Tufts
UNIVERSITY
**Program on Science,
Technology, and Society**

Sam Weiss Evans
Assistant Research Professor

10 January 2019

Matthew S. Borman
Deputy Assistant Secretary of Commerce for Export Controls
Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Re: ANPRM on "Review of Controls for Certain Emerging Technologies", Docket BIS-2018-0024[1]

Dear Deputy Assistant Secretary Borman,

Thank you for the opportunity to comment on the interagency process to identify and define emerging technologies of security concern. These opportunities have historically had significant impact on the direction that the Department of Commerce takes on dual-use export control issues, and I hope that this Advanced Notice of Proposed Rule-Making (ANPRM) is no different (See Appendix 1 for a short history of prior ANPRMs related to emerging technology export controls).

I have been studying dual-use export controls, and specifically their role in addressing security concerns in research and emerging technology, for over a decade. Over that time, we have seen the coming and going of both the Deemed Export Advisory Committee and the Emerging Technology and Research Advisory Committee (ETRAC). As ETRAC's successor, the Emerging Technology Technical Advisory Committee (ETTAC), gets up and running, I hope that this comment may inform both its day-to-day operations and the interagency process of which ETTAC will be a part. The recommendations contained in this comment are designed to promote national security and international stability, while also making the work of ETTAC and the interagency process efficient. They are also designed to benefit businesses, academia, and the other government agencies with non-export control remits for security governance.

I begin my comment with three features of the environment within which ETTAC and the interagency process will work in the coming years and decades.

[1] Bureau of Industry and Security, Commerce. 2018. "Review of Controls for Certain Emerging Technologies." 83 FR 58201. Available at https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

1. Non-US capacity in developing emerging technology will continue to grow, including capacity outside of the multilateral Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.[2]
2. The strength of ETTAC, and through it the capacity of export controls to remain relevant and effective, will rely heavily on recognizing the limited applicability export controls have on emerging technology and the requirement that whatever controls are sought should be harmonized both with other governments and with other ways of governing security concerns.
3. Over the long term, the value of ETTAC and the interagency process will not be its capacity to impose export controls on emerging technology, but to identify potential security concerns in emerging technology and be a venue for debating how to understand those concerns, and therefore what should be the appropriate tool to govern them.

Below I provide both overarching recommendations, and specific recommendations related to the questions posed in the ANPRM. My three main recommendations concern the pace of export controls, the role of export controls in relation to other forms of governing security concerns, and the importance of transparency.

Recommendation 1. With up to four years between emerging technology identification and international harmonization, formal definition of emerging technology of security concern should only be done for the narrowest band of technology that the US can guarantee it will possess and other nations will not possess within that time frame.

The international harmonization process for export controls is a necessary component of any national export control system that wishes to add items of concern to its control lists that are available from foreign suppliers. Moreover, Section 1758(c)(1) of the Export Control Act of 2018 requires that "any technology identified [through this process] be added to the list of technologies controlled by the relevant multilateral export control regimes."

To get that international harmonization, however, is a long process. Because the Commerce Department is required to "establish appropriate controls under the Export Administration Regulations" that ETTAC and the interagency process identifies,[3] it is important to understand the amount of time likely to pass between the establishment of these unilateral controls and the harmonization of those changes in other countries' control lists.

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technology, the multilateral venue that is most active in dual-use export control harmonization and the likely place where the US will need to negotiate the definition for most technologies identified by ETTAC, takes at least a year to modify its lists.[4] Before that, proposals

[2] This has been argued for decades, as noted in NRC (National Research Council). 2005. *Avoiding Surprise in an Era of Global Technology Advances*. Washington, D.C.: National Academies Press. https://doi.org/10.17226/11286.
[3] Section 1758(b)(1) of the Export Control Act of 2018.
[4] For an analysis of the process at the multilateral level, see Evans, Samuel A W. 2014. *Revising Export Control Lists*. Brussels: Flemish Peace Institute. https://www.vlaamsvredesinstituut.eu/sites/vlaamsvredesinstituut.eu/files/files/reports/revising_export_control_lists_web.pdf. For a detailed analysis of the Wassenaar Arrangement process for modifying its Dual-Use List, see Evans, Samuel A. 2009. *Technological Ambiguity & the Wassenaar Arrangement*. DPhil Thesis. University of Oxford. Available at: https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.519768

must be developed in ETTAC and through an interagency process. After multilateral agreement, changes must then propagate to the national level lists, a process that, in the US, takes on average 8.5 months,[5] and in other states can vary between instantaneous and years.

Recommendation 2. **The US must develop security governance capabilities over emerging technology that are more attuned to the interconnected nature of global research and commerce than export controls are, and ETTAC is ideally placed as a forum for working out what those new capabilities might be, and how they will relate to export controls.**

ETTAC and the interagency process are invaluably situated to augment the government's capabilities in broad spectrum horizon scanning for security concerns and other risks from emerging technology, while balancing it with economic, academic, and other concerns. This capability has been significantly reduced since the shuttering of the Office of Technology Assessment in 1995. The Defense Intelligence Agency's Technology Warning Division appears to fulfill part of this mandate,[6] but there is no publicly available information on its current status, and its location within the intelligence community puts a hinderance on its public oversight and engagement with academia, industry, and foreign actors, as well as a commitment to balancing security concerns with other concerns in emerging technology.

ETTAC's charter allows for this forum capacity, as it states that "the committee's primary focus is the identification of emerging technologies with potential dual-use applications as early as possible in their developmental stages both within the United States and abroad."[7] Only secondarily is ETTAC tasked with, "advis[ing] BIS[8] regarding the potential impact of Export Administration Regulations (EAR) on research activities, technical and policy issues relating to controls under the EAR, revisions of the Control List…"[9] ETTAC, as a committee, is a direct descendent of the Deemed Export Advisory Committee (DEAC). The final report from the DEAC is seen as a pivotal moment in the use of export controls in governing security concerns in emerging technology. The main finding of the report was that

> the erection of high "walls" around large segments of the nation's science and engineering knowledge base has become not only increasingly impracticable, but that attempts to build such walls are likely to prove counterproductive—not only to America's commercial prowess but also, in balance, to America's ability to defend itself.[10]

[5] See Appendix 2 for analysis of the time between proposal development, multilateral negotiation, and implementation within the US Commerce Control List. In three of the last 5 years, Commerce has had to issue corrections to its original Wassenaar List implementations, which took closer to 18 months from the time they were agreed at Wassenaar, or 27 months since initial proposals were likely developed.

[6] NASEM (National Academies of Sciences, Engineering, and Medicine). 2005. *Avoiding Surprise in an Era of Global Technology Advances*. Washington, D.C.: National Academies Press. https://doi.org/10.17226/11286.

[7] ETTAC Charter, filed June 25, 2018. Available at https://tac.bis.doc.gov/index.php/documents/pdfs/370-ettac-bis-charter/file

[8] Department of Commerce's Bureau of Industry and Security, which is tasked with administering dual-use export controls.

[9] ETTAC Charter.

[10] Deemed Export Advisory Committee. 2007. *The Deemed Export Rule in the Era of Globalization.* Washington, DC: Department of Commerce. p.14.

If the call for developing more globally interconnected governance capabilities sounds familiar, it is because it echoes those of just about every National Academies and National Research Council report addressing export controls in the last two decades.[11]

The lack of a government, or even pseudo-governmental body tasked with being a forum for discussing the tension between academic, economic, and security concerns is a gap felt even more acutely after the unexpected shuttering of the FBI's National Security Higher Education Advisory Board (NSHEAB) earlier this year.[12] There are been many calls for such a body to be established on a permanent basis, citing particularly the issues around export controls, research, and emerging technology. This issue was at the heart of the proposed Science and Security Commission of the National Research Council 2007 report, *Science and Security in a Post 9/11 World*, and also at the heart of proposed Research Policy Board in the 2016 National Academies report, *Optimizing the Nation's Investment in Academic Research*. Until such a body is formed, ETTAC can at least lay the groundwork for its operation by acknowledging the limited—but vital—applicability of export controls as a useful form of governing security concerns in emerging technology and maintain the reasoning behind deciding that specific emerging technologies are or are not amenable to export control governance (Recommendation 7 below).

Export controls are a niche tool of security governance, and yet they have historically had a significant perceived impact on the flow of intangible technology since controls began in the late

[11] NASEM (National Academies of Sciences, Engineering, and Medicine). 2006. *Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future*. Washington, D.C.: National Academies Press. https://doi.org/10.17226/11463.
———. 2016. *Optimizing the Nation's Investment in Academic Research: A New Regulatory Framework for the 21st Century*. Washington, D.C.: National Academies Press. https://doi.org/10.17226/21824. Recommendation 12.3
———. 2017. *Dual Use Research of Concern in the Life Sciences: Current Issues and Controversies*. https://doi.org/10.17226/24761.
NRC (National Research Council). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: National Academy Press. https://doi.org/10.17226/10415.
———. 2004. *Biotechnology Research in an Age of Terrorism : Confronting the Dual Use Dilemma*. Washington, DC: National Academies Press. https://www.nap.edu/catalog/10827/biotechnology-research-in-an-age-of-terrorism.
———. 2005. *Avoiding Surprise in an Era of Global Technology Advances*. Washington, D.C.: National Academies Press. https://doi.org/10.17226/11286.
———. 2007. *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities*. Washington, D.C.: National Academies Press. http://www.nap.edu/catalog/12013.html.
———. 2009. *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World*. Washington, D.C.: National Academies Press. https://doi.org/10.17226/12567.
———. 2012. *Export Control Challenges Associated with Securing the Homeland*. Washington, D.C.: National Academies Press. https://doi.org/10.17226/13369.
NRC (National Research Council), and AAAS (American Association for the Advancement of Science). 2009. *A Survey of Attitudes and Actions on Dual Use Research in the Life Sciences / Committee on Assessing Fundamental Attitudes of Life Scientists as a Basis for Biosecurity Education*. Washington, D.C.: The National Academies Press. http://www.nap.edu/catalog.php?record_id=12460.

[12] Smith, Lamar and Clay Higgins. 2018. "Scholars or Spies?" *Inside Higher Education.* June 26. Available at https://www.insidehighered.com/views/2018/06/26/universities-must-take-steps-protect-american-rd-foreign-agents-opinion. On the NSHEAB, and in particular the important and tenuous role in it played by its chair, Graham Spanier, see Golden, Daniel. 2017. "The CIA's Favorite College President: How the CIA Secretly Exploits Higher Education." *The Chronicle of Higher Education; Washington*, October. https://search.proquest.com/docview/1968452262/abstract/AC12527F56E04BF4PQ/1.

1970s.[13] This perceived impact has been argued to be a good thing, if one is looking at the security gains assumed from such control. It has also, however, been argued to be a bad thing, if one is looking at the undue burden controls are assumed to place on economic and academic research and development. This back and forth on the appropriateness of export controls as a tool to govern security concerns in intangible technology transfer has been going on for decades, with several key moments that have defined the debate: the "fundamental research" exclusion codified in National Security Decision Directive 189 in 1985;[14] the concerns over in-country transfer of intangible technology to foreign nationals which lead to the establishment of the Deemed Export Advisory Committee in 2006 and subsequently to the ETRAC; and the current establishment of ETTAC.[15]

While differences between perceived and actual impact are very hard to measure (and has been a continual point of contention within export controls generally), what is not as disputed is that there are many goods and technologies that might be considered security concerns, but are not amenable to export controls because they do not meet a wide range of requirements, like lack of foreign availability.[16] Understanding the continued relevance of export controls in this space requires further criteria (Recommendation 10).

Developing a capacity to acknowledge and address the security importance even of those technologies that do not seem amenable to export control solutions allows for both the streamlining of export controls—a goal of the last decade of export control reform—and the development of novel governance tools that may be better suited to an interconnected world where much dual-use technology is in the hands of non-state actors and multiple generations of advances can happen in the span of time required to harmonize multilateral export control lists. Both these missions would be advanced if there were a clear governmental focal point for identifying and assessing the security implications of emerging and foundational technologies. ETTAC can serve this purpose.

Recommendation 3. The methodology of ETTAC and the interagency process should be open to public scrutiny, even though the application of any particular instance of that methodology will likely be restricted for national security and proprietary reasons.

Defining any good or technology such that it is able to be caught within an export control system is central to the functioning of that system, and yet the process itself is rarely a point of open debate. As noted to me by an export control official with decades of experience in administration:

> Let's get rid of this idea that we won't talk about what we do [in modifying export control lists]. I mean, information exchange—sensitive government information—Hell, you've got to keep that secret. But how we do what we do, and why we do what we do, is not a secret.[17]

[13] Evans, Samuel A. 2009. *Technological Ambiguity & the Wassenaar Arrangement*. DPhil Thesis. University of Oxford. p. 279-322.

[14] https://fas.org/irp/offdocs/nsdd/nsdd-189.htm

[15] Evans, Samuel A. W., and Walter D. Valdivia. 2012. "Export Controls and the Tensions Between Academic Freedom and National Security." *Minerva* 50 (2): 169–90. https://doi.org/10.1007/s11024-012-9196-4.

[16] https://www.wassenaar.org/app/uploads/2015/06/Criteria_for_selection_du_sl_vsl.pdf

[17] Interview with British Government Official A & British Government Official B, 9 February 2006.

ETRAC had never publicly enunciated any method by which it identified or defined emerging technology, nor is there any description of a method upon which the government will be iterating using the comments provided in this ANPRM. Transparency about methodology provides assurances to industry, clarity to the people involved in the process, and the capacity for public debate about its appropriateness, which currently does not exist. Public comment on this methodology is required through Section 1758(a)(2)(C) of the Export Control Act of 2018 and is the function of this ANPRM.

ETTAC should make its methodology a point of public discussion in the open sessions of its quarterly meetings,[18] and specifically seek out and incorporate advice from experts in horizon scanning and other assessment methodologies in refining its own process. This is in line with several recommendations from the 2016 National Academies report *Optimizing the Nation's Investment in Academic Research: A New Regulatory Framework for the 21st Century*, as well as the Deemed Export Advisory Committee report.[19]

Specific comments

1) How to define emerging technology to assist identification of such technology in the future

It is unclear from this question whether Commerce is seeking help on defining the concept of 'emerging technology' or defining specific emerging technologies. These are two very important questions, both of which deserve an answer.

Defining the Concept of Emerging Technology

Any definition of the concept of 'emerging technology' is extremely problematic, because there will always be technologies which are of interest but fall outside of the definition. That said, a useful working definition may be something like, "any technology with a potential to disrupt the status quo that has not yet been used successfully." For ETTAC, it might be useful to specifically be looking for technologies that are outside of the scope of other TACs, which would require ETTAC to consult with the other TACs on how they define the scope of their remit.

Defining Specific Emerging Technologies

There is an extremely important differentiation between the identification and definition of emerging technologies of security concern that the ANPRM makes, which is not made within the Export Control Act of 2018 (ECA) Section 1758, which only denotes the need to "identify emerging and foundational technologies...[for which] the Secretary shall establish appropriate controls." The ANPRM, on contrast, talks about both "identifying and describing" or "defining and identifying" emerging technologies. This difference in language brings up a very important feature of work that needs to be done in ETTAC and the interagency process.

[18] ETTAC is required to meet at least once every 120 days.

[19] E.g. Recommendation 11.3, 12.2 and 12.3 of National Academy of Sciences. 2016. *Optimizing the Nation's Investment in Academic Research: A New Regulatory Framework for the 21st Century*. Washington, DC: National Academies Press. Deemed Export Advisory Committee. 2007. *The Deemed Export Rule in the Era of Globalization.* Washington, DC: Department of Commerce.

<u>Recommendation 4.</u> ETTAC and the interagency process should have clear stages before formal export control definition construction where alternatives to export controls can be employed.

The ANPRM notes that, "Certain technologies, however, may not yet be listed on the CCL [Commerce Control List] or controlled multilaterally because they are emerging technologies. As such, they have not yet been evaluated for their national security impacts." *These two sentences are at the heart of the problem of defining emerging technology within an export control framework.* The uncertainties and ambiguities around emerging technology make them difficult if not impossible to govern from an export control perspective, and yet this is exactly what the process to be established through this ANPRM is tasked to do.

What the difference between the ECA text and the ANPRM text point out is that there are different zones of work needed to a) understand technical capacities which are developing that have unknown security concern, b) decide whether export controls are an appropriate governance tool for particular technologies of concern and c) craft a specific definition of an item of concern for an export control list. **When the ECA says that a technology is 'identified', I am reading that as "explicitly defined for the purposes of export controls."** In contrast, the ANPRM points to the need to also address the other zones of work in export controls, and security governance more generally.

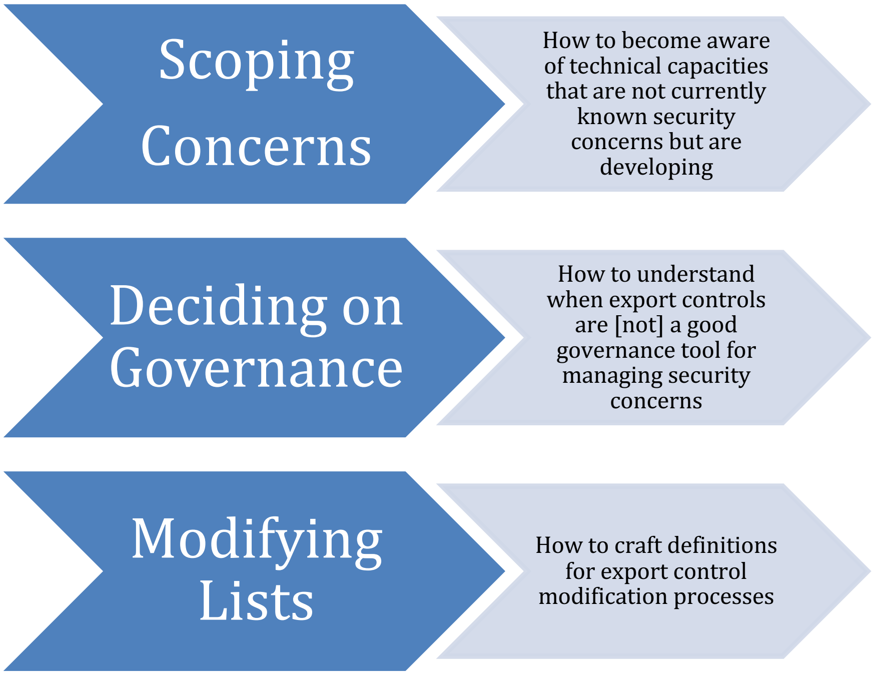

Scoping Concerns
How to become aware of technical capacities that are not currently known security concerns but are developing
Deciding on Governance
How to understand when export controls are [not] a good governance tool for managing security concerns
Modifying Lists
How to craft definitions for export control modification processes

Figure 1 - Zones of work in governing security concerns of emerging technology

(a) Scoping Concerns

Recommendation 5. Horizon-scanning or other future visioning should be focused on functional capabilities of concern, in addition to specific technical categories.

The way that the ANPRM is laid out is tightly bound with first scoping technical categories of concern, and then focusing on particular technologies within those categories to create definitions for export control lists.

I encourage ETTAC and the interagency process to not be bound by a particular technical category but instead focus on functional capabilities that might warrant increased security attention, and only then focus on a specific technology that can provide those functional capabilities.

If some means of achieving the sensitive functional capabilities are amenable to export controls but others are not, export controls on the controllable technologies and items may not accomplish the desired security objective.

In some cases, an emerging technology can offer a functional capability that had not previously been considered, motivating a search across technologies. In such cases, it would be the objective of the horizon-scanning process to be sensitive to new technologies that offer such new functional capabilities. However, when such new technology-driven capabilities are uncovered, further analysis should be based on that new capability, and not restricted to that originally identified technology.

(b) Deciding on Governance

Recommendation 6. ETTAC should be seen as a place to understand the security governance landscape for emerging technology broadly, and therefore reshape what an 'export control' is in the 21st Century.

The majority of list modification questions in export controls begin after it is decided or assumed that export controls are an adequate tool to govern the security concerns of a technology. On the one hand, this make sense, as the list modification process is export control-based. But how do we, or the institutions that we work within, decide when we should use export controls and not another governance tool? The question becomes ever-more important the further we tread into the spaces of technology where the assumptions export controls make are increasingly contentious.

ETTAC is very much in this contentious space. This is its strength as well as its weakness, and the recommendations ETTAC makes in deciding what should fall into and out of the realm of export controls will depend on whether ETTAC sees itself as solely concerned about export controls or more concerned about the place of export controls within a wider governance system. I strongly recommend that ETTAC take the latter approach.

Part of what this approach can do is point out the need for new ways to organize the category structure of the export control lists themselves. This may seem like a mammoth task to people in the export control business, but it is something that has happened before: the 1990-1991 Core

List revision of the Coordinating Committee for Multilateral Export Controls (CoCom).[20] This revision process removed categories that had been in place for over 70 years, and there is no reason to not think it might be time again to revisit export controls at this very high level. ETTAC is an ideal place where this kind of high-level awareness and debate can start.

Recommendation 7. ETTAC and the interagency process should include significant attention to how to manage technologies that are considered not amenable to control through export controls.

It may seem counterintuitive to focus on what will not be caught through this process, but it is vital that ETTAC and the interagency have a plan for how to deal with technologies that are not visible to export controls *but may still be considered security concerns within other governance mechanisms.* Say, for example, that desktop synthesis of synthetic DNA is something that ETTAC considers but ultimately rejects as a security concern within the confines of export controls. This does not mean that desktop synthesis is not of concern at all to the United States. Knowledge of both the reasons why export controls cannot apply and why a state might still be concerned about the technology could be of significant use to other governing processes within the state. To continue with this example, a decision on the non-controllability of desktop synthesis could be used as evidence by the FBI's Biological Countermeasures Unit of the need to further strengthen community networks of norm and information sharing within biology to identify aberrant behavior in the use of desktop synthesis.

In addition to offering the potential for the development of non-export control governance mechanisms that may apply to these other technologies, it is also important to address non-export-controllable technologies in case any of them can accomplish the same objectives as export-controlled ones.

Recommendation 8. As technologies in the residual category of emerging technology of security concern that are not amenable to export controls grow, the interagency process should be used to publicly debate how to govern them appropriately.

Export controls are a blunt tool of security governance, initially designed for the control of the international transfer of tangible items of use to a foreign military, and gradually expanded over the years to cover more intangible aspects, such as software and technology, which could be used by non-state actors like terrorist groups. Its roots are really in an age when an export was a cargo net of stuff being put on a sailing ship that might be sent to a belligerent state in a time of war, rather than a computer in someone's home connected to a continuous global stream of data.

The interagency process should be considered firstly a forum for discussing the different ways an area of emerging technology may be seen as a security concern, and only secondly whether export controls are the most effective tool to use to govern those security concerns. This will have at least two benefits: the process will keep export controls in conversation with the wider range of governance tools a state has at hand to address security concerns in technology; and it will ensure that export controls are pursued only for those technologies for which they are optimally suited.

[20] Evans, Samuel A. 2009. *Technological Ambiguity & the Wassenaar Arrangement.* DPhil Thesis. University of Oxford. p. 167-184.

It is entirely likely that, over the course of several years of work by ETTAC and the interagency process, the residual category will grow, and there will be no current governance tools that seem appropriate to use to address the security concerns of technologies in it. Having documentation on what these technologies are and the reasons why export controls are not appropriate for them will greatly aid in the construction of more appropriate governance tools. To continue with the desktop synthesis example, while control of the tangible synthesizers may not be possible, ETTAC discussions may identify a possible role that international genetic code repositories could take on in controlling access to specific DNA segments. This is well outside the scope of export controls, but having documentation of this discussion could be very useful in making the case, either by the interagency process or another unit, of the need for, e.g., harmonization of information sharing about access requests across public and private genetic code repositories globally.

An already-existing body with which ETTAC may share this residual category is the National Academy of Sciences *Intelligence Community Studies Board*.[21]

(c) The Definition Process to Modify the Lists

<u>Recommendation 9.</u> ETTAC should embrace, rather than shun the political nature of the work it is trying to do, even in the definition process. This will enable it to get national and international support for the definitions it proposes.

The content of a definition has little to do with specific characteristics of items under consideration, and much to do with the political, economic, strategic, and organizational context within which the definition process happens. This is clearly shown in Appendix 3, where I show how the process of creating the current control text for "quantum cryptography" was more about managing information hazards and the politics of Wassenaar's *Security and Intelligence Experts Subgroup* as it was about any technical parameters of quantum cryptography. And in the end, the definition of "quantum cryptography" we currently have does not have any technical parameters at all!

Every item on the Wassenaar Arrangement Dual-Use list has a similar history, and while I have only examined some of them (mainly computing and night vision, in addition to quantum cryptography),[22] understanding the politics, economics, and other reasons for wanting to define items one way or another has been essential to the success of all proposed list changes, whether contentious or not.

While historically export controls have sought to separate technical and political discussions in the process of modifying export control lists,[23] ETTAC sits within the contentious space where agreement is not readily achieved on whether export controls are even the most appropriate

[21] http://sites.nationalacademies.org/DEPS/icsb/

[22] Evans, Samuel A. 2009. *Technological Ambiguity & the Wassenaar Arrangement*. DPhil Thesis. University of Oxford. Deliberation histories are maintained by the Wassenaar Secretariat, and any Participating State can request access to particular deliberation records in the process of developing proposals for changing the lists. Moreover, the Secretariat itself provides those histories for each proposal once submitted to the Arrangement by a Participating State.

[23] The Wassenaar Arrangement, for example, does this by having an Experts Group and a General Working Group.

mechanism for governing security concerns. It is appropriate to assume, then, that the rare cases when a definition process should be initiated will be politically and socially charged.

Embracing the social nature of definition-making means recognizing that any definition will be the result of negotiation between many concerns, not just security. Other types of concerns include:

- Economic: Crafting definitions is often about deciding how to *not* include goods or technologies that companies within a state produce. Arguing for security being the only concern that should matter not only closes off debate, thereby preventing any decision, but also creates ill will between those who want control and those who will be affected by controls. This is exactly what happened when negotiating controls on night vision components in the early 2000s at Wassenaar.[24]
- Scientific: These concerns will likely come up both in deemed export discussions and when debating the line between fundamental research and emerging technology.[25]
- Organizational: All of the categories in the Commerce Control List (CCL) are permeable. There is even permeability between the CCL and the Munitions list, as is noted by the fact that the Wassenaar Arrangement maintains a Correspondence List, which is a list of items on the Dual-Use List and the Munitions List with similar functionality.[26] Some technologies may be able to fit into multiple categories, and the technologies within any of the categories may have very little to do with one another. Decisions about where to put a definition, therefore, are not just technical. This is doubly true for the construction of new categories.[27]
- Political: even with the best of intentions, some years are bad for changing lists because of tensions at the international level. If it's likely those tensions will be around during the period when export controls on a technology make sense, then it may be best to put energy into non-export control options to govern the security concern.

By recognizing these other concerns as well, ETTAC can open up possibilities for negotiating definitions in ways that build support for the final definition, rather than antagonize those groups who prioritize non-security concerns and whose support is necessary for an effective export control system.

Therefore, the significant uncertainties and ambiguities that are present in emerging technologies can actually be a source of reconciliation between security and non-security concerns as our security governance system evolves.

[24] Evans, Samuel A. 2009. *Technological Ambiguity & the Wassenaar Arrangement*. DPhil Thesis. University of Oxford. Available at: https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.519768. P. 220-246.

[25] Evans, Samuel A. W., and Walter D. Valdivia. 2012. "Export Controls and the Tensions Between Academic Freedom and National Security." *Minerva* 50 (2): 169–90.

[26] Evans, Samuel A. 2009. *Technological Ambiguity & the Wassenaar Arrangement*. DPhil Thesis. University of Oxford. Appendix H.

[27] As an example, Category 6 'Sensors and Lasers', of the Wassenaar Arrangement Dual-Use List was created in Wassenaar's predecessor, CoCom, in the Core List revision process of 1990-1991. It is a combination of items from across the old CoCom Lists, including Groups F & G 'Electronic equipment including communications, radar, computer hardware and software' (the 1500s), Group C 'Electrical and power generating equipment' (the 1200s), Group D 'General industrial equipment' (the 1300s), and Group I 'Chemicals, metalloids, and petroleum products' (the 1700s). For electronic versions of CoCom's lists, see https://evansresearch.org/cocom-lists/.

2) Criteria to apply to determine whether there are specific technologies within these general categories that are important to U.S. national security

Recommendation 10. In determining whether specific technologies are a) important to national security and b) amenable to export controls, criteria must go beyond the Wassenaar Arrangement *Criteria for the Selection of Dual-Use Items* to include considerations of whether export controls are the most appropriate tool, and the time sensitivity of list modifications.

Building on the last Recommendation, criteria must go beyond the Wassenaar Arrangement *Criteria for the Selection of Dual-Use Items*:[28]

- Foreign availability outside Participating States.
- The ability to control effectively the export of the goods.
- The ability to make a clear and objective specification of the item.
- Controlled by another regime.

Additional criteria that should be considered include:

- **An analysis of the relative benefits of export control over other governance tools that might also be used**: this criteria would explicitly require ETTAC to make the case that export control is the *best* tool available, instead of just using export control it is the most *familiar* tool.
- **The lack of any other appropriate governing tool**: if export control is a tool of last resort in governing security concerns in emerging technology, as happened when it was employed to stop publication of research on avian influenza in 2011,[29] this exceptional occurrence should be extremely temporary, while other governing capabilities are developed.
- **The ability to get control text agreed at the multilateral level and incorporated in foreign government systems in a timely manner** (Recommendation 1): this is, in a way, a combination of all three of the Wassenaar criteria above, but places a specific emphasis on the temporality of controls.

Recommendation 11. Since control text at this early stage of development is likely to be technology-based rather than parameter-based, proposals which come out of ETTAC and the interagency process should always include sunset clauses (also known as 'validity notes').

There is currently much discussion and action on making export control lists, especially dual-use lists, into more 'positive' lists, where controlled items are described using specific parameters, as opposed to general descriptions. Examples of general descriptions can be found throughout the United States Munitions List.[30] Items are grouped in broad categories, such as 'ground vehicles', 'vessels (surface or underwater)', or 'electronic equipment' that are 'specially designed for

[28] https://www.wassenaar.org/app/uploads/2015/06/Criteria_for_selection_du_sl_vsl.pdf

[29] Evans, Samuel A. W., and Walter D. Valdivia. 2012. "Export Controls and the Tensions Between Academic Freedom and National Security." *Minerva* 50 (2): 169–90.

[30] 22 CFR §121.1. Available at https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.121

military use'. This is in contrast to what can be considered a very 'positive' approach to controlling dual-use night vision goods by defining specific components to control, such as a "Non-'space-qualified' non-linear (2dimensional) infrared 'focal plane arrays' based on 'microbolometer' material having individual elements with an unfiltered response in the wavelength range equal to or exceeding 8,000 nm but not exceeding 14,000 nm."[31]

A positive list is considered more transparent than a broad list, but this transparency works both for and against the goal of ensuring security. In areas of emerging technology, early-stage control texts are likely to be more general, both because the specific parameters are not yet known, and because giving away known parameters at this stage is tantamount to exporting the technology itself. We have already seen this in the development of the current control text for 'quantum cryptography' (see Appendix 3).

As a result, as the technology moves from emerging to emerged, the control texts will need to be revisited. To enable this to happen fluidly, all proposals originating from ETTAC should include sunset clauses on the proposed text, such that the EAR and the multilateral lists will have to be reviewed within a set time, otherwise the controls cease. This will likely go a long way in easing tensions with businesses that are developing these technologies.

3) Sources to identify such technologies

Recommendation 12. ETTAC should develop extensive public outreach and engagement to raise its visibility as a forum for debating how to govern security concerns in emerging technology. This will establish it as a place where people developing technology can bring their concerns without fear of immediate export control restrictions being in place.

Major sources for very early stage identification of security concerns in emerging technology will likely come for those developing the technology. These groups are likely to be of any size, from multinational organizations to government departments to individuals working in their homes. The Technical Advisory Group structure currently in place in Commerce primarily reaches the large corporations and government departments, and much more effort needs to be given to engaging those outside of this remit who are developing technologies which might be of security concern.

An example to learn from is the FBI's Biological Countermeasures Unit, which over the past ten years has developed extensive capacities to listen to researchers without that interaction turning into a formal inquiry. As a result, they are approached more frequently about novel developments within biology that might be of security concern, often long before journal articles have even been written.

Another place in government that ETTAC might look include the *Intelligence Community Studies Board* within the National Academies of Sciences, which is doing many similar horizon-scanning and assessment processes. They have recent or forthcoming reports on robotics and

[31] This text is found on the Wassenaar Dual-Use List, item 6.A.2.a.3.f.

artificial intelligence,[32] and on quantum computing,[33] and have also conducted workshops on quantum sensing[34] and identifying and understanding emerging breakthroughs in science and technology.[35]

The GAO and National Intelligence Council are also places to look for regular reports on emerging technology and horizon scanning.[36] That the recent GAO report on *National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies* didn't even think to reach out to the Commerce Department as an agency with a national security role in emerging technology speaks to the need for ETTAC to have broad outreach and public visibility, so that people know to include it in discussions on emerging technology.

4) Other general technology categories that warrant review to identify emerging technology that are important to U.S. national security

<u>Recommendation 13.</u> Focus on technology that is not currently advancing, as well as that which is advancing.

The list of categories that was included in the ANPRM reads like the top 20 pop hits of emerging technology. While these categories should certainly be subject to review from a security perspective (at some point), if the ETTAC and interagency process wants to think about the future categories, they should be looking towards areas that are not currently advancing, which, if they were, might produce functional advances that warrant them becoming a concern. This can be achieved, in part, by first focusing on functional capabilities of concern, rather than specific technical categories (Recommendation 5).

5) The status of development of these technologies in the United States and other countries

No Comment.

6) The impact specific emerging technology controls would have on U.S. technological leadership

No Comment.

[32] http://sites.nationalacademies.org/PGA/step/PGA_177034

[33] http://sites.nationalacademies.org/CSTB/CurrentProjects/CSTB_173986

[34] http://sites.nationalacademies.org/DEPS/icsb/DEPS_187931

[35] http://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_175778.pdf

[36] NIC (National Intelligence Council). 2017. "Global Trends: Paradox of Progress." NIC 2017-001. Washington, D.C. https://www.dni.gov/index.php/global-trends-home. Previous Global Trends reports can be found here: https://www.dni.gov/index.php/digital-extras/previous-reports
GAO (Government Accountability Office). 2018. "National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies." GAO-19-204SP. Washington, D.C. https://www.gao.gov/products/GAO-19-204SP.

7) Any other approaches to the issue of identifying emerging technologies important to U.S. national security, including the stage of development or maturity level that would warrant consideration for export control.

No Comment.

Acknowledgements

This comment was made possible in part due to my position as CRASSH Visiting Fellow in Cambridge University's Centre for the Study of Existential Risk (CSER), and with the support of a grant from Templeton World Charity Foundation, Inc. The opinions expressed in this publication are those of the author and do not necessarily reflect the views of Templeton World Charity Foundation, Inc.

Appendix 1

A short history of prior ANPRMs related to emerging technology export controls

Deemed Export Advisory Committee

In 2004, the Office of the Inspector General of the Department of Commerce recommended expanding the control of 'deemed exports'—in-country intangible technology transfers of export controlled items to foreign nationals—by changing a single word in the definition of information for the 'use' of controlled technology within the Export Administration Regulations (EAR).[37] The definition comprises six components (operation, installation, maintenance, repair, overhaul, refurbishing) which are connected by an 'and' conjunction. The Inspector General recommended changing this to an 'and/or' conjunction. Such a change would cause a dramatic shift in the license exceptions for 'use' of controlled technology, and an export license would be required for the in-country transfer of information (the intangible aspects of the technology) connected with any of the six components of 'use', instead of only information pertinent to all six components. A company or academic institution engaged in fundamental research with foreign nationals, and using export controlled equipment, would then be required to obtain an export license for every foreign national working on any piece of equipment if that foreign national's work satisfied any of the 'use' criterion, instead of all of them. The justification of such a change was simply to close a loophole in the control system:

> Other academic representatives we met with contend that in the context of fundamental research, technology relating to the 'use' of controlled equipment is also exempt under the EAR fundamental research exemption. However, according to BIS, technology relating to controlled equipment—regardless of how 'use' is defined—is subject to the deemed export provisions even if the research being conducted with that equipment is fundamental (p. 15).

In addition to modifying the definition, the Inspector General said that industry and academic institutions should only be notified after the modification had taken place. The Department of Commerce, however, decided to solicit comments on the recommendation before it was implemented,[38] as is common policy when the Department believes these communities might be significantly affected by the change. There was significant outcry from the academic and industrial communities, with the Department receiving 310 replies,[39] mostly pointing out that "the 'or' interpretation would capture too many routine operations carried out by foreign national students and employees, and that the proposed rules would constitute a large (and, it was asserted, generally unnecessary) compliance burden on affected organizations."[40] The

[37] OIG (Office of the Inspector General). 2004. *Deemed Export Controls May Not Stop the Transfer of Sensitive Technology to Foreign Nationals in the US*. US Department of Commerce. http://www.oig.doc.gov/oig/reports/2004/BIS-IPE-16176-03-2004.pdf.

[38] Bureau of Industry and Security, Commerce. 2005. "Revisions and Clarification of Deemed Export Related Regulatory Requirements." 70 FR 15607. Docket No. 050316075-5075-01.

[39] All replies are available at https://efoia.bis.doc.gov/index.php/documents/public-comments/724-advance-notice-of-proposed-rulemaking/file

[40] Deemed Export Advisory Committee. 2007. *The deemed export rule in an era of globalization*. A Report to the Secretary of Commerce. Available at https://fas.org/sgp/library/deemedexports.pdf. Hereafter referred to as the "DEAC Report".

Department of Commerce's Bureau of Industry & Security actually worked through these comments and decided on two courses of action. The first was not to adopt the recommendation of the Inspector General.[41] The second was to establish the Deemed Export Advisory Committee (DEAC) in May 2006 in order to come up with recommendations on how to improve the regulations on deemed exports.[42]

Emerging Technology and Research Advisory Committee

After the DEAC Report came out, the Department of Commerce once again requested public input on its recommendations and the Departments planned response, including the formation of the Emerging Technology Research Advisory Committee (ETRAC), the predecessor to ETTAC.[43]

[41] Bureau of Industry and Security, Commerce. 2006. "Revisions and Clarification of Deemed Export Related Regulatory Requirements." 71 FR 20840. Docket No. 050316075-6122-03.

[42] For the Charter of the DEAC, see Appendix B of the DEAC Report in note 40.

[43] Bureau of Industry and Security, Commerce. 2008. "Request for Public Comments on Deemed Export Advisory Committee Recommendations: Narrowing the Scope of Technologies on the Commerce Control List Subject to Deemed Export Licensing Requirements and Implementing a More Comprehensive Set of Criteria for Assessing Probable Country Affiliation for Foreign Nationals." 73 FR 28795. Docket No. 080512652-8653-01. The 22 comments submitted to this request are available at https://efoia.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=734&Itemid=526

Appendix 2

Time between multilateral proposal development and implementation in US export controls of list changes for the last decade

This table shows the average time it would take if a proposal was approved in the first year that it was debated within the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, the location where most export control list modifications happen, and the most likely place for multilateral debate on proposals that might originate within ETTAC. A few caveats:

- While I assumed that proposals would begin development in January of the year they are submitted to Wassenaar, there is very little if any public data on the deliberation time within a country before submission to Wassenaar. Proposals are usually uploaded onto Wassenaar's secure data information system in March, so that other countries can have time to review them before the first Expert Group meeting in June.[44]
- Wassenaar receives about 60 proposals per year.[45]
- The process for contentious proposals often spans several years, and it is likely that a disproportionate number of proposals originating in ETTAC will be contentious, because they are likely to be very close to what other states may consider to be fundamental research. Section1758(c)(2) of the Export Control Act of 2018 states that, if a proposal is not successful within three years, "the applicable agency head may determine whether national security concerns warrant the continuation of unilateral export controls with respect to that technology."
- I have included the date of US implementation of changed multilateral text, but it is important to note that it is possible the US will have already implemented unilateral controls on the technology while it is being debated within Wassenaar.
- The changed Wassenaar Dual-Use lists are usually published at the conclusion of the annual Plenary meeting, which is usually held the first week in December.

[44] Evans, Samuel A W. 2014. *Revising Export Control Lists*. Brussels: Flemish Peace Institute. p. 38.

[45] Interview with Wassenaar Secretariat Official, 13 June 2007 and Interview with British Former Government Official, 8 March 2007.

Proposals developed for Wassenaar	Changes incorporated into Wassenaar Lists	Changes incorporated into US lists	Difference
January 2017	December 2017	October 24, 2018[46]	~22 months
January 2016	December 2016, Corrected February 2017	August 15, 2017[47]	~19 months
January 2015	December 2015, Corrected April 2016	September 20, 2016[48], corrected June 14, 2017[49]	~21 months (~29 months for corrected version)
January 2014	December 2014, Corrected March 2015	May 21, 2015,[50] corrected December 3, 2015[51]	~17 months (~23 months for corrected version)
January 2013	December 2013	August 4, 2014,[52] corrected May 20, 2015[53]	~19 months (~29 months for corrected version
January 2012	December 2012	June 20, 2013[54]	~18 months
January 2011	December 2011, Corrected February 2012	July 2, 2012[55]	~18 months
January 2010	December 2010	May 20, 2011[56]	~17 months
January 2009	December 2009	September 7, 2010[57]	~20 months
January 2008	December 2008	December 11, 2009[58]	~23 months
Average time between beginning proposal development and implementation of changed controls within CCL			~19 months (~27 months for corrected versions)

[46] Bureau of Industry and Security, Commerce. 2018. "Wassenaar Arrangement 2017 Plenary Agreements Implementation." 83 FR 53742.

[47] Bureau of Industry and Security, Commerce. 2017. "Wassenaar Arrangement 2016 Plenary Agreements Implementation." 82 FR 38764

[48] Bureau of Industry and Security, Commerce. 2016. "Wassenaar Arrangement 2015 Plenary Agreements Implementation, Removal of Foreign National Review Requirements, and Information Security Updates." 81 FR 64655

[49] Bureau of Industry and Security, Commerce. 2017. "Wassenaar Arrangement 2015 Plenary Agreements Implementation, Removal of Foreign National Review Requirements, and Information Security Updates; Corrections." 82 FR 27108

[50] Bureau of Industry and Security, Commerce. 2015. "Wassenaar Arrangement 2014 Plenary Agreements Implementation and Country Policy Amendments." 80 FR 29431

[51] Bureau of Industry and Security, Commerce. 2015. "Wassenaar Arrangement 2014 Plenary Agreements Implementation and Country Policy Amendments; Correction." 80 FR 75633

[52] Bureau of Industry and Security, Commerce. 2014. "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Commerce Control List, Definitions, and Reports; and Extension of Fly-by-Wire Technology and Software Controls." 79 FR 45287

[53] Bureau of Industry and Security, Commerce. 2015. "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items." 80 FR 28853

[54] Bureau of Industry and Security, Commerce. 2013. "Wassenaar Arrangement 2012 Plenary Agreements Implementation: Commerce Control List, Definitions, and Reports." 78 FR 37371

[55] Bureau of Industry and Security, Commerce. 2012. "Wassenaar Arrangement 2011 Plenary Agreements Implementation: Commerce Control List, Definitions, New Participating State (Mexico) and Reports." 77 FR 39353

[56] Bureau of Industry and Security, Commerce. 2011. "Wassenaar Arrangement 2010 Plenary Agreements Implementation: Commerce Control List, Definitions, Reports." 76 FR 29609

[57] Bureau of Industry and Security, Commerce. 2010. "Wassenaar Arrangement 2009 Plenary Agreements Implementation: Categories 1, 2, 3, 4, 5 Part I, 6, 7, and 9 of the Commerce Control List, Definitions, Reports." 75 FR 54271

[58] Bureau of Industry and Security, Commerce. 2009. "Wassenaar Arrangement 2008 Plenary Agreements Implementation: Categories 1, 2, 3, 4, 5 Parts I and II, 6, 7, 8 and 9 of the Commerce Control List, Definitions, Reports." 74 FR 65999

Appendix 3

Analysis of the development of multilateral export controls on quantum cryptography[59]

In 2004, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies debated whether and how to add quantum cryptographic technology to its Dual-Use List. As 'quantum encryption' is one of the categories (7)(ii) in the ANPRM that the Department of Commerce requested feedback on, this Appendix provides an analysis of how the current control text for quantum cryptography was developed, and thus serves as a useful case study for the complexity of creating definitions of emerging technology.

Background

Almost all of the ciphers that have been created to date are susceptible to some form of cryptanalysis; that is, they can be cracked. There is at least one cipher, however, that is theoretically uncrackable without the key, and it is this cipher that is used in quantum cryptography. It is called the 'one-time pad' and was developed by Gilbert Vernam around 1919[60] and proved uncrackable by Claude Shannon.[61] This cipher depends entirely on the secrecy of the key, which has to be changed after every message. The difficulty of securely transmitting a key between the sender and receiver has meant this cipher has been used relatively little, except for situations where the highest levels of secrecy were demanded.

The difficulty of key transfer is what quantum cryptography claims to overcome.[62] Quantum cryptography is therefore more usefully called 'quantum key distribution' (QKD). If Alice is able to give Bob a key in such a way that she knows if anyone has looked at it during the transfer (thus compromising it), then she can use the key as a one-time pad cipher and can securely transfer information to Bob knowing that the mathematical properties of the one-time pad ensure that no one can crack her cipher text. The properties of quantum bits, or 'qubits', allow the key exchange to occur in such a way that, in theory, any eavesdropping can be detected. Knowledge of this theoretical capability gave quantum cryptography a lot of public attention and a fair degree of sensationalization in the early 2000s.[63]

In the early 2000s, there are at least three companies that claimed to sell quantum cryptographic systems, Magiq Technology, BBN Technologies, and Id Quantique. It is important to note that, while quantum cryptography may be in principle a perfectly secure way to transfer a key, to ensure complete secrecy would require a perfectly noiseless communication channel. Since such channels do not exist, error correction and noise cancelling algorithms must be employed as well,

[59] A version of this appendix first appeared as Evans, Samuel A. 2009. *Technological Ambiguity & the Wassenaar Arrangement*. DPhil Thesis. University of Oxford. p. 211-222.

[60] US Patent number 1,310,719, issued 22 July 1919.

[61] Shannon, Claude E. 1949. "Communication Theory of Secrecy Systems." *Bell System Technical Journal* 28 (4 (October)): 656–715.

[62] Sergienko, Alexander V. 2006. *Quantum Communications and Cryptography*. Boca Raton, FL: Taylor & Francis.

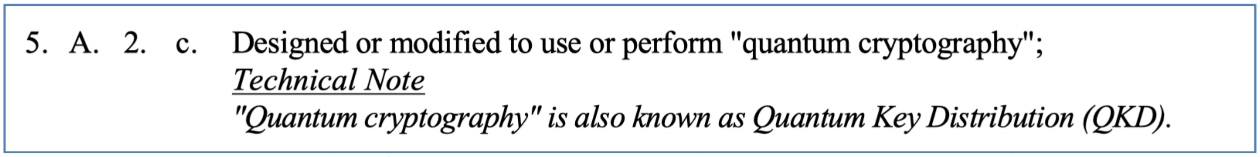
[63] Hastings, Michael, and Stefan Theil. "Now You See It..." *Newsweek International*, June 30, 2003, p. 58. Markoff, John. "A New Cryptography Uses Photon Streams." *New York Times*, November 4, 2002. Marks, Paul. "Quantum Cryptography to Protect Swiss Election." *New Scientist*, October 15, 2007. Singh, Simon. 1999. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*. New York: Doubleday.

which make the system no longer 'perfectly' secure. At the time, the amount of noise in a communication channel was the primary limiting factor in attempts to employ quantum cryptography.

The proposal process

As with most debates at the Wassenaar Arrangement, this one started with a proposal for a list change, this time from the British government, and specifically from the Communications-Electronic Security Group (CESG) at the Government Communication Headquarters (GCHQ). The text of any proposal has the potential to become anomalous, undermining the classification system as a whole. While the proposal offered a specific change—the text to go on the list—the process of accepting the proposal was one that involved discussion on both what the technology was, and whether it was anomalous. Those in the debate had to decide whether the technology was actually a form of cryptography, and, if it was, whether or not it was covered under the current controls. In creating the final text of *5.A.2.c* (the item entry that resulted from the debate),[64] they further had to decide how specified (and conversely how ambiguous) the text should be. We will look at each of these aspects in turn.

Is quantum cryptography a form of cryptography? It has the label of 'cryptography', and for some, that is enough for them to consider it a cryptographic system. But what does a cryptographic system do? Does it transfer information securely, or does it *allow for information to be transferred securely*? The former is a more widely accepted definition, but quantum cryptography falls more into the latter. Recall that quantum cryptography can more accurately be called 'quantum key distribution'; it transfers the key that is used in the onetime pad cipher, but does not actually encrypt the message itself. This is why one member of a national delegation to Wassenaar, when I mentioned quantum cryptography, replied, "It's now controlled. And we had an interesting debate on that because it's not really cryptography, it's quantum key distribution."[65] And indeed, when we look at the text of the list, there is a Technical Note after *5.A.2.c* that says, "'Quantum cryptography' is also known as quantum key distribution (QKD)" (Figure 2). This is further supported by the definition of quantum cryptography provided in the list (Figure 3).

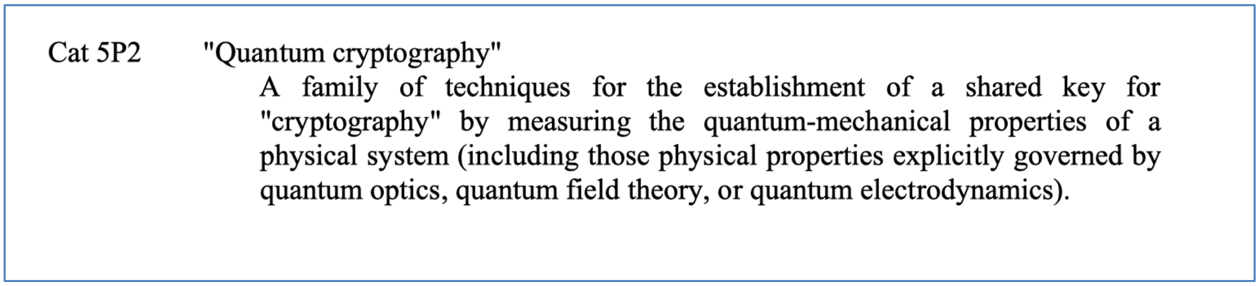


5. A. 2. c. Designed or modified to use or perform "quantum cryptography";
Technical Note
"Quantum cryptography" is also known as Quantum Key Distribution (QKD).

Figure 2 - Control text for "quantum cryptography" in the Wassenaar Arrangement Dual-Use List

[64] Before 2015, *5.A.2.c* was listed as *5.A.2.a.9*. This change was propagated to the US Commerce Control List through Bureau of Industry and Security, Commerce. 2015. "Wassenaar Arrangement 2015 Plenary Agreements Implementation, Removal of Foreign National Review Requirements, and Information Security Updates." 81 FR 64656-65692. Docket No. 160217120–6120–01.

[65] Interview with US State Department Official A & US State Department Official B, 11 September 2006.



Cat 5P2 "Quantum cryptography"

A family of techniques for the establishment of a shared key for "cryptography" by measuring the quantum-mechanical properties of a physical system (including those physical properties explicitly governed by quantum optics, quantum field theory, or quantum electrodynamics).

Figure 3 - definition of 'quantum cryptography' in the Wassenaar Arrangement Dual-Use List

Recall that a cryptographic system is composed of an encryption and decryption algorithm and a key. The algorithm used in quantum cryptography—the one-time pad—is very simple and widely known. Trying to control the international dissemination of the algorithm, then, is not an option for the Arrangement. Controlling the knowledge of and technology for producing and transferring the key, however, is an option, and in this way Wassenaar can in effect control the whole quantum cryptographic system. This process of identifying the best point of control is common in the list modification process, as one participant noted:

> [People working on our delegation are aware of] what's being developed, what's being used, what is an enabling technology or a key enabling technology for a given military system. And when that's identified, we say, "ok. Can we control it and where can we control it? What's a critical choke point that needs to be controlled? Is it the software? Is it the materials? Is it the manufacturing technology for it, which is just a know-how beyond the software?"[66]

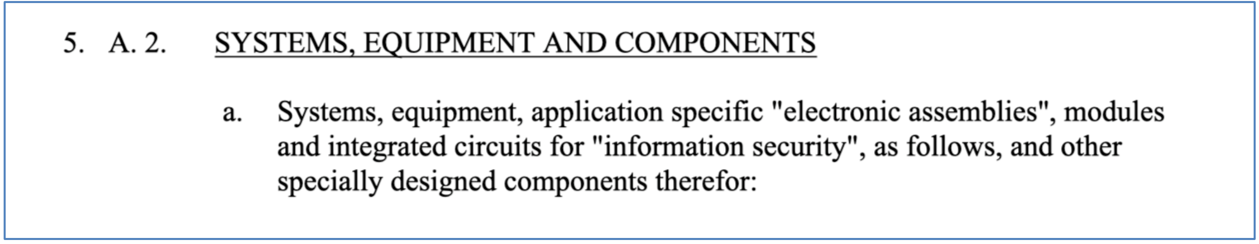
When quantum key distribution is viewed as a 'critical choke point' for the application of a quantum cryptographic system, we can understand why the proposal placed this text within Category 5 – Part 2: it is, for the purposes of control, cryptography. This was succinctly stated by a member of the British delegation:

> Interviewee: From my angle it [quantum cryptography] was a very very simple thing, and the least controversial of all the topics going forward. It was CESG's proposal. There was no reason from any angle why a new form (or new to us anyway) of encryption should not be added to the control, particularly because it seemed to us to be quite important. So in practical terms the proposal went forward. The interested parties were shut in a room upstairs in Wassenaar to really make sure that everybody understood what it was that we wanted to control.
>
> Sam Weiss Evans: Which is not at all clear on the actual lists. It says that you control 'quantum cryptography'.
>
> Interviewee: I think that was deliberate, at the end of the day, as a lot of the Cat 5 controls are. They are open to interpretation. It's not something that I ever felt very happy about, but one couldn't change overnight controls that had been there for a long time.[67]

[66] Interview with US Defense Department Official A, 8 August 2006.
[67] Interview with British Former Government Official, 8 March 2007.

Quantum cryptography was therefore established by at least one delegation as being a *relevant* technology for the purposes of the Wassenaar Arrangement. The next step in the proposal process was to determine if the technology was already controlled in *Category 5 – Part 2*.

It is useful here to recall that, if such a proposal had come up on 1980, it is very likely that no one would have seen the need to add text to the control list because *IL 1527* (*5.A.2*'s predecessor category in the CoCom Lists)[68] covered "Cryptographic equipment and ancillary equipment…designed to ensure secrecy of communications…" When the quantum cryptography proposal was submitted in 2004, however, the then-current control text was the chapeau[69] for *5.A.2.a*, shown in Figure 4.



5. A. 2. SYSTEMS, EQUIPMENT AND COMPONENTS

a. Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", as follows, and other specially designed components therefor:

Figure 4 - Chapeau for 5.A.2.a in the 2004 Wassenaar Arrangement Dual-Use List

This chapeau does not actually control any technology itself. The "as follows" denotes that items to be controlled are only specified in the sub-entries. This chapeau was created in the Core List revision of 1991, when *IL 1527* became *Category 5 – Part 2*.[70] With that move there was an important shift in the structure of the controls. *IL 1527* controlled all cryptographic equipment and components, whereas *5.A.2* only controls that equipment specified in the sub-entries. What was a blanket control text became a blanket *decontrol* text. Thus, the 1991 Core List revision was a shift from controlling all technology with specific decontrols, to only controlling the most important technologies. This shift tends to create more anomalies because a more fine-grained classification system will leave more technology out than in. As a very simple analogy, the old CoCom lists would control 'blocks', whereas the post-1991 lists would control 'blocks meeting any of the following criteria: red; square; smaller than 2 metres on any side'. For something to be controlled under the former classification system, it would only have needed to be understood as a block, but under the latter system, many things which are blocks would not fall under control. The former system is designed to prevent many anomalies by having a broad characteristic that covers a large range of technology. The latter system will generate more anomalies because it tries to control only specific instances of a general category.

Whether a system is broad or fine-grained is, of course, a relative matter. One could say that calling something a block is more fine-grained than just calling it a 'shape'. Returning to the Wassenaar lists, they could be very simple and just control 'technology' instead of having so many categories and items. Such a system would likely have few anomalies arising from something not being controlled but, as we shall see below, many more anomalies arising from contestations over whether technologies under control can actually be controlled. For now, it is sufficient to say that within *5.A.2* there was no text under which the participants thought

[68] CoCom, or the Coordinating Committee for Multilateral Export Controls, was the predecessor to the Wassenaar Arrangement, and existed from about 1949 until its disbanding in 1994.

[69] The Wassenaar Arrangement *Guidelines for Drafting Lists* states that entries are to be broken down into chapeaux, sub-entries, Notes, Technical Notes, and Note Benes, in that order.

[70] You can compare the March (old category structure) and September (new category structure) 1991 versions of the CoCom lists here: https://evansresearch.org/cocom-lists/

quantum cryptography could be placed, and therefore new text needed to be created. This solidified quantum cryptography as an anomaly within the dual-use classification system, which meant an anomaly-handling strategy was now necessary.

We can now see that the team that put together the proposal on quantum cryptography positioned it to be relevant to the Arrangement and not currently under control. Moreover, we have the beginnings of the next part of the proposal process—determining whether the technology can be controlled. At the time, only a handful of companies were known to have quantum cryptographic systems on the market, and those were based in the US and UK, which were seen as controllable spaces.

Having established that quantum cryptography is relevant, is not already controlled, and can be controlled, Britain then submitted the proposal to the Wassenaar Arrangement, where the other Participating States had an opportunity to comment on it and debate whether the modification should actually be made to the list. The discussions to make the list change for quantum cryptography were typical in that there was little debate over whether the technology should be controlled. There were also characteristics of the discussions typical specifically of changing *Category 5 – Part 2*.[71] They were conducted in a Technical Working Group (TWG) in a room on the upper floor of the Wassenaar Arrangement building in Vienna, at the same time of day as the Expert Group (EG) main meeting in the room downstairs. The TWG meeting was composed mostly of members of national delegations from their respective intelligence ministries. When this group—sometimes called the 'security & intelligence experts subgroup'[72] —proposes a change, it is usually accepted without debate by the main EG. With quantum cryptography, however, there were a lot of people in the room who would not necessarily be thought of as security and intelligence experts, and were there more to find out about this new technology that they did not know about than to help establish controls.[73]

This raises an important point about how specific the control text becomes in a list change. While there is the official specification that the text must be a "clear and objective specification of the item"[74], there is also the concern of giving away too much information. The lists, in other words, are not meant to be blueprints and procedure manuals for technology.

But why state the text of the list as simply controlling 'quantum cryptography' with no parameters other than that it is also known as 'quantum key distribution'? They could have been more specific, for instance by breaking it down into aerial systems and optical-fiber systems. They could have included parameters for the number of qubits per second that could be transferred, or the distance over which the system could work. One answer could be that the artefacts which currently existed were still more at the theoretical stage than the production stage. Until the technology was more developed, they might be satisfied with a broad level of control.

[71] Interview with British Former Government Official, 8 March 2007.
[72] Personal correspondence with US State Department Official A, 23 October 2008.
[73] Interview with British Former Government Official, 8 March 2007.
[74] Wassenaar Arrangement. 2005. *Criteria for the Selection of Dual-Use Items*. Available at https://www.wassenaar.org/app/uploads/2015/06/Criteria_for_selection_du_sl_vsl.pdf

There are several analytic points that come to light here. First is that the text functions as a technology under control. Providing information about the technology for the purposes of control is itself an uncontrolled transfer of knowledge about the technology. This leads to the second analytic point, which is that the decisions on the text involved decisions on creating strategic ignorance[75] for potential adversaries by purposefully building ambiguity into the definition of dual-use technology. There is as much interest in what is not used to define quantum cryptography as what is. Finally, a third analytic point is that the decision on how specific to make the definition was also a matter of finding parameters acceptable to all, getting agreement where possible and leaving the rest alone.

How could this proposal have been defeated? Those that might have focused on the economic aspects of controls could have used the point that the text is very broad to argue that the item should not be controlled because the text was not a "clear and objective specification of the item," and could not be because the technology is still in the early stages of development (including the development of the global market for the technology). Another point that could have been raised by this framing at the national as opposed to international level is that the controls would have put too heavy a burden on industry, or that the controls would significantly hinder competition on the global marketplace. To my knowledge, however, these arguments were not made. One reason may be that people expressing this competitive/economic framing were placated by those framing quantum cryptography as a security concern early on. "Nobody's saying they are going to be stopped from using [quantum cryptography]. The only factor that I perhaps put into [the design of the proposal] was that it didn't seem to me to be any burden on UK industry whatsoever."[76] Another reason may be that significant potential uses of this technology were already specifically decontrolled. Banking and financial transactions were decontrolled by *5.A.2. 'Note d'*, and mass market uses were decontrolled with *5. 'Note 3'*. The competitive framing therefore was assured that marketing the technology would not be subject to undue hindrance from export controls. Agreement was therefore reached with little dispute and the avoidance of all uncomfortable knowledge.[77] And thus, *5.A.2.c* was inscribed and the anomaly was successfully resolved into the now-expanded classification system.

[75] McGoey, L.. 2007. 'On the will to ignorance in bureaucracy', Economy and Society 36(2), 212–235.
[76] Interview with British Former Government Official, 8 March 2007.
[77] Rayner, Steve. 2012. "Uncomfortable Knowledge: The Social Construction of Ignorance in Science and Environmental Policy Discourses." *Economy and Society* 41 (1): 107–25. https://doi.org/10.1080/03085147.2011.637335.