CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Internet Freedom and Export Controls

Tim Maurer
Associate
Cyber Policy Initiative
Carnegie Endowment for International Peace

Briefing before the Commission on Security and Cooperation in Europe

March 3, 2016

Chairman Smith, Co-chairman Wicker, Members of the Commission,

It is an honor to testify before you today. Thank you for the opportunity to address the important issue of the role of export controls and internet freedom.

I am an associate at the Carnegie Endowment for International Peace, where I co-lead Carnegieôs Cyber Policy Initiative. For the last six years I have been working at the intersection of human rights, cybersecurity, and internet governance. I currently serve as a member of the Freedom Online Coalitionôs cybersecurity working group ñAn Internet Free and Secure,ò am a member of the Research Advisory Network of the Global Commission on Internet Governance.

Export controls are among the most complicated policy issues to address. Export controls combine law, technology, and policy with national- and international-level implications and in this case also sit directly at the intersection of human rights, security, and business. Striking the right balance between benefits and costs is a common challenge across all export control categories for dual-use items. This is especially difficult in the context of new technologies and emerging markets which still lack comprehensive empirical data.

In December 2013, the 41 member states of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies agreed to create two new export controls focusing on ñcybersecurity items.ò[1] The proposed implementation of these two new controls by the U.S. government sparked significant controversy last year and touch on four dimensions that are important to consider:

- Growing empirical evidence of technologies sold by companies in North America and Europe to customers in countries that use them to violate human rights
- The benefit of these technologies for legitimate law enforcement and intelligence activities
- The benefit of these technologies for cybersecurity, for example, to test and improve defenses
- The risks of these technologies for cybersecurity, for example, by providing more sophisticated hacking tools to actors who will use them for offensive purposes

My remarks will focus on the first of these four dimensions, controlling exports of technologies that can be used to violate human rights in the context of Internet Freedom, given the focus of this briefing but each of them raises important questions and challenges worth exploring further. In addition to the substantive considerations, process is another important factor to consider. The controversy over the past year and the significant pushback against the U.S. governmentôs proposed implementation of the two new controls are signs that processes need to be improved. Only two days ago, Secretary Pritzker announced in a letter that

> ñIn response to these concerns...the United States has proposed in this yearôs Wassenaar Arrangement to eliminate the controls on technology required for the development of óintrusion softwareô. We will also continue discussions both domestically and at Wassenaar aimed at resolving the serious scope and implementation issues raised by the cybersecurity community concerning remaining controls and hardware tools for the command and delivery of óintrusion software.ôò

As we enter this new phase in this discussion following Secretary Pritzkerôs letter, it is helpful to start by looking back at the original problem that led to these new controls. This is worth highlighting because this history and underlying human rights problem were occasionally lost in the controversy over the past year and has yet to be addressed. It is also worth noting that export controls are only one mechanism among a variety of tools to effectively address this first dimension but an important one which is why this briefing is particularly timely.

Introduction: The Emergence of a Difficult Problem

The driving force originally pushing for updated export controls were human rights groups who had grown increasingly concerned[2] that repressive governments were using new technologies to spy on their citizens.[3] These new technologies can be used for different purposes and have been sold on an emerging and growing market. This market first entered into the spotlight after the 2011 Arab uprisings; when the archives of fallen Arab regimes opened to the public, they provided a unique insight into those regimesô inner workings and trade relationships. This included shedding light on companies in North America and Europe who had exported technologies to security and intelligence agencies in countries ranging from Muammar Gadhafiôs Libya[4] to Bahrain[5]. In 2011, the *Wall Street Journal* published a catalog[6] shedding light on this burgeoning industry.

One particularly prominent example of the type of company and products that have been at the center of this debate is Hacking Team, an Italy-based company selling technologies designed to access computer networks and collect data. On July 5, 2015, Hacking Team was hacked. The intruder not only changed the firm's Twitter account to ñHacked Teamò but exposed some 400Gb of proprietary data to the public. Subsequent media analysis shed light on Hacking Teamôs client relationships with security agencies in more than 20 countries, including some with dubious human rights records such as Sudan.[7] Another example illustrates that certain governments use these technologies not only within their own borders. A federal court in Washington is currently weighing a lawsuit[8] alleging that the Ethiopian government remotely spied on a U.S. citizen in Maryland. To do so, the Ethiopian government used commercial internet-based technology sold by Gamma International, a company based in the United Kingdom and Germany. This activity was discovered not by the U.S. government, but by Citizen Lab, an academic research center based at the Munk School of Global Affairs at the University of Toronto.

These news reports and research publications also revealed that existing export control regulations did not cover some of the technologies of concern to human rights advocates. Therefore, the French[9] and British governments, which were both particularly criticized for allowing the export of technologies to authoritarian governments that eventually used them for surveillance, each submitted a proposal to amend the list of the Wassenaar Arrangement leading to the adoption of two new controls by its full membership in December 2013.

Background: Wassenaar Arrangement

The creation of these two new controls set a precedent by adding a human rights component to the Wassenaar Arrangement. The stated mission of the Wassenaar Arrangement is ñto contribute to regional and international security and stability, by promoting transparency and greater

responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations.ò[10] Unlike its predecessor, the Cold War-era Coordinating Committee for Multilateral Export Controls (COCOM), the Wassenaar Arrangement does not target any state or group of states, nor can members exercise veto power over other membersô export decisions. Rather, the arrangement aims to create a framework for harmonizing national approaches to export controls and to offer a forum for information-sharing.[11]

In December 2013, Wassenaar signatories, including the United States, the member states of the European Union, Japan, and Russia, reached a consensus on adding the two new aforementioned export controls focusing on ñintrusion softwareò and ñIP network surveillance systemsò to the arrangementôs list of regulated technologies. These are technologies used to gain access and to monitor data. Some[12] have described this addition as an attempt to bring ñcyberweaponsò into the fold of international arms-control agreements and the U.S. government would later describe them as ñcybersecurity items.ò[13]

Because the Wassennaar Arrangement is voluntary and nonbinding, it has no direct effect on national or international law; states must integrate its terms into their respective national frameworks for controlloing exports. Over the nearly two years since the passage of the 2013 amendments, the 41 signatory states have focused on implementing the change. So far, implementation across these 41 states remains uneven and while the majority of the membership including Japan and the member states of the European Union implemented the new controls, implementation by the U.S. has been lagging behind.

Analysis of Post--2013 Events and Proposed Implementation in the United States

Because the Wassenaar Arrangement is updated annually, its signatories have generally well-established mechanisms to implement any amendments, and the United States is no exception. Usually the U.S. interagency process takes six months to implement changes agreed to in the multilateral Wassenaar dual-use-technologies export-control list given the consultative process with industry beforehand through the Department of Commerceôs Technical Advisory Committees.[14] However, this time it took until May 2015, nearly three times longer than usual, for the U.S. government to publish its decision through the Department of Commerceôs Bureau of Industry and Security.

This long delay occurred for two reasons. First, there was a prolonged interagency discussion about the implementation of these two new controls. The outcome was not, as it usually is, a final rule but a proposed rule, which enabled the public to provide feedback during a two-month period. This was unusual and an encouraging demonstration of the governmentôs willingness to engage the public. In fact, Secretary Pritzkerôs letter now states that this practice will become institutionalized and a standard mechanism moving forward, a decision to be applauded. This can produce more effective outcomes in the future and help build trust among the actors involved, as long as it is used to meaningfully engage in dialogue rather than used to block action.

The second reason for the delay was that despite the administrationôs long internal deliberations, the proposed rule for implementing the new controls met with stiff resistance from major multinational companies as well as from members of the cybersecurity research community once

it was made public. During the subsequent two-month public comment period following the publication of the proposed rule, many businesses, industry groups, and security researchers argued that the bureauôs proposal interpreted the Wassenaar language too broadly, echoing more general concern over the wording the Wassenaar Arrangement itself. Companies including Google[15], Cisco and Symantec,[16] and firms under the umbrella Coalition for Responsible Cybersecurity[17] organized against the governmentôs formulation. They expressed concern about the potential cost to the industry, the potential effect of slowing down cybersecurity information sharing, and the uneven implementation of the new controls across the Wassenaar membership. Even some of the civil society organizations who had been advocating for an update of export controls[18] voiced concern about the possible effects of the changes and broad language on cybersecurity research offering specific recommendations for how to narrow and tailor their implementation.

The reaction made clear that addressing the problem and updating the export-control regime would be complicated for both historical and technical reasons. Historically, much of this debate is reminiscent of the heated discussions around the Computer Fraud and Abuse Act (CFAA) and encryption controls, known as the ñCrypto Warsò of the 1990s, which left scars and entrenched positions among those involved. Moreover, in several cases over the past two decades, federal prosecutors stretching the lawôs language have used the CFAA to pursue harsh court sentences.[19] Cybersecurity researchers worry that an overly vague or broad regulation could be similarly used in the future. It is therefore no surprise that the U.S. governmentôs proposed implementation of the new controls resurfaced old grievances and revealed significant levels of mistrust among some of the actors involved.

Moreover, the proposed rule exceeded the original language of the 2013 amendment to the Wassenaar Arrangement. That wording had focused more narrowly on network-surveillance systems and intrusion software that is usually developed by companies for sale to governments, not by individual researchers. By contrast, the U.S. proposal outlines a policy of ñpresumptive denialò and is therefore inclined to deny rather than approve exports and specifically references ñzero-day exploits,ò the vulnerabilities in software that remain undetected and have been known for zero days. Cyber researchers often seek out such vulnerabilities to test a systemôs security and to alert developers to weaknesses. There are also so-called bug bounty programs and an active market where such vulnerabilities are traded. As the Electronic Frontier Foundation[20] argues, ñthe only difference between an academic proof of concept and a 0-day for sale is the existence of a price tag.ò The concern is that the new regulations could have a chilling effect on researchers fearful of being found in violation of the letter of the law, even though their objective is the exact opposite. Department of Commerce representatives have stated[21] that the proposed controls are not intended to limit security research or even the legal trade in zero-day vulnerabilities, but critics worry that such a chilling effect will occur.

As a result of this feedback, the Department of Commerce, in an unusual departure[22] from its normal implementation process, first indicated that it would revise its proposal[23] and eventually the U.S. government followed up with the aforementioned letter by Secretary Pritzker on March 1, 2016..

Moving Forward and Recommendations

It is clear that addressing this problem can only be successful if coordinated multilaterally and informed by technical analysis.[24] Initially, human rights groups expected that the United States would be a leader in implementing these export controls given its prominent Internet Freedom agenda. Now, the United States is part of the minority of countries that have yet to implement the new controls and is reacting to other countriesô implementation rather than proactively shaping the standard itself. As others have already observed, the United States is ñhome to most of the world's cybersecurity companies, holding the number one provider position in the global market - which topped $75 billion in 2015 and could reach $170 billion by 2020.ò[25] U.S. leadership on this issue and full investment in striking the right balance can therefore have a significant impact and set an example for others. One of the positive outcomes of the controversy of the past several months is a heightened awareness among all actors involved. The underlying human rights problem that led to the development of the new controls has yet to be addressed.

Export controls can be an effective tool to influence corporate behavior.[26] The challenge is designing them so they only target the type of behavior deemed of concern without affecting the rest. Weighing these interests and weighing human rights and security concerns is not a novelty in the context of export controls especially for dual-use technologies.[27] However, this is a new and growing industry with a limited amount of data available therefore making this process more complicated.

Moving forward, I therefore recommend focusing on the following two strategic priorities:

- **Increasing transparency**: a major challenge to addressing this problem effectively and to tailoring export controls accordingly is the lack of information about this market, its players, and the trade of products. Greater transparency can be accomplished through various avenues including voluntary action by companies. In addition, the notification requirements of the export control regime can be a useful mechanism for the government to get a better picture about the market without necessarily imposing a licensing requirement. The data can then be reviewed after a few years to develop a tailored export control regime based on more reliable data.

- **Establishing an efficient and inclusive process**: The controversy of the past year shows that the process to develop, adopt, and implement new export controls needs to be improved. The U.S. governmentôs decision to request public feedback is a promising sign to solicit input beyond the existing standing Technical Advisory Committees. This is particularly important to reach communities such as the cybersecurity research community. A further improvement of the process could consist of the government hosting more consultations at some of the major security research and Internet Freedom conferences composed of representatives from different government agencies. Moreover, representatives from the human rights community must be invited in these discussions at all, including the highest levels.

With regard to the immediate task of implementing the two new controls in the United States, I recommend two parallel tracks:

- A first track reviewing the language of the two new controls and exploring how the language could be improved in a process involving the human rights and security research communities as well as industry.[28] Following Secretary Pritzkerôs letter, it is now clear that at least part of the language of the two new controls will be reviewed at Wassenaar. However, this process is likely to encounter several challenges including the trade-off between (i) keeping language thatôs fairly broad but can therefore take into account future technological developments without having to be updated or (ii) narrowing the language and therefore scope of the control but likely to require revisions sooner. The former requires more trust in the government not to use broad language for overly strict implementation policies. At the same time, major revisions to the language are not feasible given that the majority of the Wassenaar membership has not only agreed to but already implemented the new controls and these are only two of many items to be reviewed and discussed overall.

- a second track focusing on how to implement and develop a licensing policy for the language to apply only to those technologies sold by companies to specific end users in countries with known human rights problems. This will require a nuanced approach combining the technology-focused controls with existing or potentially new country charts. This also needs to include developing FAQs to be issued by the U.S. government to clarify its interpretation of the language. In terms of process, it is important to include industry, the cybersecurity research and human rights communities for all parties to develop a shared understanding of the interpretation of adopted language and implementation. One option for implementing the two new controls more narrowly in addition to taking into account otherôsrecommendations[29] about possible exemptions is:
    - Only exports of technologies to countries with systemic human rights violations will be subject to a review for approval or denial by the U.S. government with a presumption of denial policy in place for those countries with empirical data of past human rights violations involving such technology[30]
    - Export of technologies that fall under the two controls to other countries will only trigger a notification requirement providing details about the export, type of product, customer etc. to the government to increase transparency but will not be subject to an approval review

At the multilateral level, it has become clear that while the 41 member states agreed to the same language in December 2013, implementation of the new controls has varied widely.[31] As Cheri McGuire, vice president for global government affairs & cybersecurity policy at the Symantec Corporation has pointed out in her testimony on January 12, 2016, ñ[t]he Hacking Teamôs public business model was to sell offensive intrusion and surveillance capabilities ï the exact technology the Wassenaar Arrangement attempted to target with the new controls. However, the Italian export authorities granted a blanket global license to the Hacking Team allowing them to freely export their products around the world to many of the countries that the Wassenaar rule is trying to prevent from obtaining these tools.ò[32] Moreover, Gammaôs actions in Switzerland are a powerful reminder that companies are likely to shop for favorable jurisdictions, and that the global impact

of export controls will remain limited without a multilateral regime with uniform and global implementation. Therefore, I recommend:

- the U.S. government to work with other Wassenaar members based on data that is now becoming available to ensure that the implementation of the new controls is consistent across its membership in order for the controls to be effective and in order for the controls not to create a competitive disadvantage.

- the U.S. government to collaborate with countries that are not members of the Wassenaar Arrangement but focus on building an industry in this area, for example, India, to engage them early on in building a broader regime with common standards.

One country particularly worth paying attention to in this context is Israel. Israel is not a member of the Wassenaar Arrangement yet implements Wassenaar controls voluntarily. Israel is therefore also implementing the two new controls, in fact, it has even broadened the language.[33] This is particularly noteworthy given Israelôs significant cybersecurity industry, the Israeli governmentôs having made growing this industry a national priority including support from Prime Minister Benjamin Netanyahu at the top,[34] and the unique security threats Israel is facing. Israelôs approach to implementing the new controls is likely to provide further insight into how to strike an appropriate balance between these various interests.

Export controls are only one mechanism in the tool kit to effectively address the underlying human rights issue, as I pointed out at the beginning. They will need to be part of the mix but we also need to consider other tools, namely:

- Corporate self-regulation and corporate social responsibility: The strong reactions from industry have produced a heightened awareness. Translating this heightened awareness into action addressing the underlying human rights problem will require leadership and support from responsible industry leaders to impose peer pressure on industry members with lower standards of due diligence. For example, Jerry Lucas, president of the company that organizes the Intelligence Support Systems conferences that have become known for showcasing surveillance and censorship technology, demurs responsibility. ñThatôs just not my job to determine whoôs a bad country and whoôs a good country,ò he has said. ñThatôs not our business, weôre not politiciansé weôre a for-profit company. Our business is bringing governments together who want to buy this technology.ò[35] A voluntary approach driven by industry could include
    - Sharing best practices for implementing Know-Your-Customer to raise the standard across industry (the Electronic Frontier Foundation has done some groundbreaking work in this area);[36]
    - Becoming a member and active participant in industry groups focusing at the intersection of business and human rights such as the Global Network Initiative;[37]
    - Working with human rights NGOs and research organizations like EFF, the Citizen Lab, Privacy International, or New Americaôs Open Technology Institute to increase transparency and help name and shame.[38]

- Expansion of ñGHRAVITYò executive order: In April 2012, the Obama administration issued *Executive Order Blocking The Property And Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria Via Information Technology*[39] to address the provision of technologies to these two countries that can be used for surveillance. The European Union established[40] a similar ban on exports to Syria. Expanding this ñGHRAVITYò[41] Executive Order is another potential avenue to pursue. However, unlike the export control system, this approach has a much less mature system to include and engage with stakeholders outside of government, an issue that will only increase in importance as the technology evolves creating a need to update the language and scope of such regulation. Exploring this option therefore requires particular investment in establishing procedures to engage with and consult experts in industry as well as the cybersecurity research and human rights communities.

Looking ahead, it will be important to make these new controls meaningful and effective. Otherwise, governments could rely on other existing controls, namely encryption controls, as a substitute to address the unresolved underlying human rights problem. Given that another objective of many civil society and industry actors is a further liberalization of encryption controls in the future building on the historic tend, further liberalizing encryption controls will become significantly more complicated and harder to disentangle if encryption controls will also be used to protect human rights in the future. Relatedly, if encryption controls will be used as a substitute some companies might start developing products without encryption automatically built into them to avoid export controls that might still be of concern from a human rights perspective.

Endnotes

[1] https://www.gpo.gov/fdsys/pkg/FR-2015-05-20/pdf/2015-11642.pdf
[2] https://static.newamerica.org/attachments/3936-uncontrolled-global-surveillance-updating-export-controls-to-the-digital-age/Uncontrolled_Surveillance_March_2014.26e1226c08774594bd8a93d5638e8a75.pdf
[3] Parts of this written statement are based on previous publications I have written and co-authored, for example: http://www.worldpoliticsreview.com/authors/1798/tim-maurer
http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=182246
[4] http://www.wsj.com/articles/SB10001424053111904199404576538721260166388
[5] http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking
[6] http://graphics.wsj.com/surveillance-catalog/
[7] http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech
[8] https://www.eff.org/cases/kidane-v-ethiopia
[9] http://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496
[10] http://www.wassenaar.org/introduction/index.html
[11] https://www.gpo.gov/fdsys/pkg/FR-2015-05-20/pdf/2015-11642.pdf
[12] http://www.npr.org/sections/alltechconsidered/2015/07/20/424473107/commerce-department-tighter-controls-needed-for-cyber-weapons
[13] https://www.gpo.gov/fdsys/pkg/FR-2015-05-20/pdf/2015-11642.pdf
[14] https://tac.bis.doc.gov/
[15] https://googleonlinesecurity.blogspot.com/2015/07/google-wassenaar-arrangement-and.html
[16] http://passcode.csmonitor.com/wassenaar-comments#chapter-235070
[17] http://www.responsiblecybersecurity.org
[18] https://cdt.org/files/2015/07/JointWassenaarComments-FINAL.pdf
[19] https://www.eff.org/de/issues/cfaa
[20] https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation
[21] http://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200
[22] http://digital-era.net/unusual-re-do-of-us-wassenaar-rules-applauded/
[23] http://www.reuters.com/article/2015/07/29/us-software-exports-regulation-idUSKCN0Q32OQ20150729
[24] http://www.cyberdialogue.ca/2013/03/against-hypocrisy-updating-export-controls-for-the-digital-age-by-danielle-kehl-and-tim-maurer/
[25] http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizing-andprojections.html
[26] Eric Rabe, the chief communications counsel for Hacking Team, provided the interesting insight stating in an email to me that Hacking Team attempts to learn about any possible abuse by vetting clients, monitoring reports of abuses, ñrequire[ing] certain behaviors which we outline in our contract,ò and ñmay decided [sic] to suspend support for that clientôs system rendering it quickly ineffective.ò His latter comment suggests that it is possible for some products to render such technology ineffective quickly even after the delivery of the system when the customer is found to contribute to human rights violations. See also: http://www.slate.com/articles/technology/future_tense/2014/05/wassenaar_arrangement_u_s_export_control_reform_keeping_surveillance_tech.html

[27] http://www.theguardian.com/world/2012/jul/13/arms-trade-arab-and-middle-east-protests
[28] https://langevin.house.gov/press-release/langevin-statement-obama-administrations-decision-renegotiate-wassenaar-intrusion
[29] https://cdt.org/files/2015/07/JointWassenaarComments-FINAL.pdf
[30] An alternative to creating this new list would be selecting or combining existing lists from the Commerce Country Charts: https://www.bis.doc.gov/index.php/forms-documents/doc_view/14-commerce-country-chart

[31]

http://www.worldpoliticsreview.com/authors/1798/tim-maurer
https://oversight.house.gov/wp-content/uploads/2016/01/McGuire-Symantec-Statement-1-12-Wassenaar.pdf
[32] https://oversight.house.gov/wp-content/uploads/2016/01/McGuire-Symantec-Statement-1-12-Wassenaar.pdf

[33] https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach
[34] http://mfa.gov.il/MFA/InnovativeIsrael/ScienceTech/Pages/PM-Netanyahu-addresses-5th-International-Cybersecurity-Conference-23-Jun-2015.aspx
[35] http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance
[36] https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment
[37] https://www.globalnetworkinitiative.org/
[38] Yet, as long as there are companies whose business does not depend on brand reputation and who refuse to follow due diligence with respect to human rights, three is need for a regulatory framework to provide a legal basis for governments to act if necessary.

[39] http://www.whitehouse.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entry-united-states-cer
[40] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:016:0001:0032:EN:PDF
[41] https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20120423_33.aspx