The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls

FABIAN BOHNENBERGER[1]

Abstract

The global trade in cyber-surveillance technologies has largely evaded public scrutiny and remains poorly understood and regulated. European companies play a central role in the proliferation of a broad spectrum of advanced surveillance systems that have legitimate uses, but have also been repurposed for nefarious ends. Export controls have become an important instrument to restrict sales of cyber-surveillance equipment and software to repressive regimes; however, these technologies pose significant challenges to traditional frameworks for the control of dual-use exports. This article provides an overview of current developments on the European level and within the multilateral Wassenaar Arrangement and presents the current state of export controls on cyber-surveillance technology. Most importantly, it discusses the outcome of the European Union export control policy review, focusing on the regulation proposed by the European Commission in September 2016, and provides an initial assessment of the key innovations and limitations of the draft text. In addition, the article presents an analysis of the current debate regarding the problematic definition of "intrusion software" in the Wassenaar Arrangement and offers insights into some alternative proposals.

Keywords

ICT surveillance systems, export controls, Wassenaar Arrangement, human rights, European Union, EU Dual-use Regulation, policy review

1 Fabian Bohnenberger recently completed his Master of Public Policy at the Hertie School of Governance in Berlin. For his Master's thesis on export controls for cyber-surveillance technologies he received an 'Aquila ascendens' young academics award for security policy in April 2017. His research focuses on international trade relations, the application and effects of sanctions and export controls, and the democratic legitimation of transnational governance.

Introduction

Increasing exports of advanced surveillance capabilities have become a focus of controversy and debate on regulatory and legal controls that can be used to limit sales to governments with dubious human rights records. European companies play a central role in the proliferation of a broad spectrum of systems for targeted and mass surveillance that are used to observe and analyze behaviors and identities of people on computers, mobile phones, and telecommunications networks. These technologies have legitimate uses but have also been repurposed by some authorities to contribute to serious human rights abuses, the suppression of journalism and civil society, and the persecution of human rights defenders, dissidents, and political opponents.[2]

Export controls today represent an important instrument to restrict sales of cyber-surveillance equipment and software to repressive regimes; however, these technologies pose considerable challenges to traditional frameworks for the control of dual-use exports. Actors in the debate offer different conceptions of what technologies or services should be subject to export authorization requirements, why these items (and not others) should be controlled, and what an effective control regime would look like. On September 28, 2016, the European Commission introduced a proposal to update the European Union Dual-Use Regulation, which includes new provisions on the export of cyber-surveillance technologies.[3] The Commission's draft will be discussed and decided upon by the European Council and the European Parliament in the ordinary legislative procedure. The Committee for International Trade (INTA), which is responsible for drafting the Parliament's position, held an initial public hearing on the dual-use reform on March 21, 2017, but it is not yet known when the regulation, if adopted, is expected to enter into force.[4,5] Concurrently, however, existing provisions on cyber-surveillance technologies at the multilateral level have come under increasing criticism. Several members of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA), most notably the United States, are concerned about unintended capture and harmful effects on computer security research.

The next few months will see important developments in the area of export controls on cyber-surveillance technologies. By discussing the control challenge and summarizing the perceptions and proposals of different participants in the debate, this article hopes to inform the ongoing policy debates. It will provide an overview of current developments on the European level and within the WA and present the current state of export controls on cyber-surveillance technology

---

2 A recent report by Ecorys and the Stockholm International Peace Research Institute (SIPRI) collected information on over 80 cases where cyber surveillance systems exported from the EU have been connected with violations of human rights or threats to international or EU security. See: "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," Ecorys and SIPRI , 2015, <https://www.sipri.org/sites/default/files/final-report-eu-dualuse-review.pdf>.

3 EU 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, Brussels, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf>.

4 The INTA nominated MEP Klaus Buchner as Rapporteur. In parallel, the Committee on Foreign Affairs (AFET) will prepare an opinion on the proposal.

5 European Parliament, "Public Hearing Dual-Use Reform: How to 'future-Proof' EU Export Controls?," 2017, <https://polcms.secure.europarl.europa.eu/cmsdata/115347/programme-dual-use-reform-hearing.pdf>.

as well as interactions across governance levels. The article will also evaluate the existing response to limit the proliferation of cyber surveillance systems on the WA level, present an analysis of the current debate regarding the problematic definition of "intrusion software," and offer insights into alternative proposals—specifically whether a definition should rely on data exfiltration and user permission. The article discusses the outcome of the EU export control policy review, focusing on the regulation proposed by the Commission in September 2016 and provides an initial assessment of the key innovations and limitations of the draft text. The conclusion summarizes important findings and offers a brief outlook.

The Wassenaar Arrangement and its Discontents

Political Rationale for and Scope of the 2013 WA Amendments

The growing market for cyber-surveillance technologies entered into the spotlight following the 2011 Arab uprisings, when governments heightened the monitoring and censorship of communications in the region and the archives of deposed Arab regimes opened to the public.[6] In reaction to these revelations, legislative bodies in both the EU and the US have called for increased restrictions on cyber-surveillance and censorship technologies. In December 2013, the WA Plenary ratified two separate proposals from the UK and France to implement export controls related to 'intrusion software' and IP network surveillance systems. These amendments represented the recognition of an increasing need by the 41 participating governments to limit the proliferation of sensitive surveillance technologies to bad faith actors. The WA publishes two lists of controlled items which are not legally binding and are periodically reviewed and implemented based on national discretion. The decision to deny transfer of any item is the sole responsibility of each participating state.

The cyber-surveillance industry is comprised of a diverse set of companies of different sizes and degrees of specialization where the contours of the sector are not clearly defined. While a report by Ecorys and SIPRI estimates "over 250" active producers in Europe, a group of NGOs that formed the Coalition Against Unlawful Surveillance Exports (CAUSE) identifies 182 companies, and a recent effort by European journalists counted 235 "spy tech vendors headquartered in Europe."[7,8,9] This contains both companies, including many small enterprises, engaged exclusively in the development, production or export of cyber-surveillance

---

6 Among many individual reports, two major US news outlets and several civil society groups and international NGOs defending privacy and human rights, such as Privacy International, started to investigate the trade in cyber surveillance technologies more closely. See: "Wired for Repression," *Bloomberg*, 2011, <http://topics.bloomberg.com/wired-for-repression/>; "The Surveillance Catalogue," *Wall Street Journal*, 2011, <http://graphics.wsj.com/surveillance-catalog/#/>.

7 "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," Ecorys and SIPRI, 2015, <https://www.sipri.org/sites/default/files/final-report-eu-dualuse-review.pdf>.

8 "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE, 2015, <https://privacyinternational.org/sites/default/files/CAUSE report v7.pdf>.

9 Maaike Goslinga and Dimitri Tokmetzis, "The Surveillance Industry Still Sells to Repressive Regimes. Here's What Europe Can Do about It," *The Correspondent*, 2017, <https://thecorrespondent.com/6249/the-surveillance-industry-still-sells-to-repressive-regimes-heres-what-europe-can-do-about-it/679999251459-591290a5>.

technologies and larger defense companies that provide a broad spectrum of cyber and non-cyber surveillance, and security solutions. Additionally, many ICT companies and technology giants produce technologies like probes, deep packet inspection, data storage, or analytics systems for both surveillance and non-surveillance end-uses. Because the sector is characterized by a high level of cross-border cooperation, the delivery of customized and integrated solutions, and the presence of a wide-range of specialized brokers and suppliers, the implementation of comprehensive controls is difficult and demanding for both licensing authorities and exporters.

The adoption of the first controls on cyber-surveillance technologies in 2013 set a precedent by introducing human rights considerations into the WA.[10] WA Member States, staying within the arrangement's narrow mandate, justified the measures arguing that these technologies, "under certain conditions, may be detrimental to international and regional security and stability."[11] According to the "Initial Elements" or foundational document of the WA, the organization shall "contribute(s) to international and regional peace and security" and does not include considerations relating to the internal affairs of states.[12] The French and UK governments—which had been heavily criticized by human rights activists for the export of surveillance technologies to authoritarian governments—were particularly interested in increasing their leverage over specific companies' export decisions. The UK government was concerned about the export of FinFisher intrusion technologies by Gamma International, a British-German company. The French government proposed the restriction on IP network surveillance systems after evidence emerged that Amesys, a French company, supplied its monitoring system to Libya under Gaddafi, where it was "deployed against dissidents, human-rights campaigners, journalists or everyday enemies of the state."[13,14] France implemented the control almost immediately after it was approved by the WA, leaving EU members behind.[15]

Neither amendment was designed to solve the totality of threats to privacy and human rights stemming from cyber-surveillance technologies, but they represented the first important steps

---

10 "Comment Submitted by Privacy International in Response to the Proposed Rule (RIN 0694-AG49) Implementing Controls on Intrusion and Surveillance Items Agreed within the Wassenaar Arrangement in 2013," Privacy International, 2015, <https://privacyinternational.org/sites/default/files/Privacy International BIS submission.pdf>; and Tim Maurer, "Internet Freedom and Export Controls," Carnegie, 2016, <http://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls/iutd>.

11 "Public Statement 2013 Plenary Meeting of The Wassenaar Arrangement On Export Controls for Conventional Arms And Dual-Use Goods And Technologies," Wassenaar Arrangement Secretariat, 2013, <http://www.wassenaar.org/wp-content/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf>.

12 "Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," Wassenaar Arrangement Secretariat, 2014, <http://www.wassenaar.org/wp-content/uploads/2015/06/Guidelines-and-procedures-including-the-Initial-Elements.pdf>.

13 "British Government Admits It Started Controlling Exports of Gamma International's FinSpy," Citizen Lab, 2012, <https://citizenlab.org/2012/09/british-government-admits-it-started-controlling-exports-of-gamma-internationals-finspy/>; "Reports from the Business, Innovation and Skills, Defence, Foreign Affairs and International Development Committees Session 2013-14 Strategic," UK Government, 2013, p. 37, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/264089/8707.pdf>.

14 Margaret Coker and Paul Sonne, "Life Under the Gaze of Gadhafi's Spies," *The Wall Street Journal*, 2011, <http://www.wsj.com/news/articles/SB10001424052970203764804577056230832805896>.

15 "Comment Submitted by Privacy International in Response to the Proposed Rule (RIN 0694-AG49) Implementing Controls on Intrusion and Surveillance Items Agreed within the Wassenaar Arrangement in 2013," Privacy International, 2015, <https://privacyinternational.org/sites/default/files/Privacy International BIS submission.pdf>.

towards imposing controls on the multilateral level. The coverage of both categories has raised some concerns with a broad range of actors and implementation of the amendments remains uneven; to date, the US has not implemented the controls.[16] The category on IP network surveillance, which covers systems that conduct high performance analysis of internet traffic, is criticized for its scope because it appears extremely narrow – and as a result risks failing to catch some of the systems that are of most concern.[17] On the other hand, the control on intrusion software came under intense criticism because it employs overly broad definitions.

Instead of adding intrusion software directly to the control list, the WA establishes a definition of "intrusion software" and derives from this a second group of items that is placed under export controls. This two-tier structure leads to the restriction of the command and control infrastructure used to generate, install, and instruct the spyware, i.e., the components that stay with the purchaser, not any component that would end up on a victim's device. Although this delineation was put in place to protect targeted users and IT security businesses, cybersecurity researchers, and multinational companies have raised significant concerns. Especially in the US, implementation met stiff resistance.[18] Several security researchers have asserted that "contrary to the WA's standards, these entries are defined by pseudo-technical language, the possible interpretations of which are manifold."[19] They worry that the definition of intrusion software applies "almost universally to the building blocks of security research," which could have "chilling effects on the development of anti-surveillance measures and on the discovery of existing vulnerabilities."[20]

---

16 The European Union adopted the provisions in October 2014, 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, Official Journal of the European Union (L 134/1) of May 29, 2009. It is unlikely that the provisions will be fully implemented in the US. The Bureau of Industry and Security retracted the implementing regulation following a comment period in which it "received more than 260 comments, virtually all of them negative." See: "Wassenaar: Cybersecurity and Export Control," United States Congress, 2016, <https://oversight.house.gov/hearing/wassenaar-cybersecurity-and-export-control/>.

17 The interception of these communications, including online searches, emails, and VoIP calls, lies at the heart of many mass surveillance systems. Because the listing specifies an extensive set of capabilities, which systems need to offer in order to fall under this export restriction, the WA language on IP network surveillance remains extremely narrow and does not cover the broad spectrum of network technologies that could be employed for repressive purposes. See Collin Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies," Access, 2015, <https://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf>; and Tim Maurer, Edin Omanovic, and Ben Wagner, "Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age," New America Foundation, Open Technology Institute, March 2014, <https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf>.

18 Katie Moussouris, "You Need to Speak Up For Internet Security. Right Now," *Wired*, 2015, <http://www.wired.com/2015/07/moussouris-wassenaar-open-comment-period/>; Kim Zetter, "Why an Arms Control Pact Has Security Experts Up in Arms," *Wired*, 2015, <http://www.wired.com/2015/06/arms-control-pact-security-experts-arms/>.

19 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," 2016, <https://drive.google.com/file/d/0B5hBKwgSgYFaN2xHUkdIYWN2Mnc/view>; Sergey Bratus et al., "Why Offensive Security Needs Engineering Textbooks," Dartmouth University, 2014, <http://www.cs.dartmouth.edu/~sergey/drafts/why-offensive-security-needs-textbooks.pdf>.

20 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," Dartmouth University 2014, pp. 1–13.

Avoiding Unintended Capture

Striking the right balance between benefits and costs is a common challenge across all export control categories for dual-use items. Unduly stringent or ill-defined controls on cyber-surveillance technologies can hurt legitimate business interests and have harmful effects on computer security research. Definitions and control lists need to provide clear guidance for companies and for national licensing authorities that encourages consistency in implementation between Member States—an issue that is also highly relevant in the context of the EU reform proposal. For many observers, the current mechanism of capture of the WA controls and its implementation on the EU level does not produce efficient controls. IT security researchers and companies have argued that the complete removal or renegotiation of the 2013 amendments is preferable to their (partial) adoption, which would make the provisions subject to divergent national interpretation.[21] NGOs, privacy and human rights activists, and other researchers, however, oppose calls for the elimination and argue for clarifications, specific exemptions, controls that apply only to end use cases and end-users facilitating or conducting surveillance, as well as clearer definitions for the most contentious categories.[22]

The core problem is that the existing WA entries on "intrusion software" (Categories 4.A.5., 4.D.4., 4.E.1.a., and 4.E.1.c.) are based on technical attributes common to both commercial surveillance and information security tools—those technologies to infiltrate targeted devices without consent and those for testing for vulnerabilities. IT security researchers emphasize that "it is impossible to distinguish among malicious and innocuous software on a technical basis" and some even argue that "unless a specific software can be confidently classified as "single-use," it would be highly unwise to regulate it."[23,24] A number of alternative proposals suggest focusing on the critical dependence of surveillance software "to secretly exfiltrate data from the computer, without user permission or knowledge" to ensure that legitimate research and

---

21 Dullien, Iozzo, and Tam, "Surveillance, Software, Security, and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting;" and Microsoft Corporation, "Written Testimony of Cristin Flynn Goodwin Assistant General Counsel for Cybersecurity at Microsoft Corporation; Joint Subcommittee Hearing on Wassenaar: Cybersecurity & Export Control January 12, 2016," United States Congress, 2016, <https://oversight.house.gov/wp-content/uploads/2016/01/Goodwin-Microsoft-Statement-1-12-Wassenaar.pdf>; Cheri F . McGuire, "Prepared Testimony and Statement for the Record of Cheri F. McGuire Vice President, Global Government Affairs & Cybersecurity Policy; Symantec Corporation Hearing on Wassenaar: Cybersecurity & Export Control Before the House Committee on Homeland," United States Congress, 2016, <https://oversight.house.gov/wp-content/uploads/2016/01/McGuire-Symantec-Statement-1-12-Wassenaar.pdf>.

22 Access et al., "Comments to the US Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements (RIN 0694-AG49)," 2015, <https://www.eff.org/files/2015/07/21/jointwassenaarcomments-final-1.pdf>; and Electronic Frontier Foundation, "Comments of the Electronic Frontier Foundation on the Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, RIN 0694-AG49," 2015, <https://www.eff.org/files/2015/07/21/effwassenaarcomments-1.pdf>.

23 Dullien, Iozzo, and Tam, "Surveillance, Software, Security, and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting," WA-CAT4 Draft, 2015, <https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file>.

24 Vincenzo Iozzo, "Speech to Members of the European Parliament and European Commission, September 30, 2015," 2015, <https://drive.google.com/file/d/0B3NL8jkEQKjYcnp5aUtsSVRoQjA/view?pref=2&pli=1>.

information sharing is still possible without the need to apply for an export license.[25] Because "the vast majority of exfiltration software has no legitimate use," it "could safely be regulated without having adverse consequences on legitimate security research."[26]

Some proposals also call for a control approach that "takes into account the intent of the technology and software developer."[27] By shifting the definition of "intrusion software" to focus on intent, not functionality, the export authorization would rely more on contextual information. Manifest intent could, for example, be established by looking at the way the software is designed, i.e., whether it is designed to be used against a non-consenting other party, or the way the software is marketed.[28] This approach tries to reconcile both sides of the debate by adding to the definition of intrusion software the criterion of authorization by the owner of the targeted device to install software or perform specific actions.[29]

However, while the overlap between offensive and defensive applications seems to necessitate increased attention to the intended use of technologies, it also complicates the export authorization process.[30] Because export controls are critically dependent on the capacity to define an item with legal precision in a manner that can be employed at some stage prior to the transfer, categories on the dual-use list are traditionally based on precisely defined performance metrics. While it might be possible to identify certain products by relying on user authorization as a criterion, this would not apply to the full spectrum of relevant technologies. Similarly, a definition of intrusion software dependent on its intended use would likely pose a higher administrative burden for licensing authorities, while exporters would be required to provide additional information on customers and develop further so-called "know your customer approaches." The ambiguity of a classification of products based on intent may also be compounded by the component nature of cyber-surveillance systems; licensing authorities would need additional technical expertise to identify critical exports.

---

25 Sergey Bratus et al., "Why Offensive Security Needs Engineering Textbooks," Dartmouth University, 2014, <http://www.cs.dartmouth.edu/~sergey/drafts/why-offensive-security-needs-textbooks.pdf>.

26 Vincenzo Iozzo, "Speech to Members of the European Parliament and European Commission, September 30, 2015," 2015, <https://drive.google.com/file/d/0B3NL8jkEQKjYcnp5aUtsSVRoQjA/view?pref=2&pli=1>.

27 "Comment Submitted by Privacy International in Response to the Proposed Rule (RIN 0694-AG49) Implementing Controls on Intrusion and Surveillance Items Agreed within the Wassenaar Arrangement in 2013," Privacy International, 2015, <https://privacyinternational.org/sites/default/files/Privacy International BIS submission.pdf>; "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE Report, June 2015, p. 17, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

28 Thomas Dullien, "An Attempt at Fixing Wassenaar," ADD/XOR/LOR Blog, 2016, <http://addxorrol.blogspot.de/>.

29 Dullien, Iozzo, and Tam, "Surveillance, Software, Security, and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting," WA-CAT4 Draft, 2015, <https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file>.

30 This can also be highlighted with reference to the Tallinn Manual on the International Law Applicable to Cyber Warfare, which defines a 'cyber weapon' by the effects it may have, rather than by its nature or components, or means of operation or construction. (See Tallinn Manual Rule 41 No 2).

Avenues for Future Activity on the WA Level

Revising the relevant WA language has proven difficult, not least because the majority of the 41 members have already implemented the provisions, and the controls on cyber-surveillance technologies are only two of many items to be reviewed and discussed.[31] On March 1, 2016, the US government sent an open letter to several business associations in which it explained that the administration "has proposed in this year's WA [review] to eliminate the controls on technology required for the development of 'intrusion software.'"[32] After some initial successes in mid-2016, when the parties agreed in principle to clarify some of the wording and asked for a report detailing specific examples of cybersecurity tools that might be inappropriately covered, the WA Plenary of December 2016 failed to rephrase the most important provisions with regard to vulnerability research and disclosure.[33] Despite the US government's two-year effort, delegates could not reach a unanimous decision to ease the export restrictions, which shows the difficulties inherent in the multilateral negotiation process.[34] It will now be up to the new US Trump administration to decide whether to continue renegotiations.[35]

The difficulties encountered when trying to modify the arrangement's existing provisions also give some indication of the challenges in creating multilateral controls for additional products and services—which remains the preferred course of action for many stakeholders, including European exporters of cyber-surveillance technologies.[36] Export controls should principally be established on the highest possible level to increase their impact and prevent circumvention. Further attempts to add cyber-surveillance technologies to the WA on human

---

31 Tim Maurer, "Internet Freedom and Export Control," Carnegie Endowment for International Peace, 2016, <http://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls-pub-62961>.

32 "Letter from Secretary Pritzker to Several Associations on the Implementation of the Wassenaar Arrangement 'intrusion Software' and Surveillance Technology Provisions," US Department of Commerce, March 1 2016, 2016, <https://www.bis.doc.gov/index.php/oee/9-bis/carousel/1010-letter-from-secretary-pritzker-to-several-associations-on-the-implementation-of-the-wassenaar-arrangement-intrusion-software-and-surveillance-technology-provisions>; "Major Business and Tech Groups Call on Administration Officials to Renegotiate Wassenaar Arrangement to Strengthen Cybersecurity," Information Technology Industry Council, 2016, <http://www.itic.org/dotAsset/9/8/98c27c3a-609b-41e3-8f7b-4fe1bb642ad6.pdf>.

33 With regard to categories 4.A.5., 4.D.4, the definition of 'intrusion software' was amended. See page 215 of the WA Dual-use List: <http://www.wassenaar.org/wp-content/uploads/2016/12/WA-LIST-16-1-2016-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf>;

34 Iain Mulholland and Katie Moussouris, "Administration Should Continue to Seek Changes to International Cyber Export Controls," *The Hill*, 2017, <http://thehill.com/blogs/congress-blog/technology/316978-administration-should-continue-to-seek-changes-to>; Iain Thomson, "Wassenaar Weapons Pact Talks Collapse Leaving Software Exploit Exports in Limbo," *The Register*, 2016, <http://www.theregister.co.uk/2016/12/21/wassenar_negotiations_fail/>.

35 Jim Langevin, "Langevin Statement on Wassenaar Arrangement Plenary Session," Congressman Jim Langevin Website, December 19, 2016, <http://langevin.house.gov/press-release/langevin-statement-wassenaar-arrangement-plenary-session>.

36 See for example the statements of expert witnesses from industry associations and producers at the European Parliament, "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation," March 21, 2017, <http://www.europarl.europa.eu/news/en/news-room/20170316IPR67192/committee-on-international-trade-21032017-(pm)>.

rights grounds will, however, likely meet significant resistance.[37] The WA's traditional focus on conventional arms and dual-use items for the production of Weapons of Mass Destruction WMDs) places significant limits on the types of surveillance technologies that can be added. The present controversy about unintended capture, the business-friendly attitude of the new US administration, and generally diverse WA membership, which, for example, includes Russia and remains subject to EU and US sanctions—are also likely to increase opposition.

Given the inefficiency of controls and the lack of progress on the multilateral level, EU Member States have—in some cases reluctantly—developed further the European control regime and independently implemented additional controls on the national level.[38] For example, Italy established restrictions in 2012 following reports that an Italian company had begun to install a monitoring center in Syria.[39] More recently, the German government introduced national controls on items that are not listed at the WA or EU level in July 2015 after a German proposal to add additional lawful interception technologies to the WA lists did not gain traction from late 2014 to early 2015.[40] Germany argued that national measures had become necessary because similar restrictions on the European level "could not be expected before 2017" but would repeal the national controls once a European solution had been implemented.[41] On the European level, an increasing number of actors, including a majority of the European Parliament, have argued for an independent mechanisms through which to control the export of cyber-surveillance technologies. The draft regulation on dual-use exports recently published by the European Commission, which will be discussed in the next section, represents an important step in this direction and takes up many suggestions made in the debate and public consultation.

---

37 Ian J. Stewart and Sibylle Bauer, *Workshop: Dual-Use Export Controls (Background Paper)*, 2015, p. 30, <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU(2015)535000_EN.pdf>.

38 Article 8 (1) of Regulation 428/2009 permits EU governments to impose national controls on non-listed items for reasons of public security or human rights considerations. This clause has repeatedly been used to control cyber surveillance technologies.

39 The company in question, Area S.p.A., announced that it would not complete the installation of the monitoring center. See Vernon Silver, "Italian Firm Exits Syrian Monitoring Project, Repubblica Says," *Bloomberg Business*, 2011, <http://www.bloomberg.com/news/articles/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says>; Italian Government, "Notices From Member States Regarding Council Regulation (EC) No 428/2009: Regarding Delivery of Monitoring System to Syria," 2012, <http://trade.ec.europa.eu/doclib/docs/2012/september/tradoc_149946.pdf>.

40 The fourth amendment to the German Foreign Trade Ordinance establishes new control list categories covering monitoring centers and data retention systems and introduces authorization requirements on the provision of 'technical assistance,' an intentionally broad concept of related services. However, the national controls affect only a small number of companies, many of which had already been subject to export controls on encryption technologies. See: Stephanie Horth, Joanna Bronowicka, and Ben Wagner, "Policy Brief Export Control," Centre for Internet and Human Rights, 2015, <https://cihr.eu/export-controls-policy-paper/>.

41 German Government, *Vierte Verordnung zur Änderung der Außenwirtschaftsverordnung*, 2015, <https://www.bmwi.de/BMWi/Redaktion/PDF/V/vierte-verordnung-zur-aenderung-der-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.

EU Dual-Use Export Controls and Policy Review

The Outcome of the Export Control Policy Review

Increasing exports of cyber-surveillance technologies have been addressed by the European Union through a series of loosely connected measures. These include the broadening of specific sanction regimes from 2011 onwards, the implementation of WA amendments in October 2014, the adoption of human rights guidelines with regard to freedom of expression online, and a wide-ranging review of the EU's dual-use export control policies.[42] This section analyzes the outcome of the export control policy review, which was broadly aimed at updating the regulatory framework on dual-use exports, regulatory simplification, and "an initiative to control ICTs to prevent violations of human rights and protect the EU's security."[43]

On September 28, 2016, the European Commission proposed a draft regulation to modernize the existing control regime, highlighting the need for "adjusting to evolving security risks and threats; adapting to rapid technological and scientific developments; [and] preventing the export of cyber-surveillance technology in violation of human rights."[44] The Commission characterized the proposal as an ambitious step that combines elements of a more pragmatic export control "system update" aimed at adjusting the existing framework with a forward-looking "system modernization" focusing on cyber-surveillance technologies and human rights.[45] The draft would replace Regulation 428/2009, adopted in May 2009, which so far formed the basis for the EU's common policy on export controls for dual-use items, including cyber-surveillance technologies. The Dual-Use Regulation establishes rules for export, transit, brokering, and intra-community transfer procedures across EU Member States and aggregates externally-originating requirements that are agreed within the WA and other multilateral export control regimes. The regulation is binding and directly applicable throughout the EU but leaves implementation and enforcement to Member States, including decisions regarding whether to grant or to refuse export licenses—although coordination measures exist to promote uniform implementation.[46]

---

42 Following revelations about European companies selling surveillance technologies to Iran and Syria, country-specific sanctions regimes were updated as part of the EU's Common Foreign and Security Policy (CFSP). In December 2011, a broad ban on equipment and software "for use in the monitoring or interception by the Syrian regime, or on its behalf, of the internet and of telephone communications on mobile or fixed networks" and the provision of associated services was added to sanctions against Syria. In March 2012, equivalent language was inserted into the Iran embargo.

43 "Roadmap. Review of the EU Dual-Use Export Control Regime," European Commission, 2015, <http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2015_trade_027_duxc_en.pdf>; and "Green Paper: The Dual-Use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>.

44 "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)," European Commission, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf>.

45 These terms describe Policy Option 3 and Option 4 set out in the Roadmap for the export control policy review, cf. European Commission, "Roadmap. Review of the EU Dual-Use Export Control Regime."

46 To avoid delays, the Commission has delegated authority to update the control list pursuant to regulation 599/2014. At the time of writing, the latest version of the control list is regulation 2016/1969 of 12 September 2016.

The proposed regulation places significant emphasis on the control of cyber-surveillance technologies. The official impact assessment for the regulation argues that a modernization of the existing regime "appears indispensable to achieve the objective to prevent human rights violation caused by the lack of appropriate controls of cyber-surveillance technology."[47] To this end, the definition of dual-use items has been revised in Article 2.1b of the draft to specifically 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." Taking up and combining some of the initial proposals in the review, the draft regulation sets out a twofold control approach: first, it introduces an EU autonomous control list of specific cyber-surveillance technologies (Annex 1B "List of Other Dual-Use Items).[48] Second, it establishes a targeted catch-all clause designed to act as an emergency brake in cases "where there is evidence that the items may be misused by the proposed end-user for directing or implementing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination."[49]

The new regulation also for the first time features a definition of cyber-surveillance technology which is broadly understood as "items specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analyzing data, and/or incapacitating or damaging the targeted system."[50] This constitutes a wide definition of the technologies in question and is developed further by explicitly stating that "[t]his includes items related to the following technology and equipment: mobile telecommunication interception equipment; intrusion software; monitoring centers; lawful interception systems and data retention systems; digital forensics."[51] Interestingly, the definition has been narrowed between July 2016, when a draft of the proposal was leaked, and the official publication in September 2016.[52] While the old definition reflected the very broad conception of cyber-surveillance technologies available in the Ecorys/SIPRI report supporting the EU impact assessment, the new version no longer explicitly refer to biometrics, location tracking,

47 "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)," European Commission, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf>.

48 Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," DG Trade, European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>, p. 2.

49 "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)," European Commission, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf>.

50 See Article 2.2.21 of the draft regulation.

51 Ibid.

52 Catherine Stupp, "Commission Plans Export Controls for Surveillance Technology," *Euractiv*, 2016, <https://www.euractiv.com/section/trade-society/news/technology-companies-face-export-hurdles-under-draft-eu-rules/>.

probes, and deep packet inspection systems.[53,54] The accompanying documents did not explain the rationale behind the clarification; it might be due to concerns regarding unintended capture and administrative costs for national agencies or exporters. This will be discussed in the next sections, which introduce key innovations in the proposal and offer an assessment of the wider implications and limitations of the draft text so far as it relates to cyber-surveillance technologies.

An EU Autonomous Control List: Additional Coverage but a Lack of Clarity

The Commission has proposed to introduce an EU autonomous list with the aim to control the export of specific items necessary in cyber-surveillance that are not part of other applicable control lists.[55] This represents an important and ambitious step that has also been advocated by different actors in the debate.[56] However, EU governments and industry have previously sought to avoid adopting EU-level controls on items that are not included on the WA level due to concerns about implementation costs and the competitiveness of EU-based companies. The Commission has therefore been very careful to highlight that the new control measures "should not go beyond what is proportionate" and the impact assessment states, "[t]he precise design of those new controls would ensure that negative economic impact will be strictly limited and will only affect a very small trade volume."[57] Reliable estimates regarding the size of the cyber-surveillance sector are, of course, hard to come by, but SIPRI recently conducted a trade analysis of dual-use related exports of ICT goods. They found dual-use related exports in electronics of €31.7 billion, in computers of at least €2 billion, and in telecommunications and 'information security' of up to €22.6 billion for the year 2014.[58] Still, it remains impossible to infer from these figures the export volume of especially critical technologies like intrusion software, which accounts only for a small percentage of these figures.[59] Further taking into account that these numbers represent global exports, it is likely that the new controls will only affect a small amount of this trade, which can be reduced further by defining the controlled technologies and circumstances in which export authorization should be denied more accurately.

---

53 Ecorys and SIPRI, "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," 2015, pp. 147-9, 218.

54 Civil society actors such as a group of NGOs represented by the Coalition Against Unlawful Surveillance Exports (CAUSE) have argued for additional controls on voice identification technology, location monitoring technology and additional systems for collecting data as it passes through communications networks (LI solutions and 'inter-connectors', probes and fiber taps). Most of these would have been part of the definition of cyber-surveillance technology in the version as of July 2016. See "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE, 2015, <https://privacyinternational.org/sites/default/files/CAUSE report v7.pdf>.

55 Regulation 428/2009 aggregates externally-originating requirements that are agreed within other forums, specifically the WA, the Missile Technology Control Regime, the Nuclear Suppliers' Group, the Australia Group and the Chemical Weapons Convention.

56 Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," DG Trade, European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>, p. 2.

57 See recital (5) of the draft EU regulation.

58 Based on Eurostat data and mirroring the ECCN categories 3 to 5. Ecorys and SIPRI, "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," 2015, p. 146.

59 This can be inferred from looking at national export statistics on cyber-surveillance technologies that is made publicly available by the UK and Switzerland.

Although the coverage of the proposed autonomous list remains limited, few countries seem to support the approach.[60] A 2015 survey by Ecorys and SIPRI of Member State governments found that only a small number of respondents are in favor of controlling additional technologies such as "LI systems, data retention systems, and covert mass surveillance."[61] Interestingly, the new Annex 1B mirrors the control provisions that were implemented by the German government on the national level with regard to Law Enforcement Monitoring Facilities and data retention systems in July 2015.[62] However, a group of EU Member States, including Germany, France, and the UK, asked the Commission before publication of the proposal to scrap the autonomous list approach, allegedly arguing that "unilateral EU lists would be less effective, [and] undermine the competitiveness of EU industry."[63] Instead, they proposed to attempt further negotiations on the WA level or in an alternative international setting beyond the EU, a shift that would further delay the establishment of effective controls for cyber-surveillance technologies. This would, of course, significantly decrease the impact and innovative character of the new EU regulation.

Unilateral, EU-wide controls have especially been opposed by the European cyber-surveillance industry but also have effects beyond Europe. Press reports indicate that the Commission has been approached by companies and industry associations fearing that the regulation would decrease their competitiveness and legal certainty, and could even force companies to move outside the EU.[64] A group of Commissioners, led by then-Commissioner for Digital Economy Günther Oettinger, allegedly argued for a more business-friendly regulation and lobbying efforts might already have led to the narrowing of the definition of cyber-

60 Section B of Annex I ("Other Items of Cyber-Surveillance Technology" contains entries for monitoring centers for lawful interception and data retention systems or parts thereof (10A001) as well as the respective provisions on the software (10D001) and technology (10E001) necessary for the items specified in 10A001. The new controls may offer a potential loophole because, according to the technical note, category 10A001 includes an exemption for products designed for and used at telecommunications companies (service providers). Especially data retention is often performed by service providers and in many authoritarian states these have close ties to the state. This exemption has already been criticized in the context of the German controls; the impact on the effectiveness of the controls remains, however, difficult to assess. See for example Catherine Stupp, "Germany Leaves Brussels behind on Surveillance Tech Export Controls," *Euractiv*, 2015, <http://www.euractiv.com/section/digital/news/germany-leaves-brussels-behind-on-surveillance-tech-export-controls/>.

61 Ecorys and SIPRI, "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," 2015, pp. 147-9, 218.

62 This relates to the German Foreign Trade Ordinance (*Außenwirtschaftsverordnung*) and especially the categories 5A902, 5D902, 5E902 in Appendix 1 (AL) Part I B (in force 18.07.2015).

63 EurActiv reported that Austrian, Finnish, French, German, Polish, Slovenian, Spanish, Swedish, and UK diplomats circulated a memo asking the Commission to scrap the list of products that will be subject to EU export controls and instead broker an international agreement that involves countries outside the EU. See: Catherine Stupp, "Tech Industry, Privacy Advocates Pressure Commission on Export Control Bill," *Euractiv*, 2016, <https://www.euractiv.com/section/trade-society/news/tech-industry-privacy-advocates-pressure-commission-on-export-control-bill/>.

64 Because the sector is highly fragmented and companies offer a very heterogeneous set of goods, services and technologies, they are not represented by a single industry association. Rather, certain companies are members of ICT-focused associations, such as Digital Europe, or IT-focused associations, such as BitKom, or defense and security associations, such as ASD, while especially smaller companies are not members of any association.

surveillance technology described above.[65] In terms of implementation, the Commission's impact assessment concedes that controls on cyber-surveillance technologies "could result in a higher administrative burden for operators and authorities, since a new category of goods and technology would be subject to control."[66] In addition, it has been argued that an autonomous list could generate some confusion with non-EU states that refer to the EU dual-use list as a synthesis of multilateral regimes that are nationally implemented.[67] Would the EU start to include additional technologies because of specific human rights concerns, these countries might stop aligning their national control lists with the EU framework, thus decreasing the indirect influence of the EU on export controls globally. On the other hand, unilateral measures—together with some active diplomacy—could also allow the EU to demonstrate how cyber-surveillance technologies can effectively be controlled and increase the chances that others might follow or enact similar controls.

Much work is still required to ensure that legitimate exports are not inadvertently caught. The proposal offers some assurances that the new controls do "not prevent the export of information and communication technology used for legitimate purposes, including law enforcement and internet security research."[68] While the Commission intends to develop guidelines to support the practical application of the proposed controls, it recently described the development of these guidelines as a principally "operational issue" that could be addressed later. For all affected communities, the vagueness of the new control provisions on cyber-surveillance technologies remains a key concern. The lack of clarity on what, for example, can be classified as "digital forensics," a term used in the proposal's definition of cyber-surveillance technology, in combination with the new catch-all provision, has been raised by companies and NGOs alike. Privacy International rightly observes that "like intrusion software, forensic tools can be used to enhance and improve cybersecurity, and by extension protect human rights globally, and must not be restricted when moving between international parties to remedy problems with IT systems."[69] The discussion on the coverage of the proposed regulation thus mirrors the situation on the WA level, where a lack of clear definitions creates legal uncertainty and inconsistent implementation.

An important question also is whether the Commission would be empowered to add technologies independently to the autonomous list (Annex 1 Section B), which is currently

---

65 Ibid.

66 "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)," European Commission, September 28, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf>.

67 Sibylle Bauer and Mark Bromley, "The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World," *Nonproliferation Papers* 48 (2016) p. 8, <http://www.nonproliferation.eu/web/documents/nonproliferationpapers/the-dual-use-export-control-policy-review-balancin-49.pdf>.

68 Preamble of the draft regulation, recital (5).

69 Edin Omanovic, "Landmark Changes to EU Surveillance Tech Export Policy Proposed, Leaked Document Shows," Privacy International, July 2016, <https://www.privacyinternational.org/node/909>.

envisioned in Article 16.2b of the draft.[70] Delegated acts were previously only used to aggregate externally-originating requirements negotiated by the Member States in multilateral export control forums. Article 16.2 would enable the Commission to assess the risks associated to non-listed technologies and to enact additional controls on cyber surveillance technologies if it proves necessary, an approach which has been suggested by some researchers.[71] It is likely that Member States would oppose this appreciation of the Commission's role and the lack of clear selection and assessment criteria for this process has already attracted criticism by national export licensing bodies.[72]

Overall, the proposal remains unclear in the details of what constitutes controlled cyber-surveillance technologies and more clarity is needed before all concerned stakeholders can fully understand the nature and functioning of these controls. Going forward, it will be crucial to work out and communicate the differences between the way in which exports of specific technologies aid in the violation of fundamental human rights and, alternatively, support legitimate IT security practices. There remains a considerable need for clarification and additional work on the control requirements at the European level and, for those Member States that seek to actively support the redrafting of the WA controls on intrusion software, a need for outreach efforts aimed at inviting affected and interested parties to provide expertise on how to implement the controls. On both levels, existing proposals to distinguish technology based on data exfiltration and user consent might certainly be worthy of further exploration.[73] Legal certainty is especially critical in the case of cyber-surveillance technologies because only clear-cut authorization requirements can act as a credible preventive and deterrent measure.

Strengthening the Role of Human Rights in the Export Authorization Process

Much of the discussion over the last years has focused on the way in which EU Member States address human rights considerations in their export licensing processes. By incorporating important innovations based on the human security approach, the Commission proposal represents a major step towards an explicit obligation for national licensing authorities to base their assessments on respect for human rights and the internal situation in the country of final destination. Going forward, it will, however, be necessary to clarify the language and obligations further and provide effective guidance or even clear criteria to the Member States specific to licensing assessments on cyber-surveillance technology.

While the inclusion of human rights considerations in licensing decisions on dual-use exports is already required under the EU dual-use regulation, Member States have interpreted and applied

---

70 According to Article 16.2b, the Commission would be empowered to adopt delegated acts to amend Section B of Annex I "if this is necessary due to risks that the export of such items may pose as regards the commission of serious violations of human rights or international humanitarian law or the essential security interests of the Union and its Member States."

71 Ian Stewart and Sibylle Bauer, "Workshop: Dual-Use Export Controls (Background Paper)," European Parliament, 2015, p. 30, <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU(2015)535000_EN.pdf>.

72 Statement by an expert of the Federal Office for Economic Affairs and Export Control, Germany, see: "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation (March 21, 2017)," European Parliament, 2017.

73 See Section 2.2 above.

these criteria differently. Article 12 of the existing regulation requires Member States to base their decisions on the authorization of exports on all relevant considerations, "including those covered by Council Common Position (2008/944/CFSP) defining common rules governing control of exports of military technology and equipment." However, while the Common Position provides a basic set of criteria, the European Parliament has repeatedly criticized that it "is being applied loosely and interpreted inconsistently by the Member States," which is especially true for the criterion on human rights.[74,75] Consequently, there is a clear need to move closer towards agreed EU-wide standards that highlight the role of human rights in assessment processes for dual-use exports.

The proposed regulation puts in place a clear obligation for EU governments to assess human rights implications and deny applications where there is a clear risk of human rights abuses. The new Article 14, which is based on Article 12 of the existing regulation, states explicitly that competent authorities should consider "respect for human rights in the country of final destination as well as respect by that country of international humanitarian law" and "the internal situation in the country of final destination." This could considerably strengthen the role of human rights criteria in the assessment process and lead to a more uniform application of the existing assessment criteria across Member States. In addition, the regulatory intent becomes evident in the preamble to the proposed regulation, which "clarifie[s] that assessment criteria for the control of exports of dual-use items include considerations regarding their possible misuse in connection with acts of terrorism or human rights violations."[76]

The draft reflects the initial proposal by the Commission which aimed at evolving the existing regime "towards a 'human security' approach recognizing that security and human rights are inextricably interlinked."[77] This approach shifts attention from national security issues related to potential military end-uses to people-centered security, for example, terrorism and human rights violations, which becomes evident with the additional catch-all clauses in Article IV.[78] The additions go a long way in addressing criticism that human rights concerns are not sufficiently

---

74 Human rights concerns are addressed in Criterion Two of the Common Position. It requires EU Member States "to deny an export license if there is a clear risk that the military technology or equipment to be exported might be used for internal repression." The User's Guide to the Common Position emphasizes that "communications/surveillance equipment can have a strong role in facilitating repression."

75 "European Parliament Resolution of 17 December 2015 on Arms Export: Implementation of Common Position 2008/944/CFSP (2015/2114(INI))," European Parliament, December 17, 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2015-0472+0+DOC+PDF+V0//EN>.

76 See preamble of the draft regulation, recital (6).

77 Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," DG Trade, European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>, p. 2.

78 In this regard, the human rights focus also contributes to the expansion of the traditional conception of 'dual-use' towards the 'legitimate versus illegitimate purpose' and 'benevolent versus malevolent use' paradigm that is discussed with regard to cyber surveillance technologies and 'manifest intent.' See for example Johannes Rath, Monique Ischi, and Dana Perkins, "Evolution of Different Dual-Use Concepts in International and National Law and Its Implications on Research Ethics and Governance," *Science and Engineering Ethics* 20:3 (2014), pp. 769–90. This shift in the understanding of 'dual-use' has also become evident in the addition of cyber surveillance technology to the definition of 'dual-use items' in the proposed regulation.

incorporated or easily ignored because of political or economic reasons. The proposal in Article 14 removes the reference to Council Common Position 2008/944/CFSP, which does not explicitly mention threats to, for example, the right to privacy and freedom of expression. Instead, a clear reference to human rights is added and the explanatory memorandum to the new regulation further underlines the risk that the export of cyber-surveillance technology poses to fundamental human rights, including the right to privacy and freedom of expression. To clarify the benchmarks for risk assessments even further, Article 14d could explicitly mention these and other human rights that are particularly exposed to violations through surveillance exports.[79]

EU Member States appear skeptical about the additional emphasis on human rights in the licensing process and are specifically concerned about implementation challenges and the administrative burden for licensing authorities and exporters.[80] Uncertainty could generate a large number of speculative license applications.[81] While some support exists for human rights criteria by, for example, the Netherlands, other Member States seem to perceive the Common Position as a good basis for export licensing assessments and see the problem primarily with its inconsistent application. Business associations have also repeatedly expressed concerns about non-specific human rights standards because they could complicate licensing assessments, increase the need for information collection about their customers, and decrease legal certainty.[82] On the other hand, NGOs and the European Parliament have repeatedly called for stronger human rights criteria.[83]

Given the cautionary remarks by some governments, the Commission proposal retained an overall high level of ambition regarding human rights criteria. To ensure proper implementation, the licensing obligation would need to be accompanied by measures that promote more uniform risk assessment across Member States. The way in which Member States interpret the provision

---

79 "Stellungnahme zum Entwurf der EU-Kommission zur Verordnung Nr . 428 / 2009 über Exportkontrollen von Dual-Use-Gütern," Reporters without Borders, January 2017, <https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Internetfreiheit/20170209_Stellungnahme_ROG_BMWi_Dual_Use_Richtlinie.pdf>.

80 According to Euractiv, a number of Member States have told the Commission that "[t]argeted sanctions are the primary instrument to prevent the misuse of technology for human rights violations." See Catherine Stupp, "Germany Leaves Brussels behind on Surveillance Tech Export Controls," *Euractiv*, 2015, <http://www.euractiv.com/section/digital/news/germany-leaves-brussels-behind-on-surveillance-tech-export-controls/>.

81 "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation (March 21, 2017)." European Parliament.

82 Instead, these associations emphasize the role of due diligence programs, reporting according to the UN Guiding Principles on Business and Human Rights and the integration of human rights into corporate culture and ethical guidelines. See: DigitalEurope, "DIGITALEUROPE Position Paper on the Review of Export Control Policy in the EU," February 2016, <http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1125&PortalId=0&TabId=353>; and "EC Dual-Use Review of the EC Dual-Use Regulation," BDI, January 2016, <http://bdi.eu/media/topics/global_issues/downloads/201601_FINAL_BDI-Assessment_Reform_EC_Dual-Use.pdf>.

83 "Human Rights and Technology in Third Countries European," European Parliament, 2015, <http://www.europarl.europa.eu/sides/getDoc.do?type=PV&reference=20150908&secondRef=ITEM-005-08&language=EN>; "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE, 2015, p. 17, <https://privacyinternational.org/sites/default/files/CAUSE report v7.pdf>; and Joe McNamee (EDRi), "Consultation on the Export Control Policy Review (Regulation (EC) No 428 / 2009)," 2015, <https://edri.org/files/export_controls_edri.pdf>.

in their export licensing processes is of critical importance for the overall effectiveness of the control regime. While difficult to establish, mandatory risk assessment criteria for licensing procedures could—in comparison to more ambiguous guidelines—significantly increase a consistent and uniform implementation of the new regulation across Member States. In any case, this should also be supplemented by strengthened human rights due diligence procedures and compliance programs that are in some cases already in place—which goes beyond the framework of the dual-use policy review and entails a broader engagement about the use of soft law measures.[84]

Convergence in Interpretation and Use of Catch-all Controls

Similarly, while the dedicated catch-all clause represents an important step towards the control of surveillance exports, there remains a need for clarifications and additional guidance to ensure the catch-all's uniform application. The Commission proposal adds a new type of catch-all to Article 4 of the dual-use regulation, which traditionally allowed Member States to deny the export of non-listed items with potential military or WMD end-use. Article 4d now states that export authorization is required for non-listed items if they are intended "for use by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination." The cyber-surveillance catch-all mechanism would be different in nature from existing ones which deal with a generally more limited range of technologies and destinations and are based on a significant body of knowledge.

Considering the pace of technological development and the variety and ambiguity of cyber-surveillance systems, catch-all provisions provide licensing authorities with the flexibility to respond quickly to critical exports. A catch-all would be useful in future proofing the control system and has so far been less controversial than list-based controls with Member States. Unlike list-based approaches, the application of a catch-all depends entirely on the Member State. Likely results are differences in national implementation and uncertainty among companies, which increase the need for coordination and accountability mechanisms. These problems already occur in the context of the military and WMD catch-all clauses, even though agreed practices and shared standards have been developed.[85] Proponents of the cyber-surveillance technology catch-all have therefore stressed the need to ensure consistent implementation. The European Parliament, for example, highlighted the need "to implement and monitor EU regulations and sanctions relating to ICTs more effectively, including the use of catch-all mechanisms, so as to

---

84 For a detailed assessment of industry self-regulation and the application of CSR guidelines see: Mark Mark Bromley et al., "ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns," *Strategic Trade Review* 2:2 (Spring 2016), pp. 37–52. The authors argue that self-regulation and CSR can form "a useful complement to export controls in the effort to create improved standards in the export of ICT surveillance systems."

85 Sibylle Bauer and Mark Bromley, "The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World," *EU Non-proliferation Paper* 48, SIPRI, March 2016, p. 8. In explaining the need for recasting the dual-use regulation, the Commission pointed out that "divergences in interpretation and application among Member States result in asymmetrical implementation and create competitive distortions within the Single Market.," see: "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)" European Commission, 2016.

ensure that […] a level playing field is preserved."[86] Industry is opposed to this measure and states that "catch-all controls should only be a last resort."[87]

The proposal so far does not offer sufficient guidance for Member States to bridge the existing differences in catch-all application and reinforce a policy of no-undercutting. The new regulation envisages a mandatory consultation procedure between licensing authorities to facilitate the use of catch-all provisions and aims at strengthening information exchanges between the Commission and Member States. However, government officials noted concerns regarding a catch-all's uniform implementation in the 2016 Ecorys/SIPRI survey and the March 2017 expert hearing in the European Parliament.[88] Establishing rules for a uniform application would, for example, first require a fundamental understanding regarding the way in which catch-all controls should be employed. Practice differs between governments with regard to the application to an entire destination country or to a specific end-user and whether the provision is used to stop a specific shipment or more broadly as a precautionary or awareness-raising measure.[89] Stakeholders also noted "that if there was a lack of specificity in both the technology and end-users covered by a cyber-surveillance catch-all mechanism it might make it hard to implement" and guarantee uniform implementation.[90] In this regard, it is noteworthy that the language of the catch-all characterizes the recipient as "persons" instead of referring to institutionalized actors such as the armed forces, the police, intelligence, or law enforcement agencies of the state, which would limit the group of relevant end-users.[91] Concerns were also raised with regard to the threshold of "serious violations of human rights" that allows recourse to the catch-all.[92] A greater role of the Commission in coordinating implementation and issuing guidance, which is sometimes suggested, would likely raise concerns with some Member States.[93]

---

86 Frans Timmermans, "Human Rights and Technology in Third Countries European," Speech to the European Parliament, September 7, 2015, <https://ec.europa.eu/digital-single-market/en/news/human-rights-and-technology-third-countries>.

87 "EC Dual-Use Review of the EC Dual-Use Regulation," BDI, January 2016, <http://english.bdi.eu/media/topics/global_issues/downloads/FINAL_BDI-Assessment_Reform_EC_Dual-Use.pdf> and "DIGITAL EUROPE Position Paper on the Review of Export Control Policy in the EU," DigitalEurope, October 2014, <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/droi/dv/412_digitaleurope_position_paper_/412_digitaleurope_position_paper_en.pdf>.

88 An expert of the German Federal Office for Economic Affairs and Export Control noted that consultations between EU Member States based on Art. 4 of the proposal might not lead to an understanding on common standards. See: "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation (March 21, 2017)," European Parliament, 2017

89 Sibylle Bauer and Mark Bromley, "The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World," *EU Non-proliferation Paper* 48, SIPRI (March 2016), p. 6; and Ecorys and SIPRI, "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," (2015), p. 103.

90 Ibid, 219–20.

91 In comparison, Article 6 of the Common Position 2008/944/CFSP states that the criteria only apply to dual-use goods and technology "if the end-user will be armed forces or internal security forces." However, many cyber surveillance technologies, such as LI equipment, are operated at the level of (privately run) network operators.

92 "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation (March 21, 2017)," European Parliament.

93 Marietje Schaake, "Written Submission to the Public Online Consultation on the Export Control Policy Review (Regulation (EC) No 428/2009)," 2015, <http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_154004.pdf>.

In comparison to measures aimed at the convergence of the new catch-all, other provisions aimed at "leveling the playing field" in export licensing procedures are relatively uncontroversial and were welcomed by a broad range of actors. These include the development of a common IT infrastructure as a shared platform to support an enhanced exchange of information between export control authorities, an EU-wide capacity-building program and outreach efforts towards non-EU countries to disseminate best practices.[94,95,96] Licensing authorities also emphasized the weaknesses of the existing system, in which information sharing is mostly limited to authorization denials.[97] Access to information in other areas, such as granted licenses, critical destinations and end-users, incidents, and violations could help to improve national risk assessment procedures and harmonize outcomes. Sharing this export data has traditionally been difficult because of national and commercial interests but will be crucial to avoid disparate national policies that facilitate licensing avoidance and create loopholes in enforcement mechanisms for cyber-surveillance technologies.[98]

Overall, the Commission proposal represents a considerable improvement to the existing export control framework for cyber-surveillance technologies. In light of the cautionary remarks by Member State governments and industry groups, the Commission presented a surprisingly comprehensive and ambitious proposal. The changes to Regulation 428/2009 will now need to be agreed upon by the Member States and the European Parliament. One further issue to consider in this process is the need for greater transparency on export licensing decisions and outreach to affected entities, experts and civil society. Over the last years, many actors have pointed out that more reliable information and data on exports is needed to ensure that existing and future control measures are clear, effective, and consistent. The proposal falls short of calling on governments to publish comprehensive data concerning export license applications for surveillance technologies. Greater openness would encourage independent systematic research and contribute to accurate impact assessments, legal clarity, and better public understanding of the issue.

Conclusion: Chasing a Moving Target

It will always prove difficult to ensure that legislative processes keep up with technological developments, especially when it regards the internet. Advances in cyber-surveillance capabilities

---

94 The European Commission proposed an extension of information sharing through a catch-all database recording catch-all licensing requirements, end-users and items of concern.

95 A critical aspect is to address the lack of expertise and staff at both Member State and EU level, which undermines the effectiveness of existing controls on cyber surveillance technologies. The Commission has suggested setting up "technical expert groups" (Article 21) which bring together key industry and government experts into a dialogue on the technical parameters for controls. Creating a pool of experts to assist licensing authorities in the area of cyber surveillance technologies could be a meaningful first step in this direction. Capacity building can also promote a uniform approach and is used to contribute to international convergence of export controls beyond the EU.

96 Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," DG Trade, European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>, p. 2.

97 Interview with the author, Expert in the Federal Ministry of Economic Affairs and Energy.

98 Sibylle Bauer and Mark Bromley, "The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World," *EU Non-proliferation Paper* 48, SIPRI, March 2016.

have so far outstripped the ability of institutions of governance to modernize the control framework. The unregulated export of cyber-surveillance technologies has exposed individuals to new risks to their human rights and created security concerns. Laws and regulation currently chase a moving target.

On the European level, the outcome of the export policy review represents an ambitious response to the control challenge, magnifying the effect of existing control lists and licensing procedures and aiming at supplementing the existing framework with requirements specifically designed to oversee the export of cyber-surveillance technology. However, considering the actions of individual Member States that introduced additional controls on a national level, the Commission proposal should also be seen as a step towards leveling the European playing field. It is likely that the draft regulation will face some resistance by Member State governments and therefore might be subject to changes. Going forward, it will be up to the European Parliament, which has repeatedly shown its determination to improve the control regime on cyber-surveillance technology, to make sure that progress is not stymied and innovative steps not diluted.[99]

Further action at the EU and WA level does not guarantee that other key technology suppliers will introduce similar controls but certainly has the potential to limit the spread of some of the most contentious technologies and set an example for others. Arguments about the replaceability of European cyber-surveillance exports, potential circumvention or relocation opportunities, and distortions of competition should not preclude governments from enacting stricter controls on the EU or even national level. On the other hand, it remains true that an effective control regime should include as many countries as possible. Even with a new control system on the European level, a clear need will remain to coordinate with countries within the WA and beyond and especially key supplier countries should be approached with ideas to establish a broader regime. This could, for example, include Israel, which has a significant dual-use industry and made considerable progress in implementing export controls on cyber-surveillance technology.[100] In light of Brexit, it will also be crucial to ask whether UK export controls will remain compatible with EU controls and to institutionalize coordination arrangements.[101]

Working towards a broader regime would enjoy support by civil society and industry associations alike because it would address concerns about an uneven global playing field.[102] However, similar undertakings such as the multilateral Arms Trade Treaty show clear limitations of such attempts. Despite the agreement's focus on conventional weapons, products with a clear impact

---

99 Frans Timmermans, "Human Rights and Technology in Third Countries European," Speech to the European Parliament, September 7, 2015, <https://ec.europa.eu/digital-single-market/en/news/human-rights-and-technology-third-countries>; "Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," European Parliament, 2014/2232(INI), August 2015, <http://www.europarl.europa.eu/oeil/popups/summary.do?id=1401513&t=e&l=en>.

100 Doron Hindin, "Can Export Controls Tame Cyber Technology?: An Israeli Approach," *Lawfare Blog*, February 12, 2016, <https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach>.

101 Mark Bromley, "Brexit and Export Controls: Entering Uncharted Waters," SIPRI, 2016, <https://www.sipri.org/commentary/topical-backgrounder/2016/brexit-and-export-controls-entering-uncharted-waters>.

102 "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE, 2015, <https://privacyinternational.org/sites/default/files/CAUSE report v7.pdf>; and "DIGITALEUROPE Position Paper on the Review of Export Control Policy in the EU," DigitalEurope.

on security, stability, and human rights, negotiations were difficult and a significant number of states have not yet ratified the agreement. Regarding dual-use cyber-surveillance technologies, which are more ambiguous in terms of definitions and risks attached, international controls will be even more difficult.

Overall, policy-makers must be aware that trade restrictions on cyber-surveillance technology are not a panacea. Yet, subjecting these heterogeneous products and services to an export licensing regime can curb their unregulated spread and promote broader norms. Even when they are not invoked to restrict a transfer, export controls can act as an essential accountability and transparency mechanism, thus shedding light on this secretive trade and informing future regulatory responses. To be truly effective, export controls will need to be complemented by foreign policy initiatives that raise awareness of the problem, build a broader regime with common standards, and promote and protect human rights online and offline.