Export Controls on Intrusion Software

Collin Anderson (@CDA)
Tom Cross (@_decius_)

Do Export Controls on Intrusion Software Threaten Security Research?

Truth is… we don't know.

(We're not lawyers and **this isn't legal advice**.)

Truth is… the Government doesn't know.

(At least they are asking questions.)

Truth is… nobody knows.

(We don't even agree about this...)

Outline:

1. **Some Basics**
   a. What is the problem?
   b. How do export controls work generally?
2. **How these new Wassenaar rules work**
   a. IP Network Surveillance Systems
   b. Intrusion Software
   c. “Technology” for the development of Intrusion Software
3. **Implications**
   a. Could these rules regulate “full disclosure” and “open source?”
   b. Do these rules apply to Vulnerability Research?
   c. Could these rules regulate coordinated disclosure or bug bounties?
   d. Could these rules regulate training classes?
   e. What if I leave pen testing tools on my laptop when I travel?
   f. What about foreign coworkers or my company’s offices in other countries?
   g. What about reverse engineering tools? Debuggers? Exploit generators? Jailbreakers?
   h. If I ask BIS for permission, will I get a license?
4. **What can we do about it?**

The Basics

Surveillance is Big Business!

What's the problem?

The Problem:

1. The Citizen Lab correctly identified 21 customers of Hacking Team.

2. The US DEA and US Army are customers. DEA are using the technology out of their embassy in Bogota, Colombia.

3. Hacking Team sold its technology to three agencies in Morocco. **The Moroccan government's intimidation of civil society… is nothing more than an attempt to silence legitimate criticism.**

4. Hacking Team have been **evading the legitimate questions from UN investigators regarding the sale of technology to Sudan.**

5. NICE Systems appears to have sold Hacking Team spyware to Azerbaijan, Uzbekistan, and Denmark.

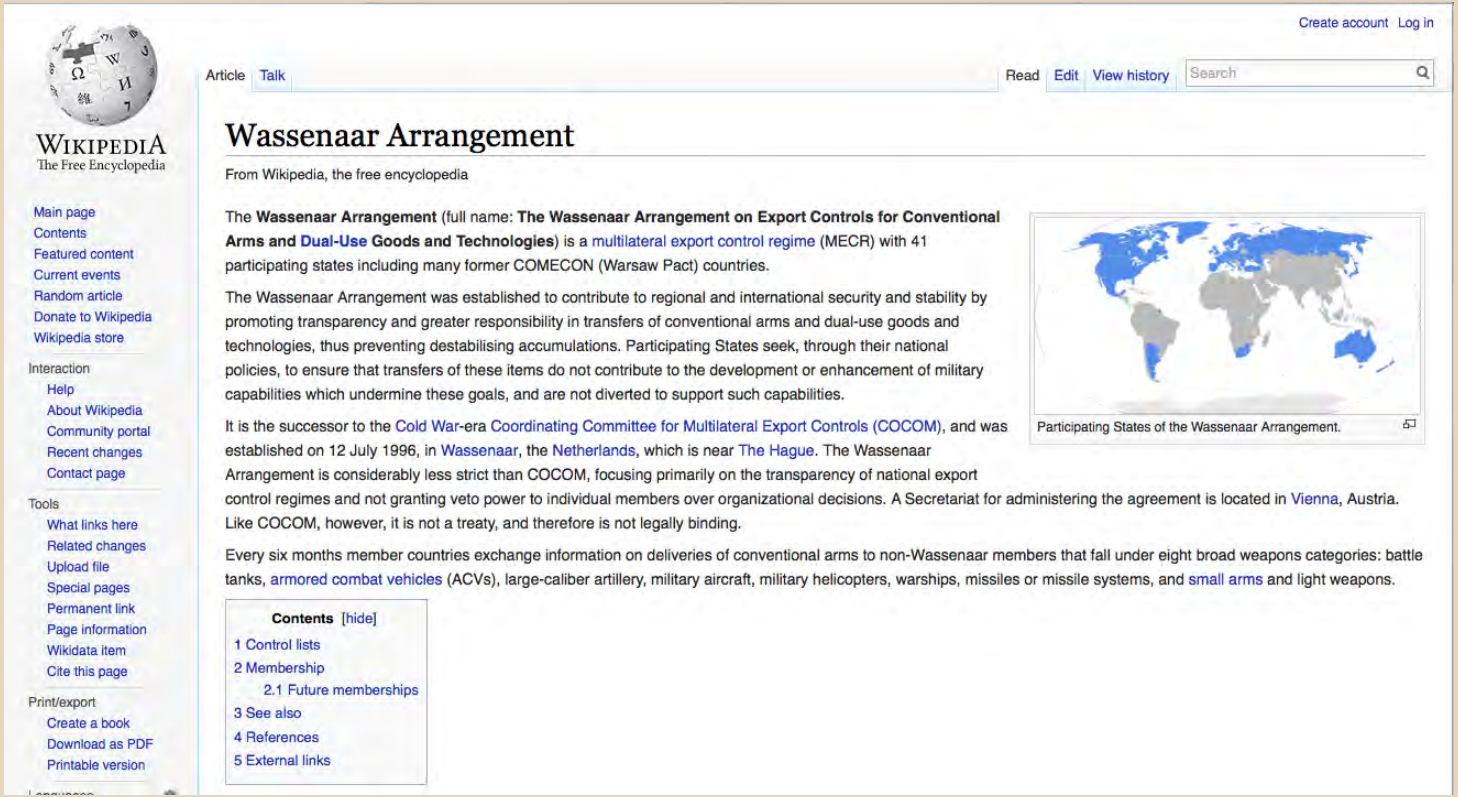
6. Hacking Team are trying to secure a sale to the Rapid Action Battalion (RAB), a Bangladesh police unit described by Human Rights Watch as a "death squad" involved in torture and extrajudicial killings.

7. Hacking team reinstated support contracts with the Ethiopian government despite reports of **the targeting of Ethiopian US-based journalists by Hacking Team's spyware.**

8. **Our lobbying of the Italian government on export controls worked.** We wrote to the Italian Ministry of Economic Development, over 100 parliamentarians, and to the regional Government calling for unilateral export controls on Hacking Team's spyware. We were successful in that the Italian government implemented the controls that we had been calling for and temporarily suspended Hacking Team's operations, citing "possible uses concerning internal repression and violations of human rights".

The Solution:

What is the Wassenaar Arrangement?



Create account Log in

WIKIPEDIA
The Free Encyclopedia

Article Talk | Read Edit View history | Search

Wassenaar Arrangement

From Wikipedia, the free encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

The **Wassenaar Arrangement** (full name: **The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies**) is a multilateral export control regime (MECR) with 41 participating states including many former COMECON (Warsaw Pact) countries.

The Wassenaar Arrangement was established to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

Participating States of the Wassenaar Arrangement.

It is the successor to the Cold War-era Coordinating Committee for Multilateral Export Controls (COCOM), and was established on 12 July 1996, in Wassenaar, the Netherlands, which is near The Hague. The Wassenaar Arrangement is considerably less strict than COCOM, focusing primarily on the transparency of national export control regimes and not granting veto power to individual members over organizational decisions. A Secretariat for administering the agreement is located in Vienna, Austria. Like COCOM, however, it is not a treaty, and therefore is not legally binding.

Every six months member countries exchange information on deliveries of conventional arms to non-Wassenaar members that fall under eight broad weapons categories: battle tanks, armored combat vehicles (ACVs), large-caliber artillery, military aircraft, military helicopters, warships, missiles or missile systems, and small arms and light weapons.

Contents [hide]

1 Control lists
2 Membership
  2.1 Future memberships
3 See also
4 References
5 External links

How do export controls work in the US?

<--------- ITAR (International Traffic in Arms Regs)

- Governed by the State Department
- Controls Military Items (US Munitions List)
- Includes items for “National Police” forces
- Includes Military Encryption Items
- Includes items that hinder the operation of adversary electronics
- Includes items that “exploit” the electromagnetic spectrum (regardless of transmission medium).

EAR (Export Administration Regulations) ---------->

- Governed by the US Bureau of Industry and Security (BIS)
- Controls “Dual Use Items” - Civilian items that have military applications
- Includes controls on Cryptography
- The new controls on “Intrusion Software” fit here

Wait, didn't we win the crypto wars?

Intel Subsidiary Agrees to $750,000 Penalty for Unauthorized Encryption Exports

| Print |

FOR IMMEDIATE RELEASE

Wednesday, October 8, 2014

www.bis.doc.gov

BUREAU OF INDUSTRY AND SECURITY

Office of Congressional and Public Affairs

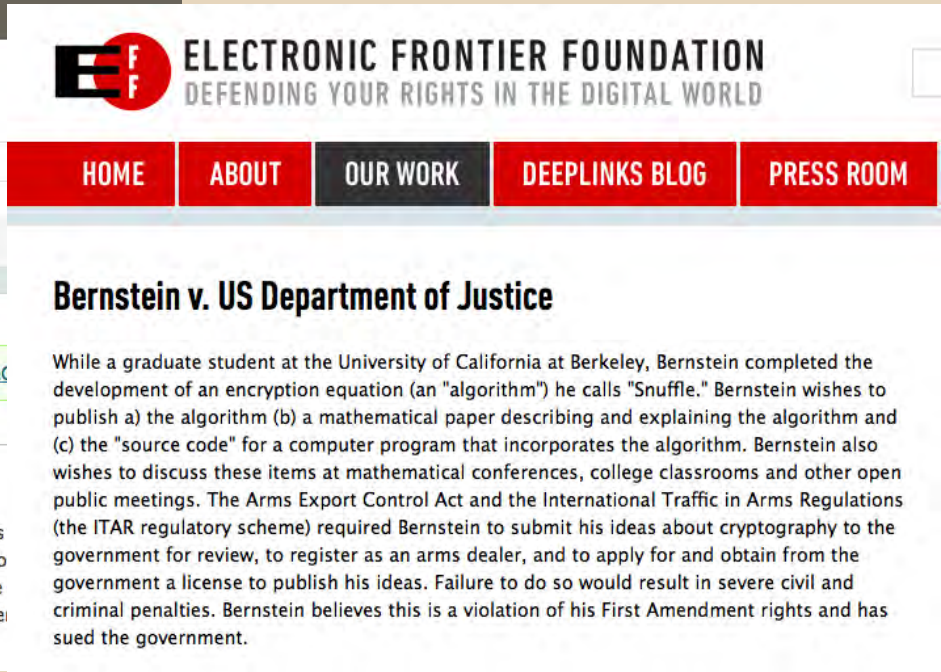
202-482-2721

Intel Subsidiary Agrees to $750,000 Penalty for Unauthorized Encryption Exports

WASHINGTON – The U.S. Department of Commerce's Bureau of Industry and Security (BIS) today announced that Wind River Systems of Alameda, Calif., a wholly-owned subsidiary of Intel Corporation, has agreed to a $750,000 civil penalty to settle charges that it sold encryption software products to foreign government customers and to organizations identified on the BIS Entity List without the required Department of Commerce licenses.

In April 2012, Wind River Systems voluntarily disclosed to BIS that between 2008 and 2011 the company made 55 exports of operating software valued at $2.9 million to governments and various end users in China, Hong Kong, Russia, Israel, South Africa, and South Korea. The operating software is controlled under Export Administration Regulations for national security reasons, and some of the export recipients in China are on the BIS Entity List.

License Exception TSU

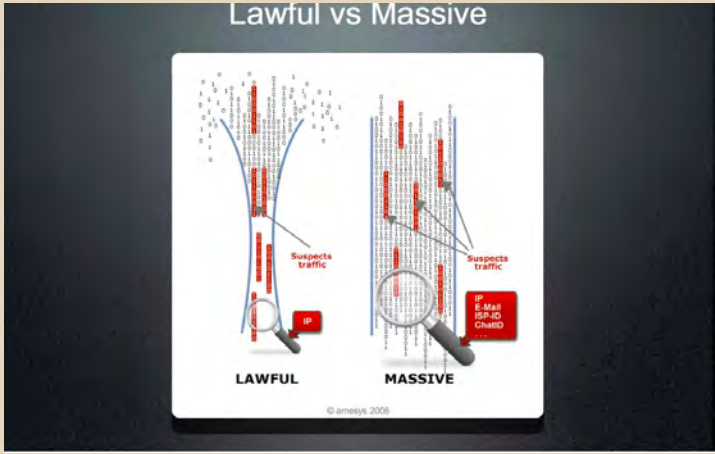


The New Rules

IP Network Surveillance Systems

5. A. 1. j. *IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:*

1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
    - Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
    - Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
    - Indexing of extracted data; and
2. Being specially designed to carry out all of the following:
    - Execution of searches on the basis of ‘hard selectors’; and
    - Mapping of the relational network of an individual or of a group of people.



What is “Intrusion Software?”

“Software” specially designed or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network capable device, and performing any of the following:

- The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or
- The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

- **‘Monitoring tools’:** “software” or hardware devices, that monitor system behaviours or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.
- **‘Protective countermeasures’:** techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) or sandboxing

Is “Intrusion Software” Controlled?

NO

Then what IS controlled?

4. A. 5. Systems, equipment, and components therefore, specially designed or modified for the generation, operation or delivery of, or communication with, “Intrusion Software”.

4. D. 4. “Software” specially designed or modified for the generation, operation or delivery of, or communication with, “Intrusion Software”.

“Technology” is also controlled

4. E. 1. c. “Technology” for the “development” of “Intrusion Software”.

Technology - Specific information necessary for the “development”, “production”, or “use” of a product. The information takes the form of ‘technical data’ or ‘technical assistance’.

NOTE: “Intrusion Software” itself is NOT controlled, but information necessary for the “development” of “Intrusion Software” IS controlled, including “technical data” and “technical assistance.”

The Implications

What about Full Disclosure and Open Source?

15 CFR 734.3 - The following items are not subject to the EAR:

Publicly available technology and software… that:

(i) Are already published or will be published as described in §734.7 of this part;

(ii) Arise during, or result from, fundamental research, as described in §734.8 of this part;

(iii) Are educational, as described in §734.9 of this part;

Encryption vs. “Intrusion Software” Stuff

Encryption:

- License Exception TSU
- Must be publicly available
- Must be open source
- You must email BIS and notify them

Controlled Stuff related to “Intrusion Software”:

- 15 CFR 734.3(b)(4)
- Must be publicly available
- Does NOT need to be open source
- BIS does NOT need to be notified

Is Vulnerability Research Covered?

BIS, in the federal register: "Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices."

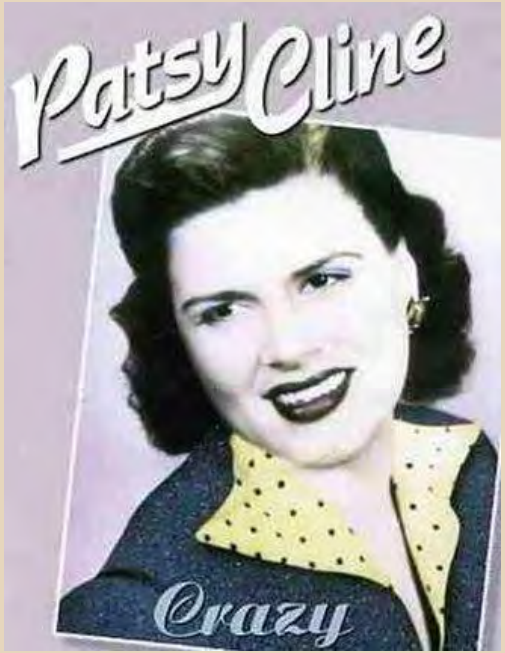
BIS, in the FAQ on their website: "The proposed rule would not control… Information about the vulnerability, including causes of the vulnerability."

BIS, also in the FAQ on their website: "Neither the disclosure of the vulnerability nor the disclosure of the exploit code would be controlled under the proposed rule."

However: "The proposed rule would control…

Technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information

Information on how to prepare the exploit for delivery or integrate it into a command and delivery platform."



Coordinated Disclosure and Bug Bounties

From the BIS FAQ: “Any technical data sent to an anti-virus company or software manufacturer with the understanding that the information will be made publicly available, would not be subject to the EAR.

However, "technology" that is not intended to be published would be subject to the control.”

Planning to disclose a mitigation bypass?

Security TechCenter

Search TechNet with Bing

Home | Security Updates | Tools | Learn | Library | Support

RESPONSE | BULLETINS | ADVISORIES | MYBULLETINS

Security TechCenter > Security Updates > Response > Security Researcher Engagement > Mitigation Bypass Bounty and BlueHat Bonus for

Mitigation Bypass and BlueHat Defense Terms

PROGRAM DESCRIPTION:

Microsoft is pleased to announce the launch of the Microsoft Mitigation Bypass Bounty and BlueHat Bonus for Defense Program beginning June 26, 2013. Through this program, individuals across the globe have the opportunity to submit a novel mitigation bypass against our latest Windows platform, and are optionally invited to submit a defense idea that would block an exploitation technique that currently bypasses the latest platform mitigations. Under this program, qualified mitigation bypass submissions are eligible for payment of up to $100,000 USD, with a bonus of up to $50,000 USD for defense submissions. Bounties will be paid out at Microsoft's discretion.

If you are submitting a new mitigation bypass technique that you have found in an active attack, please note that that we have a similar but separate program for you, and the terms appearing here are aimed at individuals submitting their own idea for a new mitigation bypass technique.

Sharing Exploit Toolkit Samples?

If you discover an exploit toolkit in the wild and want to share it with other infosec professionals or software vendors across borders, apparently, this may not be allowed under the proposed rule.

BIS, in their FAQ: “Exploit toolkits would be described in proposed ECCN 4D004… There are no end user or end use license exceptions in the proposed rule.”

What about training classes?

On the one hand: Technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information. Information on how to prepare the exploit for delivery or integrate it into a command and delivery platform.

On the other hand, 15 CFR 734.7(a)(4): Release at an open conference, meeting, seminar, trade show, or other open gathering.

(i) A conference or gathering is "open" if all technically qualified members of the public are eligible to attend and attendees are permitted to take notes or otherwise make a personal record (not necessarily a recording) of the proceedings and presentations.

(ii) All technically qualified members of the public may be considered eligible to attend a conference or other gathering notwithstanding a registration fee reasonably related to cost and reflecting an intention that all interested and technically qualified persons be able to attend, or a limitation on actual attendance, as long as attendees either are the first who have applied or are selected on the basis of relevant scientific or technical competence, experience, or responsibility (See Supplement No. 1 to this part, Questions B(1) through B(6)).

Planning to travel outside the USA?

§ 740.14 Baggage (BAG).

(a) ***Scope.*** This License Exception authorizes individuals leaving the United States either temporarily (i.e., traveling) or longer-term (i.e., moving) and crew members of exporting or reexporting carriers to take to any destination, as personal baggage, the classes of commodities, software and technology described in this section.

BIS, in the Federal Register: "No license exceptions would be available for these items, except certain provisions of License Exception GOV, *e.g.,* exports to or on behalf of the United States Government pursuant to § 740.11(b) of the EAR."

What about foreign coworkers & offices?

BIS, in their FAQ: “The proposed rule does not provide for any exceptions to deemed export license requirements.”

BIS on “Deemed Export” - “Release of controlled technology to foreign persons in the U.S. are "deemed" to be an export to the person’s country or countries of nationality.”

Also, BIS, in their FAQ: “There is **no license exception for intra-company transfers** or internal use by a company headquartered in the United States under the proposed rule.”

Debuggers and exploit generators?

BIS, in their FAQ: “General purpose tools, such as IDEs, are not described under proposed ECCN 4D004 because they are not "specially designed" for the generation of "intrusion software." Some penetration testing tools (FAQ #12) and exploit toolkits (FAQ #18) are described in proposed ECCN 4D004, as they are command and delivery platforms for "intrusion software."”

Jailbreaking Software?

BIS, in their FAQ: “If particular jailbreak software did meet all the requirements for classification under ECCN 4D004 (such as a commercially sold delivery tool "specially designed" to deliver jailbreaking exploits) then it would be subject to control and a license would be required to export it from the United States. Note that if such software were "publicly available," it would not be subject to the Export Administration Regulations.”

Will I get a license?

BIS, in the Federal Register: “Note that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.”

Dave Aitel: “If you are modular in any way, you facilitate 0day. An 0day is just a program after all. So anything that can execute commands or auto update is now "default deny" for export.”

What do we do about it?

Comment Period?

At the time these slides were composed, the open comment period will close before Defcon, on July 20th, 2015.

However, we anticipate that BIS may extend this comment period, or open up a new one in the future.

Key Points:

- **At least, the US has published their interpretations and asked for feedback.**
  - The Wassenaar Negotiators did not.
  - Many countries in Europe have enacted this without publishing information about how they plan to interpret it.

- **Regulators will probably be responsive to clear, negative impacts the regs will have on:**
  - Legitimate information security research.
  - Legitimate computer security work.
  - Legitimate business activity and the economy as a whole.

- **Regulators will not be responsive to vitriol or paranoid, overly broad misinterpretations of their proposed regs.**
  - Its important to relate potential problems to the specific statements that regulators have made about how they interpret the regulations.

Stay Informed:

Federal Register: https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

BIS FAQ: http://www.bis.doc.gov/index.php/licensing/embassy-faq

Regs list: https://lists.alchemistowl.org/mailman/listinfo/regs