "You Need To Speak Up For Internet Security. Right Now," *Wired*, 16 July 2015, available at https://www.wired.com/2015/07/moussouris-wassenaar-open-comment-period/. See also Kim Zetter, "Why An Arms Control Pact Has Security Experts Up In Arms," *Wired*, 24 June 2015, available at https://www.wired.com/2015/06/arms-control-pact-security-experts-arms/.
136 Katie Moussouris (note 135).

tools used in security research," such as network penetration testing products.[137] A particularly controversial issue was the potential inclusion of research involving vulnerabilities and exploits. The proposed language stated that "[t]echnology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices."[138] This created considerable confusion and anxiety over the status of vulnerability research and disclosure.[139] Overall, the implementation proposed by the Department of Commerce was seen as an "unworkably-broad set of controls" that are not "required by Wassenaar, nor are they included in other Wassenaar implementations."[140] Moreover, even if certain activities were excluded by the proposed rule, information sharing and collaboration in the cybersecurity sector might still be negatively impacted.[141] Companies and individual researchers would be incentivized not to share information "even if permitted by the proposed rules, due to the difficulty in understanding their restrictions."[142]

Second, industry representatives and researchers argued that even the more restrictive language of the 2013 Wassenaar provisions would capture a number of important cybersecurity products. Companies such as Symantec and FireEye asserted that legitimate security products, such as endpoint security systems, could be captured by the controls, rendering security research and information sharing overall much more difficult.[143]

Third, critics argued that the implementation efforts and costs associated with national export controls would negatively impact cybersecurity activities. Commentators argued that legitimate tech companies would be put out of business "due to excessive license application burdens and delays in the ability to sell security products and compete globally."[144] Even large corporations warned that the proposed US rule would create a "significant regulatory burden" that would drive up prices and increase time to market.[145] Equally challenging, companies pointed out that restricting information sharing between individuals based on US and non-US citizenship

137 Nate Cardozo and Eva Galperin, "What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?" *Electronic Frontier Foundation*, 28 May 2015, available at https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation.

138 Proposed language quoted in Nate Cardozo and Eva Galperin (note 137).

139 Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," *Lawfare*, 5 January 2018, available at https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.

140 Nate Cardozo and Eva Galperin (note 137).

141 Internet Association, *Internet Association Comments on BIS Implementation of the Wassenaar Arrangement 2013 Plenary Agreements on Intrusion and Surveillance Items*, July 2015, available at http://internetassociation.org/wp-content/uploads/2015/07/Internet-Association-Comments-on-BIS-Implementation-of-Wassenaar-7.20.15.pdf.

142 Ibid.

143 Garrett Hinck (note 139).

144 Katie Moussouris (note 135).

145 Internet Association (note 141).

appears increasingly unworkable in a globalized world where company teams are multinational and operate across international borders.[146] Lastly, individual security researchers would be even more affected by the complexity of regulatory hurdles.[147]

In the end, the proposed rule was retracted and never went into effect. Following the plethora of comments submitted to the Commerce Department, as well as significant pressure from lawmakers, the Secretary of Commerce announced in March 2016 that the US would seek to re-negotiate the original Wassenaar language regarding the development of intrusion software.[148] These efforts resulted in the changes of 2016 and 2017 described above that carved out exemptions for vulnerability disclosure and cyber incident response activities. These changes were, for the most part, welcomed by industry and security researchers, though representatives voiced their hopes that the controls related to intrusion software would be narrowed down even further.[149]

Even though US efforts seeking to amend the language of the 2013 Wassenaar controls had been successful, the US government did not move ahead with implementation for several years. Not until 2021 did the Bureau of Industry and Security issue a new rule that introduced export restrictions on surveillance and intrusion items, finally aligning the US with the EU and other Wassenaar members that had already implemented the relevant controls.[150]

An Interim Final Rule introducing restrictions on certain "cybersecurity items" was issued in October 2021 and went into effect on March 7, 2022.[151] US government officials stated that the restrictions were meant to "deter the spread of certain technologies that can be used for malicious activities that threaten cybersecurity and human rights" and that the rule represented

146 Ibid.

147 Ibid.

148 Department of Commerce, *Letter from Secretary Pritzker to Several Associations on the Implementation of the Wassenaar Arrangement 'Intrusion Software' and Surveillance Technology Provisions*, 1 March 2016, available at https://bis.doc.gov/index.php/forms-documents/about-bis/newsroom/1434-letter-from-secretary-pritzker-to-several-associations-on-the-implementation-of-the-wassenaar-arrang/file.

149 Shaun Waterman, "The Wassenaar Arrangement's latest language is making security researchers very happy," *CyberScoop*, 20 December 2017, available at https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/.

150 Ellen Nakashima, "Commerce Department announces new rule aimed at stemming sale of hacking tools to Russia and China," *The Washington Post*, 20 October 2021, available at https://www.washingtonpost.com/national-security/commerce-department-announces-new-rule-aimed-at-stemming-sale-of-hacking-tools-to-repressive-governments/2021/10/20/ecb56428-311b-11ec-93e2-dba2c2c11851_story.html.

151 See Department of Commerce, *Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and other Malicious Cyber Activities*, Press Release, 20 October 2021, available at https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private. The Rule was set to go into effect on 19 January 2022, but implementation was later moved to 7 March 2022 to allow companies more time to adjust their compliance procedures accordingly.

"an appropriately tailored approach that protects America's national security against malicious cyber actors while ensuring legitimate cybersecurity activities."[152] The US implementation of 2022 sought to take account of the cybersecurity concerns that had derailed the 2015 implementation attempt, while addressing the spread of surveillance and intrusion tools that enable human rights abuses.

Arguably, the additions to the Commerce Control List were narrowly drawn and combined with a newly created license exception to minimize the controls' impact on cybersecurity activities.[153] Export controls were imposed on IP network surveillance systems as well as items related to intrusion software, and incorporated relevant Wassenaar exemptions for vulnerability disclosure and cybersecurity incident response activities.[154] A new License Exception Authorized Cybersecurity Exports (ACE) was introduced that allows for the export, re-export, and transfer (in-country) of "cybersecurity items" to most destinations.[155] Export licensing requirements remain for nearly 40 countries, including Russia and China, that are of national security or weapons of mass destruction concern. Exports to government and non-government end-users in these countries are subject to complex limitations, essentially restricting exports to "problematic countries."[156] Human rights concerns were reflected in a new "catch-all" restriction that was added for exporters with knowledge or "reason to know" that cybersecurity items will be used for certain malicious activities without the authorization of the owner, operator, or administrator of an information system.[157]

The 2022 implementation of Wassenaar controls concluded almost a decade of controversy and hesitancy in US export control policy relating to commercial spyware technologies. Coupled with other developments, the long overdue implementation has also suggested that the US was beginning to place greater emphasis on the issue of surveillance and intrusion tools and their potential misuse in the early 2020s. At the US-initiated Summit for Democracy in December 2021, the US, Australia, Denmark, and Norway announced an "Export Controls and

152 Ibid.

153 The text of changes to the Commerce Control List can be found in Rules and Regulations, Federal Register, Vol. 86, No. 201, 21 October 2021, available at https://www.govinfo.gov/content/pkg/FR-2021-10-21/pdf/2021-22774.pdf. For a good summary overview, see Melissa Duffy et al., *Being a White-Hat Hacker Just Got Tougher: US Commerce Department Issues New Cybersecurity Export Controls on Intrusion and Surveillance Tools*, Fenwick Insights blogpost, 21 October 2021, available at https://www.fenwick.com/insights/publications/being-a-white-hat-hacker-just-got-tougher-u-s-commerce-department-issues-new-cybersecurity-export-controls-on-intrusion-and-surveillance-tools.

154 Melissa Duffy (note 153).

155 Ibid.

156 Senior government official quoted in Ellen Nakashima (note 150).

157 Melissa Duffy (note 153).

Human Rights Initiative."[158] The initiative, also supported by Canada, France, the Netherlands, and the UK, is meant to "stem the tide of authoritarian government misuse of technology."[159] In March 2023, the initiative produced a "Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights" (ECHRI Code of Conduct).[160] The ECHRI Code of Conduct is a voluntary document outlining political commitments to apply human rights criteria to export control policies and practices.[161] Although the Export Controls and Human Rights Initiative is separate from, and does not operate through, the Wassenaar Arrangement, it nevertheless reaffirms the use of export controls as an important mechanism to regulate and restrict cyber tools, and places human rights considerations at its center. It is explicitly designed to complement existing multilateral commitments.[162]

In addition, the US enacted a number of policy changes in the early 2020s that signaled that, after a phase of stagnation, the US was engaged again on issues related to commercial spyware technologies, and was seeking to lead international policy efforts to address their proliferation. These included sanctioning of spyware companies by the US Department of Treasury Office of Foreign Assets Control,[163] visa restrictions for individuals involved in the development and sale of commercial spyware,[164] and, most notably, an Executive Order that prohibited the US government from "operational use of commercial spyware that poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person."[165]

Going beyond the Wassenaar additions and their implementation in the US, broader developments in the US export control regime could impact the regulation of commercial spyware

158 Governments of Australia, Denmark, Norway, and the United States, *Joint Statement on the Export Controls and Human Rights Initiative*, Statement, 10 December 2021, available at https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/12/10/joint-statement-on-the-export-controls-and-human-rights-initiative/.

159 The White House, *Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy*, Statement, 10 December 2021, available at https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/.

160 Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights, text available at https://www.dwt.com/-/media/files/blogs/broadband-advisor/2023/06/230303updatedechricodeofconductfinal.pdf?rev=284458e5b00e497a9ed195723e79332a&hash=995310840249E0CC880AA8DB4545B80E.

161 Ibid.

162 Ibid.

163 Brian Fung, "Biden administration sanctions makers of commercial spyware used to surveil US," *CNN*, 5 March 2024, available at https://www.cnn.com/2024/03/05/business/biden-administration-sanction-commercial-spyware/index.html.

164 Stephanie Kirchgaessner, "US announces new restrictions to curb global spyware industry," *The Guardian*, 5 February 2024, available at https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions.

165 Executive Order 14093, Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security, 27 March 2023, available at https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to.

technologies in the future. Similar to the European Union, the US export control regime has been undergoing a review and reform process since 2009.[166] However, in contrast to the human rights-oriented debate in the EU, US efforts have been marked by the increasing geopolitical competition between the US and China.

In 2018, Congress enacted the US Export Control Reform Act (ECRA), which, among other policies, creates controls on a new category of "emerging and foundational technologies."[167] Because the ECRA was passed during a time of increasing confrontation between the US and China over commercial and technological dominance in the ICT sector,[168] observers have remarked that the ECRA was "clearly adopted in a context where the US is seeking to prevent a group of specific Chinese firms from acquiring certain types of vital technologies originating from US citizens and companies."[169] US export controls are thus used as a "protectionist tool to reinvigorate domestic industry concerning 'emerging and foundational technologies' and to guard its dominance against growing foreign actors in the global technology market."[170]

Be that as it may, the ECRA and its regulation of "emerging and foundational technologies" could enable the US to control commercial spyware technologies beyond those that have been added to the Wassenaar Arrangement's Dual-Use List. As a result, the US government could unilaterally add restrictions for spyware tools, driven presumably by concerns over economic and technological competition from China. This stands in contrast to the human rights motivation espoused in the reform efforts of the EU export control regime. It remains to be seen how the scope of "emerging and foundational technologies" will be defined in detail, and whether additional surveillance and/or intrusion tools will become subject to the controls of the ECRA. Similarly, it remains open whether (and to what extent) these export control reforms, as well as other initiatives regarding commercial spyware, will be continued by subsequent administrations.

• • •

Following the additions of certain commercial spyware technologies within the Wassenaar Arrangement, the controls have to be implemented on a national basis. An analysis of imple-

166 See, for example, Congressional Research Service, The U.S. Export Control System and the Export Control Reform Initiative, Report, 5 April 2019.

167 The US Export Control Reform Act (ECRA) of 2018 was passed by the US Congress as part of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA). The text is available at https://www.congress.gov/bill/115th-congress/house-bill/5040/text.

168 Heejin Kim (note 16).

169 Ibid.

170 Ibid.

mentation efforts among the Arrangement's major members — the United States and the European Union — reveals partly diverging, partly converging trends.

In the US, implementation has been fraught with difficulties and delays. The first implementation attempt in the US was highly controversial, resulting in the US government seeking amendments in 2016 and 2017. Specifically, industry representatives and the research community argued that the controls on intrusion software had considerable unintended consequences impacting essential cybersecurity practices. These difficulties had a lasting impact: only after a considerable delay (and following a change in administration) were the Wassenaar additions of 2013 (and, as amended, 2016 and 2017) finally transposed into US export control regulations in 2021.

In contrast, the European Union moved to implement the 2013 changes relatively quickly. Individual member states even added further commercial spyware technologies to national control lists.[171] Attention thus shifted to questions of uniformity and consistency in the national application of controls, and an expansion of controls as part of efforts to reform the EU export control regime.

As a result of these developments, a gap emerged in the implementation of the 2013 Wassenaar controls on commercial spyware, limiting or delaying the potential impact of Wassenaar's provisions for several years. In a way, the implementation experiences in the EU and the US reflected their domestic situations. Whereas the EU had a large base of companies providing surveillance technologies and was keen to address the related human rights abuses that had been revealed, the US was home to a large cybersecurity community and industry that saw itself as unduly affected by the regulations. On the other hand, the EU's cybersecurity industry is smaller, while the number of US companies selling surveillance and intrusion technologies is limited. Even in light of these differences, the hesitancy of the US in implementing the controls on surveillance and intrusion tools called into question the use of export controls as a mechanism for addressing the proliferation of commercial spyware — and the significance of human rights considerations. The EU, on the other hand, actively sought to expand controls on surveillance technologies, and the role of human rights considerations in the export control process, with ambitious proposals for the recast of the Dual-Use Regulation. US efforts in this

171 For example, in 2015 Germany added monitoring centers and data retention systems to its control lists, citing Article 8 of the EU Dual-Use Regulation, which enables member states to pass controls on non-listed items for reasons of public security or human rights. See Bundesministerium für Wirtschaft und Energie, *Gabriel: Export von Überwachungstechnik wird stärker kontrolliert*, 8 July 2015, available at https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2015/20150708-gabriel-export-von-ueberwachungstechnik-wird-staerker-kontrolliert.html.

respect were halted for a considerable time. The result was a divergence of regulatory regimes regarding certain commercial spyware technologies.

This trend seems to have stopped with the belated implementation of controls in the US in 2022. With numerous policy measures emerging in the US, including the Human Rights and Export Control Initiative, positions on both sides of the Atlantic have even shown signs of convergence. While EU export control policy is still decidedly oriented toward human rights, the recast Dual-Use Regulation does not go as far as initial proposals indicated with regard to the regulation of surveillance technologies and the role of human rights. Meanwhile, the US has embraced these issues again, placing stronger emphasis on human rights concerns and even seeking a leadership role by spearheading new initiatives. It remains to be seen how far this convergence will go, in light of changing US administrations and broader US export control reforms that are characterized by the US-China relationship.

The degree of convergence between the EU and US approaches will undoubtedly affect prospects for further controls with the Wassenaar framework. The uneven implementation of the 2013 controls, different priorities in the respective export control reforms, and outside initiatives question the role of the Wassenaar Arrangement as the primary forum for further action relating to the regulation of commercial spyware technologies.

PART IV
Regulating Commercial Spyware
Other International Efforts

States' efforts in the Wassenaar Arrangement stand out as a first multilateral attempt to regulate commercial spyware technologies, albeit with a focus on a limited set of surveillance and intrusion tools. While export controls had dominated the international regulatory debate for several years, other international efforts also merit discussion. In particular, recent initiatives led by governments and non-governmental stakeholders, as well as developments in the United Nations (UN), offer promising avenues for the future multilateral regulation of commercial spyware.

8. MORATORIUMS AND BANS

Both governmental and non-governmental stakeholders have called for moratoriums on commercial spyware technologies, which would institute a temporary ban on the development, export, and/or use of these technologies.[172] This would give the international community time to negotiate international regulatory frameworks and norms while seeking to limit the misuse of commercial spyware technologies that have already entered the market.[173] Going beyond a temporary stop, an international ban would permanently restrict the development, export, and/or use of commercial spyware by states and companies.[174]

In August 2021, UN human rights experts, including the Special Rapporteur on the promotion and protection of the right to freedom of expression, called on states to impose an international moratorium on the sale and transfer of "life threatening" surveillance technologies until international regulations that guarantee compliance with international human rights law are established.[175] Similarly, dozens of civil society organizations and experts published a joint open

172 Freedman Consulting, LL, *Spyware Accountability Mechanisms Framework: A Guide to Support Discussions Around Spyware Accountability*, Report, September 2023, available at https://tfreedmanconsulting.com/resources/spyware-accountability-mechanisms-framework/.

173 Ibid.

174 Ibid.

175 United Nations Office of the High Commissioner for Human Rights, "Spyware scandal: UN experts call for moratorium on sale for 'life threatening' surveillance tech," press release, 12 August 2021, available at https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

letter in 2021 calling on states "to implement an immediate moratorium on the sale, transfer and use of surveillance technology."[176] A joint statement issued by civil society actors in 2023 condemned the use of spyware against journalists and media workers, and likewise called for an "immediate moratorium" on surveillance technologies as well as "a ban on abusive commercial spyware technology and its vendors."[177] Among governments, in 2022, Costa Rica became the first state to publicly call for an "immediate moratorium on the use of spyware technology until a regulatory framework that protects human rights is implemented."[178]

Despite this multitude of statements from various stakeholders, an international moratorium, let alone a permanent ban, has neither materialized nor gained significant support from a majority of states. The rapid proliferation of commercial spyware, particularly over the past few years, coupled with the legitimate use of these technologies by governments, may make international moratoriums or bans increasingly unlikely.

9. PALL MALL PROCESS

On 6–7 February 2024, the governments of the United Kingdom and France jointly organized a conference in London centered on "tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities."[179] This event kicked off the so-called Pall Mall Process, a global process to design a multistakeholder response to the proliferation and irresponsible use of commercial cyber intrusion capabilities. A follow-up conference in France is planned for April 2025 as a next step in the Process.[180]

176 Amnesty International, Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology, 27 July 2021, available at https://www.amnesty.org/en/documents/doc10/4516/2021/en/.

177 Access Now, Joint statement: States must take immediate action to stop spyware threatening press freedom, 3 May 2023, available at https://www.accessnow.org/press-release/spyware-press-freedom-statement/.

178 Access Now, Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology, 13 April 2022, available at https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/.

179 For overview commentary, see Sven Herpig and Alexandra Paulus, "The Pall Mall Process on Cyber Intrusion Capabilities," *Lawfare*, 19 March 2024, available at https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities, and Fionnuala Ní Aoláin and Adriana Edmeades Jones, "Seizing the Moment: Opportunities to Regulate Spyware and the 'Pall Mall Process,'" *Just Security*, 29 October 2024, available at https://www.justsecurity.org/104363/spyware-pall-mall-opportunities/.

180 French Ministry of Foreign Affairs, "Cybersecurity — Meeting of the Pall Mall Process to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities," news release, 12 November 2024, available at https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/cybersecurity-meeting-of-the-pall-mall-process-to-tackle-the-proliferation-and.

The London conference, which was attended by a range of government representatives and non-governmental stakeholders,[181] represents the most significant development in the international governance debate in recent years. While it remains to be seen what, if any, concrete results the Pall Mall Process can yield, the high-level political attention and support provided by the governments of the UK and France have created newfound momentum to move international regulatory debates significantly forward. Whether this potential will be realized in coming years remains an open question.

The London conference produced a declaration that was signed by both government and non-governmental stakeholders, outlining key policy issues and setting our four "pillars," principles to frame international action to regulate commercial cyber intrusion capabilities. The four pillars are (1) accountability, (2) precision, (3) oversight, and (4) transparency.[182] According to the Pall Mall declaration, the first pillar, accountability, provides that activities should be legal and responsible, in line with the framework for responsible state behavior in cyberspace, existing international law, and domestic frameworks. States as well as non-state actors should be held accountable for activities that are inconsistent with international human rights law.[183] The second pillar states that capabilities should be developed and used with precision in order to avoid unintended, illegal, or irresponsible consequences.[184] Pillar three, oversight, establishes that assessment and due diligence mechanisms should be in place for both users and vendors to ensure that activities are legal and responsible.[185] Finally, pillar four calls for transparency in business interactions so that vendors and users understand their supply chains and are able to build trust and confidence in responsible business practices.[186]

Aside from setting out these four pillars for multi-stakeholder cooperation, the London conference left open questions about the overall governance outcome of the Pall Mall Process. The declaration merely stated that the signatories "resolve to explore the parameters of both legitimate and responsible use, by State, civil society, legitimate cyber security, and industry actors alike."[187] The initiators of the Process did not advocate a specific regulatory tool or instrument

181 Alexander Martin, "Britain and France assemble diplomats for international agreement on spyware," *The Record*, 5 February 2024, available at https://therecord.media/britain-france-assemble-diplomats-international-agreement.

182 The Declaration is contained in UK Government, The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities, 6 February 2024, available at https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

183 Ibid.

184 Ibid.

185 Ibid.

186 Ibid.

187 Ibid.

to govern the development, sale, transfer, and use of commercial cyber intrusion capabilities. They did, however, introduce the concept of "responsible" use to the international debate around the governance of commercial spyware technologies. The prospects as well as contents of this concept as a potential tool for the international regulation of commercial spyware have yet to be explored.

It is important to note that the focus of the Pall Mall Process on commercial cyber intrusion capabilities goes beyond commercial spyware technologies, and includes hacker-for-hire services as well as vulnerability and exploit marketplaces.[188] With this broad approach in mind, the initiators of the Pall Mall Process point to the growing commercial market for cyber intrusion capabilities and its negative impacts on human rights, cyber stability, national security, and digital security at large.[189] While the Pall Mall declaration acknowledges that "many of these tools and services can be used for legitimate purposes,"[190] it recognizes human rights concerns alongside national security and cybersecurity concerns. In this way, the Pall Mall Process incorporates the different concerns that have surfaced during the conception and implementation of the Wassenaar export controls. Interestingly, the Wassenaar Arrangement and its controls are not directly referenced, with the declaration merely noting "efforts made via existing international export control frameworks."[191]

10. EFFORTS IN THE UNITED NATIONS

For most of the 2010s, governance debates around commercial spyware revolved around export controls without any significant involvement from the United Nations system. Only in recent years have various UN bodies begun to discuss commercial spyware technologies, their impact, as well as potential avenues for regulation.

188 Program of the Pall Mall Conference, London, 6 February 2024, on file with author. See also Annex of Working Definitions contained in UK Government, The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities, 6 February 2024, available at https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

189 Declaration in UK Government, The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities, 6 February 2024, available at https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

190 Ibid.

191 Ibid.

In 2021, the issue of commercial spyware surfaced in the UN Working Group on the use of mercenaries as part of a broader examination of the use of mercenaries and private military and security companies in cyberspace.[192] Among other topics, the report covered the work of private companies that offer services related to data collection, intelligence, and surveillance.[193] The Working Group focused on entities that offer certain services or supply certain products in cyberspace, i.e., non-governmental actors, rather than on specific cyber tools. In other words, they approached the regulation of commercial spyware technologies by focusing on actors involved in their development, provision, and operation.

The Working Group on the use of mercenaries (formally the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination) is a group of independent experts nested under the Human Rights Council.[194] Along with Special Rapporteurs, Working Groups are a part of the Human Rights Council's so-called Special Procedures, a system of independent fact-finding and monitoring mechanisms.[195] Established in 2005,[196] the Working Group issues annual thematic reports and presents them to the Human Rights Council and the General Assembly.[197] The Group's report in 2021 was dedicated to the provision of military and security products and services in cyberspace by "cyber mercenaries."[198] It was the first time the Working Group examined mercenary-related activities involving cyberspace.

In its report, the Working Group pointed to the growing range of "cyberservices" being offered by private actors and their impact on a range of human rights both in peacetime and during armed conflicts.[199] They noted that a wide range of non-governmental actors provide diverse products and services, including entities that offer commercial spyware capabilities.[200] In response to these developments, the Working Group issued a number of recommendations to states.

192 Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, A/76/151, available at https://digitallibrary.un.org/record/3936236/files/A_76_151-EN.pdf.
193 Ibid.
194 See the website of Working Group on the use of mercenaries, available at https://www.ohchr.org/en/special-procedures/wg-mercenaries.
195 See the website of Special Procedures of the Human Rights Council, available at https://www.ohchr.org/en/special-procedures-human-rights-council.
196 Website of Working Group (note 194).
197 Ibid.
198 Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, A/76/151, available at https://digitallibrary.un.org/record/3936236/files/A_76_151-EN.pdf.
199 Ibid.
200 Ibid.

Among other suggestions, the Group called on states to initiate an international dialogue on new and evolving forms of mercenaries, particularly those operating in cyberspace, as well as on their risks to international humanitarian and human rights laws — and effective ways to counter these risks.[201] As part of this, the Group referred the issue to the UN General Assembly's cybersecurity discussions and suggested that the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) address the "human rights concerns arising from the involvement of mercenaries and related actors in cyberoperations."[202] It is important to note that the Working Group referred to the question of "human rights concerns," as opposed to international security or cybersecurity considerations.

The Open-Ended Working Group (OEWG), on the other hand, had not discussed commercial spyware technologies. Its mandate has focused on developing an international framework to govern states' activities in cyberspace — the so-called framework for responsible state behavior in cyberspace.[203] As a part of the First Committee of the UN General Assembly, which is tasked with issues of international security and disarmament, discussions in the OEWG have focused on stability and security in cyberspace.[204]

While the regulation of commercial spyware had not been explicitly or directly dealt with in the OEWG, the framework for responsible state behavior in cyberspace, which outlines norms of behavior and international law obligations for states, is arguably still relevant. It sets standards of expected behavior for states — in other words, what states should or should not be allowed or expected to do. More specifically, the framework contains 11 voluntary, non-binding norms of responsible state behavior that have subsequently been endorsed by consensus by the UN General Assembly.[205] The use of commercial spyware technologies by states would arguably have to be consistent with these norms of behavior and international law obligations.[206]

In this context, several norms are relevant for the governance of commercial spyware tools. Norm (i) provides that states should seek to prevent the proliferation of malicious ICT tools

201 Ibid.

202 Ibid. While the Group of Governmental Experts had already concluded their work by the time the Working Group on the use of mercenaries issued their report, the Open-ended Working Group of 2021–2025 is free to consider this issue.

203 UN General Assembly Resolution A/RES/75/240, available at https://docs.un.org/en/A/RES/75/240.

204 For an introductory overview, see the website of the UN Office of Disarmament Affairs, available at https://disarmament.unoda.org/ict-security/.

205 See, for instance, provisions in the 2014/2015 GGE report, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, available at https://docs.un.org/en/A/70/174.

206 While the 2012-2013 Group of Governmental Experts acknowledged the applicability of international law — specifically the UN Charter — to activities in cyberspace, controversies persist with regard to certain areas such as international humanitarian law.

and techniques, and the use of harmful hidden functions.[207] In line with norm (j), states should encourage responsible reporting of ICT vulnerabilities.[208] Norm (e) highlights states' human rights obligations in their use of technologies.[209] Lastly, norm (a) stipulates broadly that states should prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.[210]

However, it currently remains unclear exactly how these norms would apply in practice to the development, sale, transfer, or use of commercial spyware capabilities by national governments. The Declaration of the Pall Mall conference, for instance, highlighted the relevance of the framework for responsible state behavior but did not provide any further detail on this question.[211] Discussions in the OEWG also have not addressed the application of the framework of responsible state behavior to the development and use of commercial spyware technologies.

Thus far, the issues of commercial spyware and its regulation have not been comprehensively addressed in OEWG discussions. A growing number of states have highlighted the increasing proliferation and use of commercial spyware capabilities as an emerging threat to security and stability in cyberspace.[212] Beyond these concerns, states have not discussed any regulatory framework for commercial spyware technologies or clarify how the norms of responsible state behavior specifically regulate commercial spyware. The current OEWG has been authorized by the General Assembly until 2025, and while possible follow-on mechanisms are currently under discussion, the time window is rapidly closing for the OEWG to pick up the recommendation from the Working Group on the use of mercenaries.

• • •

Following the experience with Wassenaar export controls, recent initiatives led by governments and non-governmental stakeholders indicate a renewed and broadened interest in curbing the

207 See, for instance, provisions in Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, available at https://docs.un.org/en/A/70/174.

208 Ibid. Relatedly, the same report proposes that "[s]tates should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate threats to ICTs and ICT-dependent infrastructure."

209 Ibid.

210 Ibid.

211 See the Declaration contained in UK Government, The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities, 6 February 2024, available at https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

212 See, for instance, Third Annual Progress Report, Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, A/79/214, available at https://docs.un.org/en/A/79/214.

proliferation and misuse of commercial spyware technologies. Civil society organizations have repeatedly called for a moratorium on commercial spyware. Significant political capital was invested by the governments of France and the UK to launch the Pall Mall Process, the first broad and collaborative process seeking to regulate commercial spyware internationally. Finally, several UN entities have taken on the issue of spyware, in accordance with their mandates and institutional perspectives.

Taken together, these developments offer promising avenues for the future regulation of commercial spyware. While it remains to be seen how these discussions will evolve and what concrete substantive outcomes they can yield, taken together, they nonetheless promise to take international regulatory debates forward and to broaden them beyond the use of export controls.

However, with an increasing number of entities and processes involved in various regulatory efforts, the risk of fragmentation arises, along with the risk of competing and potentially incompatible regulatory regimes. This risk arises both with regard to the interaction of recent initiatives outlined above, as well as with the interplay of those initiatives with the export control efforts already undertaken in the Wassenaar Arrangement (and beyond).

PART V
Lessons Learned

The experience of Wassenaar export controls offers valuable insights for states' national and international efforts to regulate commercial spyware technologies. The following observations seek to highlight three lessons learned that are based on the comparative analysis of the implementation of Wassenaar controls in the US and the EU: (1) new equities and considerations have emerged and need to be addressed by export control regimes and other regulatory efforts, (2) Wassenaar export controls have proved to be a contentious tool, and (3) Wassenaar export controls and their effectiveness are inherently limited. Collectively, these observations help assess the utility of export controls, and in particular the Wassenaar Arrangement, as a multilateral tool to regulate commercial spyware tools.

11. LESSON #1: EXPORT CONTROLS AND NEW EQUITIES

Traditionally, export control regimes have sought to reconcile two competing interests or equities: the economic benefit from the sale and international distribution of items, and the national or international security interest in restricting the spread of capabilities to certain actors. The experience of controlling certain commercial spyware technologies through export controls has complicated this balance by adding new equities that raise new questions.

The implementation efforts in the United States have shown the importance of cyber tools both for offensive and defensive purposes. According to industry representatives and security researchers, tools that are essential for defensive security cannot be separated from tools used in surveillance or intrusion tools through a precise and workable definition. Arguably, it is impossible to distinguish malicious and innocuous software on the basis of technical specifications.[213] Cyber tools may encapsulate the dual-use problem in its thorniest incarnation. More importantly, however, during the failed implementation attempt in the US, cybersecurity activities have entered the export control equation. In addition to affecting economic interests, the controls on intrusion software have illustrated the potential for unintended consequences that

213 Thomas Dullien, Vincenzo Iozzo, and Mara Tam, Surveillance, Software, Security, and Export Controls Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting, Draft Report WA-CAT4, 10 February 2015, available at https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file.

can affect legitimate third interests — in this case, efforts to secure and defend information and communication networks nationally and internationally.

The second equity that has rendered export control efforts more complex is the increasing relevance of human rights considerations. While human rights have played a role in export controls of conventional weapons, the situation is less clear with regard to the export of dual-use technologies.[214] In this regard, the 2013 additions to the Wassenaar Arrangement set "a precedent by introducing human rights considerations" into the Arrangement.[215] The European Union seems to actively embrace a more prominent role for human rights considerations in its export control framework, while the US's consideration of human rights is more recent. This indicates the emergence of a broader question about what role human rights concerns should play in the export control of dual-use items. Should international mechanisms designed to address international stability and security concerns be used to address human rights issues? While EU member states seem to answer in the affirmative, other countries may be more reluctant to use the particular instrument of export controls to do so.

12. LESSON #2: CONTROVERSY OVER WASSENAAR CONTROLS

In the context of the Wassenaar Arrangement, the 2013 introduction of controls that were (at least partly) aimed at addressing human rights concerns generated considerable controversy over the use of export controls to regulate commercial spyware dual-use items.

For some, the original 2013 changes to the Wassenaar Arrangement were seen as an overdue and appropriate policy tool to remediate human rights violations that had been uncovered in the aftermath of the Arab Spring (and even before). Since the spyware tools in question were accessible and traded on open markets, the imposition of licensing requirements through export controls represented a natural policy response to regulate transfers. Human rights campaigns had advocated such an approach, which was ultimately reflected in proposals to Wassenaar made by France and the United Kingdom. Because many European companies were exposed to have provided commercial spyware to repressive regimes during the Arab Spring, the EU embraced the Wassenaar export controls approach and sought to go even further during its export regime reform efforts.

214 Mark Bromley (note 24).
215 Fabian Bohnenberger (note 88).

On the other hand, following the failed implementation in the United States in 2015 and early 2016, the rationale for export controls was brought into question, particularly by private-sector entities and the cybersecurity research community, which took issue with the use of export controls to regulate even a subset of commercial spyware tools. The impressively influential response by these groups, which ultimately led to a change of policy by the US government and its subsequent efforts to amend the original 2013 Wassenaar language, had to some extent shifted the focus of the debate. At least in the US context, the original human rights concerns were muted for several years, compared to prominently voiced cybersecurity-related concerns. According to skeptics of the Wassenaar additions, export controls were ill-equipped to regulate intangible technology, particularly without impacting tools, activities, and processes related to cybersecurity defense. Only after a considerable delay was the US government ready to emphasize human rights considerations and to actively pursue export control regulations in this area.

Particularly in the US, the Wassenaar experience has shown that positions regarding the utility and effectiveness of export controls in regulating certain commercial spyware tools have been deeply divided. This included the controversy over the scope of existing provisions, but also extended to the more fundamental question of whether export controls would be an appropriate regulatory tool in the first place. Different positions resulted in significant controversy and an impasse in the debate for several years. As for the Wassenaar Arrangement, "[w]hile the updates to Wassenaar have been closely reflected in the equivalent mechanisms at national and regional levels, the addition of cyber surveillance technology has changed this narrative of broad acceptance and impact."[216]

As a result, the controversy over Wassenaar export controls on certain commercial spyware tools has had a lasting effect on the Wassenaar Arrangement and its members, questioning the utility of export controls, and impacting international progress on the issue.

13. LESSON #3: INHERENT LIMITATIONS TO WASSENAAR CONTROLS

Despite the controversy over the Wassenaar controls, their implementation thus far offers important insights into the effectiveness of the additions. This enables the identification of important limitations to the regulation of commercial spyware through export controls. If the Wassenaar additions were a necessary first step in addressing the misuse of commercial

216 Heejin Kim (note 16).

spyware, these limitations indicate gaps for further action. Many of the limitations are not necessarily specific to the nature of commercial spyware but are limits of the Wassenaar regime more generally.

First, the membership of the Wassenaar Arrangement provides a natural limit for the regulatory reach of the Arrangement. As discussed in Part II, membership in Wassenaar is limited to select nations; although it includes most major industrialized countries, the controls on commercial spyware do not cover all countries with relevant industry. Israel is a notable example in this regard; it has a vibrant tech sector and is not a member of the Wassenaar Arrangement. Although Israel generally has adopted controls similar to those of Wassenaar through domestic legislation, the controls on intrusion software are less stringent than those agreed to in Wassenaar in 2013.[217] By definition, export controls adopted by members of the Wassenaar Arrangement do not extend to non-members. If these non-members are home to a significant industry for controlled items, potential buyers can easily circumvent the export licensing requirements of Wassenaar member states. Similarly, companies that become subject to export control regulations in Wassenaar states can simply decide to move offices and operations elsewhere.[218] Thus, the effect of controls adopted within Wassenaar is limited if significant industry actors are distributed across states that do not participate in the Wassenaar Arrangement and do not voluntarily follow its policies.

Second, as described in Part III, the implementation of Wassenaar controls is left to individual participating states. Items that have been agreed to within the framework of the Arrangement need to be incorporated into export control lists on a national level. States are reserved a large measure of discretion in this regard. This discretion applies to crafting the scope of national controls (as either narrower or broader than the Wassenaar controls), as well as to the application and enforcement of national regulations once adopted. Thus, the effectiveness of Wassenaar controls ultimately depends upon the uniformity of national implementations. However, the survey of the Wassenaar experience has revealed an uneven implementation across its membership. On the one end, the European Union moved to implement the 2013 additions fairly quickly, while some EU states chose to adopt even more stringent controls. On the other end, the United States delayed its implementation of the Wassenaar regulations concerning commercial spyware, even after the changes of 2016 and 2017. Further, the application of controls — even among EU member states that have implemented the additions — can differ. For example, as described in Part III, the governments of Germany and Italy required different types of licenses — individual versus global — for the export of similar items. A system-

217 Garrett Hinck (note 139).

218 Jen Roberts et al. refer to this as "jurisdictional arbitrage". See Jen Roberts et al. (note 7).

atic assessment of national practices and licensing decisions is needed to identify differences that further limit the effectiveness of Wassenaar controls. This, in turn, requires relevant data to be collected, collated, and made accessible.

Concluding Thoughts

The international market for commercial spyware technologies has gained considerable notoriety in the past 15 years. Coordinated and sustained civil society campaigns have highlighted the detrimental human rights effects and have called for international regulatory action. States' responses have centered around the inclusion of certain commercial spyware technologies, namely IP surveillance systems and intrusion software, in the Wassenaar Arrangement export controls. However, this approach has not been without contention, resulting in the "most controversial addition to [the Wassenaar dual-use] list since its adoption in 1996."[219] In the US in particular, implementation efforts have led to serious questioning about the utility of export controls for the regulation of commercial spyware. In addition to human rights concerns, which motivated the additions in the first place, unintended consequences affecting cybersecurity researchers and practitioners have been flagged, complicating the picture of export control considerations.

However, despite the controversy, the Wassenaar Arrangement still represents the most concrete attempt at regulating commercial spyware to date. Even after a considerable period of inactivity, both the EU and the US (finally) implemented the 2013 changes. And both seem to have embraced a stronger focus on human rights considerations in their export control regimes, though to varying degrees. In the case of the EU, the recast Dual-Use Regulation is markedly human rights oriented, though not to the extent initially hoped for by human rights advocates. In the case of the US, human rights concerns were elevated in the early 2020s through a number of policy measures. It remains to be seen, however, what (if any) policy changes the second Trump administration will bring.

To move international regulation debates constructively and effectively forward, a look at past experiences in the Wassenaar Arrangement and the lessons learned is a crucial first step, not only for improving upon existing export controls but also for approaching and designing additional multilateral measures and frameworks to address the proliferation and misuse of commercial spyware. This paper identified three lessons from states' first multilateral attempt at regulating commercial spyware that capture important insights for future international regulation efforts.

219 Heejin Kim (note 16).

First, export control decisions have been compounded by the need to balance new and additional equities. The uneven implementation of the Wassenaar additions between the United States and the European Union points to the need for states to engage with human rights as well as cybersecurity consideration in the context of export controls, in addition to economic interests and national security and nonproliferation concerns. This multitude of considerations requires individual states to wrestle with their own prioritization of these equities in order to effectively engage in and shape international regulation efforts.

Second, it has become apparent that export controls come with imperfections and limits. This realization — and the identification of those limits — is crucial for improving existing controls and designing new ones. The implementation of the 2013 controls provides an opportunity to assess the efficacy of controls, but to conduct such an assessment, data regarding license applications, approvals, and denials needs to be systematically gathered, synthesized, and analyzed. The opaqueness of the commercial spyware market makes this point only more pressing.

Third, and lastly, recognizing and identifying the limits of export controls as a regulation mechanism opens the conversation for additional and alternative regulatory efforts. Given that the Wassenaar controls target only a very small subset of commercial spyware technologies, the use of export controls hardly constitutes a silver bullet to address the destabilizing effects stemming from the development and diffusion of commercial spyware. While Wassenaar controls and the controversy surrounding them had actively engaged stakeholders in this community, this has created a situation where alternative or complementary measures have not received any significant attention for many years. Shifting the international focus away from one regulatory effort, the Wassenaar controls, to a web of national and international measures to address commercial spyware promises to avoid some of the pitfalls that the contentious experience of Wassenaar controls has exposed.

It is noteworthy that recent initiatives, particularly the Pall Mall Process, explore a range of governmental, non-governmental, and international regulatory mechanisms. These developments indicate not only growing political momentum to tackle the question of commercial spyware and its international regulation, but also an openness to consider more than one mechanism. The outcomes of this and other processes, however, remain open, and a noteworthy ambiguity exists with regard to its purported outcome.

Acknowledgments

The author would like to thank the Swiss Federal Department of Foreign Affairs (FDFA) for financially supporting the research for this study.

The author would also like to thank Herb Lin for providing valuable feedback and comments, and Charles Kapelke for his diligent and patient editorial work.

All views expressed in this white paper are the author's, as are any remaining errors.

About the Author

ELAINE KORZAK is a research scholar at the Berkeley Risk and Security Lab focusing on international cybersecurity governance. She is a research affiliate at the Center for Long-Term Cybersecurity at UC Berkeley and an affiliate at the Center for International Security and Cooperation (CISAC) at Stanford University.

Her research covers international legal, policy, and governance aspects in cybersecurity, including norms and international law governing state conduct in cyberspace, cybersecurity negotiations at the United Nations, cyber policy positions and diplomatic strategies of states (in particular Russia and China), and international export controls for commercial spyware.

She holds a PhD in War Studies and an MA in International Peace and Security from King's College London, as well as an LL.M. in Public International Law from the London School of Economics and Political Science (LSE).


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley