Treatment of information security tools under the Wassenaar Arrangement

Applicants

Supervisor Name	Department/Group	Faculty
1. Arno Lodder	TLS/Internet Law	RCH
2. Herbert Bos	CS/Systems & Netw. Security	FEW

Project description

This proposal seeks to evaluate the treatment of information security research tooling under the Wassenaar Arrangement. As a result of developments outlined below, many tools that the information security research community commonly produces and uses, and that are readily distributed amongst the members of this community are now, or will soon be, in scope of the export control regime maintained as a result of the Wassenaar Arrangement. Not surprisingly, the Arrangement has led to much concern among hackers, security experts and scientists alike.[1]

The study is particularly relevant in light of increasing concerns over state sponsored cyber espionage and following the 2013 agreement under the Wassenaar Arrangement to add certain types of "intrusion software" and "communication surveillance equipment" to the list of controlled Dual Use Goods.[2] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement") is a global multilateral arrangement between 41 nation states to regulate global arms trade and to prevent destabilizing accumulations of arms. Member states undertake to implement and enforce compliance with the Wassenaar Arrangement's list of controlled goods under their national laws.[3]

The EU Dual Use list that is maintained as part of the EU Dual Use Regulation was amended in line with this on 31 December 2014 (EC Regulation 428/2009). More recently on 20 May 2015, the US Commerce Department's Bureau of Industry and Security published a proposal to

[1] "Why Wassenaar Arrangement's Definitions of "Intrusion Software" and "Controlled Items" Put Security Research and Defense At Risk", https://www.usenix.org/system/files/login/articles/wassenaar.pdf
[2] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies of December 4th 2013", 4 December 2013
[3] http://www.wassenaar.org/index.html

implement these requirements in the USA by means of a license requirement for the export, reexport, or transfer (in-country) of these cybersecurity items out of the USA.[4]

The project entails studying and classifying categories of information security research tools from a technical perspective along with their qualification and treatment as goods that can be used for civil or military purposes for export control purposes ("Dual Use Goods").

Project Organization

1. Computer science / System and Network Security (M.Sc Student)

The student needs to be familiar with current practices in security, program analysis and reverse engineering, especially in the area of security. Concretely, this translates into course-level requirements in the form of Binary and Malware Analysis and/or Systems Security. In addition (and perhaps most challenging), the ideal candidate should have not just hacking skills, but also a keen interest in the (legal) context in which hacking and analysis takes place. Fortunately, many of the students in the security classes prove to be very involved (and activistic) in these matters.

2. Law student (LL.M level)

The student needs to be familiar with the area of internet law with special interest for cyber security. Fortunately, yearly 40-50 students enroll for the Law Master Internet, IP & ICT at VU. The student should analyse the legal aspects from the Wassenaar Agreement as well as relevant criminal and public international law. For a proper legal analysis understanding of the object studied is essential. For which the input from computer scientists is essential. Affinity with technical issues is required, and a plus would be some hands on or related experience with technology.

Collaboration

Proposed research takes place at exactly the intersection between Law and Computer Science, requiring deep understanding of both legal issues (analysing existing legal norms and suggesting new ones where necessary) and the tools, techniques, and practices used in the security and the analysis of software. The participating groups have long agreed on the need for a cross-disciplinary approach in the research conducted by both, this crucial collaboration is also emphasised by i.a. the National Cyber Security Research Agenda[5] and the KNAW[6]. Different angles used in both disciplines resulted in a lack of solid common ground, which has made it

[4] https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items
[5] https://iipvv.nl/sites/stw.demo.infi.nl/files/mediabank/NCSRA-II.pdf
[6] https://www.knaw.nl/nl/adviezen/adviezen-en-verkenningen/lopende-adviezen/ethische-en-juridische-aspecten-van-informaticaonderzoek

difficult to cooperate in their shared research interests and write joint research proposals for NWO or similar funding bodies.

Besides the intended research results, the Academy Assistants will forge longer-lasting ties between the research groups that will generate knowledge for the *supervisors*. Such growing knowledge and the involvement and interaction of the faculty will stimulate further collaboration, e.g. joint research proposals.

The main reason why we believe the collaboration to be successful is that both groups are convinced that it is *essential* to advance their research. Bos' group has repeatedly encountered exactly the issues that form the proposed research topic. Which was the case in the ERC proposal, even already accepted the project was delayed *by almost a year* due to dual-use issues. It now operates with an ad-hoc committee to monitor the release of potentially sensitive material and information. Similarly, previous research interests in Lodder's group on cyberwar and proposed legislation that allows the police to "hack back" (attack the criminal infrastructure by means of hacking) was being hampered by generally available knowledge of the technical details of such infrastructures and potential attacks. Both groups have reached the point that they *need* to gain experience in each others' disciplines.

Deliverables

- Brief summary of current information security research tools, classification based on key characteristics
- Qualification of identified categories of tools under the proposed normative framework (Wassenaar Arrangement, the EU and US export control regimes) leading to determination (in-scope, out-of-scope)
- Summary of the mission statement of the Wassenaar Arrangement in respect of Dual Use Goods (incl. key criteria driving classification)
- Summary of the rationale driving inclusion of information security tools under recent changes to the Wassenaar Arrangement controlled goods list
- Synthesis and proposal for any improvements

Planning

Throughout the project, the students will join alternate between meetings in the Computer Science department and the Law Faculty, in which all supervisors will also be present.

- M1-M3: Study of Wassenaar Agreement (WA) and a reading list compiled by both of the groups (and therefore consisting of papers from both disciplines), followed seminar for both groups

- M4-M6: Report about the implications of the WA from both a legal and computer science perspective. Establish contact with other researchers around the world who study and/or comment on the WA.
- M7-M10: Criticism and proposed improvement of WA. Request feedback from other researchers.
- M10: Closing seminar for both groups.