Surveillance, Software, Security, and Export Controls

Reflections and recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting

Draft report
by

Thomas Dullien
Vincenzo Iozzo
Mara Tam

The authors thank the many members of the regulatory, human rights, and information security communities on both sides of the Atlantic who have reviewed and commented on this report. Its recommendations are the product of continuing and exceptional collaboration among these groups.

WA-CAT4 DRAFT
02-10-2015

Contents

Contacts

Supporting Documents

Surveillance, Software, Security, and Export Control

Background

In December 2013, the Wassenaar Arrangement Plenary Meeting ratified proposals from the UK and France aimed at curbing the transfer of commercial surveillance software products and IP network surveillance systems. These are known to have been employed by sovereign governments engaged in repressive activities against their citizenry, contributing to numerous human rights abuses.[1] The introduction of these new entries, 4.A.5., 4.D.4., 4.E.1.c., and 5.A.1.j., to the Control List remains highly exceptional. The Wassenaar Arrangement (WA) was never intended as an instrument of mitigation for human rights concerns,[2] and the Plenary Meeting had not previously been tasked with implementing controls in Category 4 or Category 5-pt.1 for this reason. Lacking a precedent for controls in these categories, for this purpose, it is to be expected that modest adjustments are required.

"Intrusion software" and information security

In their current form, entries 4.A.5., 4.D.4., and 4.E.1.c. do not identify a viable point of control. The current definition of "intrusion software" – upon which these entries are dependent – is constructed such that numerous security practices and tools are captured, while several classes of malicious software highly relevant to commercial surveillance products are not.

Somewhat counterintuitively, defensive security measures increasingly bear the attributes of offensive technologies; "offensive security", "penetration testing", and "red teaming" are just a few of the common descriptors for defensive practices demonstrating this logic. This convergence of offensive and defensive technology leaves few viable points of control for the former which do not also impair the latter. We see this difficulty in the existing mechanisms of capture for entries 4.A.5., 4.D.4., and 4.E.1.c.; these are trained on

---

[1] *See*, e.g., Karen McVeigh, 'British firm offered spying software to Egyptian regime – documents,' *The Guardian*, 28 April 2011. http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher; Morgan Marquis-Boire and Seth Hardy, "Syrian Activists Targeted with BlackShades Spy Software," *The Citizen Lab*, Research Brief No. 6 (June 2012), https://citizenlab.org/wp-content/uploads/2015/03/Syrian-Activists-Targeted-with-BlackShades-Spy-Software.pdf; Morgan Marquis-Boire, "Backdoors are Forever: Hacking Team and the Targeting of Dissent," *The Citizen Lab*, Research Brief No. 12 (October 2012), https://citizenlab.org/wp-content/uploads/2015/03/Backdoors-are-Forever-Hacking-Team-and-the-Targeting-of-Dissent_websitepdf.pdf

[2] The Wassenaar Arrangement, *Basic Documents* (Vienna : The Wassenaar Arrangement Secretariat, Jan. 2015), 1-3, 8, http://www.wassenaar.org/publicdocuments/2015/WA-DOC%20(15)%20SEC%20001%20-%20Basic%20Documents%202015%20-%20January.pdf. Hereafter *WA-DOC (15) 001 - Basic Documents*. *See* Annex I.

technical attributes which are – without exception – *common* to both commercial surveillance products and to information security tools.

Effects and side-effects

Participating States are struggling to effectively implement these new Category 4 entries. It is becoming more and more clear that their current mechanisms of capture do not produce controls of the intended scope or efficacy. In their current form, entries 4.A.5., 4.D.4., and 4.E.1.c. cannot meet their human rights objectives without placing a significant, additional burden on activities and tools vital to national and international security. It is proving similarly impossible to safeguard these same security interests without severely compromising the human rights objectives which motivated the addition of these entries to the Control List in the first place.

Implementations of 4.A.5., 4.D.4., and 4.E.1.c. by Participating States *are* capturing offensive security techniques and tools, as well as threat information sharing activities.[3] In the absence of adjustments to the existing WA criteria for control, there are only two ways for Participating States to avoid unintended negative consequences for security interests arising from implementation. One is through a series of exceptions and carve-outs which leave virtually nothing within the scope of these entries. The other is through licensing standards so excessively generous that they do not meaningfully impact the transfer of commercial surveillance infrastructure.[4]

---

[3] Recent guidance from the UK Department for Business, Innovation & Skills' Export Control Organisation (BIS/ECO) is instructive on this point. BIS/ECO clearly indicate that these entries *are* relevant to vulnerability disclosure, and that they do impose strict limits on the extent to which a proof-of-concept (PoC) may be elaborated in the course of reporting to a vendor either directly, or through a bug bounty program. It is important to note that closed vulnerability disclosure involving an exploit and PoC is indistinguishable from threat information sharing among – and sometimes within – private sector entities. Worryingly, BIS/ECO also presume that security professionals sharing samples of malware, or malware command and delivery platforms, whose cryptographic features surpass the threshold for control under WA Category 5-pt.2 have been obtaining export licences for each instance of transfer. BIS/ECO's guidance is indicative of the extent to which these entries, in their current form, are incompatible with time sensitive or real-time threat information sharing. UK Department for Business Innovation and Skills, Export Control Organisation, Notice to Exporters 2015/24 : *Intrusion Software and Export Control*, 10-08-2015, http://blogs.bis.gov.uk/exportcontrol/files/2015/08/Intrusion-Software-Tools-and-Export-Control1.pdf. *See* Annex III.

[4] Following the EU-wide implementation of the 2013 Plenary Meeting Agreements in December 2014, Italian authorities are known to have granted a global export license to at least one commercial surveillance and intrusion software vendor, Milan-based Hacking Team. *See* Antonello Vitale to David Vincenzetti, "A: Situation HT SRL," 18 November 2014 (Email-ID 158220), https://www.wikileaks.org/hackingteam/emails/emailid/158220; David Vincenzetti to Stefano Molino, *et al*., "Re: Clausola CATCHALL, Aggiornamento, Ieri martedì 4 a Roma," 19 November 2014 (Email-ID 174537), https://wikileaks.org/hackingteam/emails/emailid/174537.

Recommendations

The amendments proposed below *harmonize scope with intent*, and achieve what the existing language does not: clear, viable points of control relevant to commercial surveillance and monitoring tools, but not relevant to the tools and practices of information security.

We, the authors and undersigned, strongly advise that the enclosed amendments be reviewed and adopted by the 2016 WA Licensing and Enforcement Officers Meeting, and ratified by the 2016 WA Plenary Meeting.

Yours &c.,

Thomas Dullien
Vincenzo Iozzo
Mara Tam

Proposed Amendment

Overview

The Wassenaar Arrangement presently understands “intrusion software” to be indicated by qualities of design or modification for the purposes of avoiding detection by ‘monitoring tools’, or for the defeat of ‘protective countermeasures’. However, such attributes – by design or modification – are found in a wide variety of analytic, system administrative, and security tools. These qualities cannot be used to distinguish between malicious and innocuous software, as they are thoroughly common to both.

Authorization and ownership

In order to accomplish that distinction, it is necessary to introduce specifications of authorization and ownership. “Authorization” is here understood to be an affirmative indication of comprehension regarding the nature, implications, and future consequences of an action, and agreement to the execution of that action. The circumvention of owner or administrator authorization, by design or modification, in order to run or install “software”, when combined with the narrowing criteria indicated by 1.a. and 1.b., is an effective identifier for many classes of malicious software, some of which are not captured by existing language.

The human rights nexus of 4.A.5., 4.D.4., and 4.E.1.c. is, as noted, exceptional in terms of the Wassenaar Arrangement’s declared scope and purpose. Exceptional, too, is the great extent to which these items are defined by end-user and end-use. WA mechanisms of capture typically target technical qualities or parameters which can be linked with a measure of confidence to a particular use. No such technical qualities or parameters exist which can differentiate between the items targeted for control by these entries, and a wide variety of tools and practices essential to ICT security.

Embracing the targeted items’ distinction by end-use and end-user, we propose to qualify ***authorization*** to run or install “software” by source: the ***owner or ‘administrator’*** of the computer or network-capable device. Because some of these items are, by design, instruments for “lawful interception” (LI), the unqualified criteria of “authorized” or “unauthorized” are not suited to the purpose of their control.[5] Qualifying authorization in the manner proposed ensures that LI systems and software remain within the scope of control.

[5] Among the items targeted for control by these entries are systems and software designed for use in lawful interception (LI) activities by government end-users. In the case of these items, the critical question to be answered is : “authorized by whom?”. Authorization for the use of LI systems and software is granted by their government end-users, making unqualified authorization an unsuitable mechanism of capture. By specifying the circumvention of authorization granted by an owner or administrator of the relevant computer or network-capable device, we ensure that these items do not escape capture.

Exfiltration

The specification of data extraction or exfiltration is central to the amended definition of "intrusion software." Though the extraction specification may appear to risk capture of innocuous software elements (e.g. cookies), this is not the case. Both the rationale for targeting extraction as a behaviour and the technical factors which release web ads and other e-commerce elements from capture are thoroughly documented elsewhere.[6]

This document proposes a concrete amendment to the WA Control List with the objective of strengthening the efficacy of these entries in their original intent (i.e. export control of key-ready surveillance infrastructure), while also preventing unwanted negative side effects to security interests. These proposals include one amendment to 4.E.1.c., and several amendments to the definition of "intrusion software".

Changes to the Control List

Entry 4.A.5.

Original text:

> 4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery, or communication with, "intrusion software".[7]

Proposed change:

> No change.

Entry 4.D.4.

Original text:

> 4. D. 4. "Software" specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".[8]

Proposed change:

> No change.

---

[6] Sergey Bratus, D J Capelis, Michael Locasto, and Anna Shubina, "Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It," *Sergey Bratus* (Dartmouth College faculty page), 4-5, http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf.

[7] The Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List* (Vienna : The Wassenaar Arrangement Secretariat, 23 March 2015), 73, http://www.wassenaar.org/controllists/2014/WA-LIST%20%2814%29%202/WA-LIST%20%2814%29%202.pdf. Hereafter, *WA-LIST (14) 2 25-03-2015*. *See* Annex I.

[8] *WA-LIST (14) 2 25-03-2015*, 74.

Entry 4.E.1.c.

Original text:

c. "Technology" for the "development" of "intrusion software".[9]

Proposed change:

c. "Technology" ***specially designed or modified*** for the "development" of "intrusion software".

Definition of "Intrusion software"

Original text:

Cat 4 "Intrusion software"

1. "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:
    a. The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
    b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes

1. "Intrusion software" does not include any of the following:
    a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;
    b. Digital Rights Management (DRM) "software"; or
    c. "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.
2. Network-capable devices include mobile devices and smart meters.

Technical Notes

1. '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.
2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) or sandboxing.[10]

---

[9] *Ibid*.
[10] *WA-LIST 14 (2) 25-03-2015*, 212.

Proposed change:

Cat 4 "Intrusion software"

1. "Software" specially designed or modified to ***be run or installed without obtaining the authorization of the owner or 'administrator' of a computer or network-capable device***, and performing any of the following:
    a. The unauthorized extraction of data or information from a computer or network-capable device;
    b. The modification of ***system or user data to facilitate access to data stored on a computer or network-capable device by parties other than parties authorized by the owner or 'administrator' of the computer or network-capable device***.

Notes

1. "Intrusion software" does not include any of the following:
    a. Debuggers or Software Reverse Engineering (SRE) tools;
    b. Digital Rights Management (DRM) "software"; or
    c. "Software" designed to be installed by administrators or users, for the purposes of ***asset tracking, asset recovery, or 'ICT security testing'***.
    d. ***"Software" that is distributed with the express purpose of helping detect, remove, or prevent its execution on computers or network-capable devices of unauthorized parties.***
2. Network-capable devices include mobile devices and smart meters.

Technical Notes

~~1. '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.~~

~~2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) or sandboxing.~~

1. 'Authorization' means the informed consent of the user (i.e. an affirmative indication of comprehension regarding the nature, implications, and future consequences of an action, and agreement to the execution of that action).
2. 'Administrator': owner-authorized agent or user of a network, computer or network-capable device.
3. 'ICT security testing': discovery and assessment of static or dynamic risk, vulnerability, error, or weakness affecting "software", networks, computers, network-capable devices, and components or dependencies therefor, for the demonstrated purpose of mitigating factors detrimental to safe and secure operation, use, or deployment.

Discussion

Overview

It has been the experience of Participating States in the course of implementing 4.A.5., 4.D.4., and 4.E.1.c. that these entries unwittingly catch a wide variety of legitimate software tools and security practices, and do not contain clear or adequate mechanisms for their release. The authors further observe that the current definition of "intrusion software" does not capture several subclasses known to be highly relevant to commercial intrusion and surveillance systems.

This section assesses the current controls and provides a detailed examination of difficulties observed in their implementation.

Unintended capture

Contrary to the intent of the relevant controls and to the mission of the WA itself, these items *are* captured by the current entries 4.A.5., 4.D.4., 4.E.1a., and 4.E.1.c. and definition of "intrusion software". The proposed amendments, if adopted, would achieve these items' release from capture and possible control, providing badly-needed clarity to defenders.

1. **Commercial penetration testing tools** such as Core Security's Impact Pro,[11] Immunity's CANVAS,[12] and Rapid7's Metasploit Pro.[13]
2. **Exploits for vulnerabilities that are not part of a penetration testing framework**, such as bug reports including proof-of-concept (PoC) exploits, and threat information sharing activities.
3. **Threat information sharing activities** among – or within – private sector entities.
4. **Malware or rootkit samples** distributed among academic / independent researchers, or security personnel (i.e. defenders).

Implications of these items' capture and the proposed mechanisms for their release are discussed in detail below.

Commercial penetration testing tools

Penetration testing tools are designed to be used by the owners, owner-authorized agents, or owner-authorized users of computers or network-capable devices to perform security testing. Ownership of the relevant systems, devices, software, or equipment may be private or public, individual or corporate; these owners may in turn authorize agents and / or users of these digital and physical assets. The class of penetration testing tools indicated here is, generally speaking, intended and designed for use against systems,

[11] http://www.coresecurity.com/core-impact-pro

[12] https://www.immunityinc.com/products/canvas/

[13] http://www.rapid7.com/products/metasploit/

devices, software, and equipment under corporate ownership, with consent of a target (i.e. authorized user) or administrator (i.e. authorized agent). To fully clarify the exempt nature of these tools, they have been specified in Note 2.c. of the proposed amendment to the definition of intrusion software.

Exploits for vulnerabilities that are not part of a penetration testing framework

PoC exploits are commonly required by software vendors or bug bounty providers in the course of reporting. A fully elaborated PoC serves to establish the severity of the vulnerability it exploits; the information contained within a PoC is critical to both mitigation and remediation. Vendors are sometimes reluctant to allocate resources to developing a patch if the severity of a vulnerability cannot be demonstrated by the reporting party, and for fully deployed software in the maintenance phase of its lifecycle, it can be costly for them to develop and deploy such patches. No law requires vendors to develop and deploy software patches, even if its users are vulnerable without them. A PoC that clearly demonstrates the significance of the vulnerability is more likely to motivate vendors to patch, in order to preserve their reputation with users.

Even if a vendor chooses to publicly report a given vulnerability, publication of associated PoC exploit(s) is extraordinarily rare.[14] These can contain highly sensitive information (e.g. intellectual property, or information of strategic value to an adversary) which would present an unacceptable security risk if made public. In these cases of private or 'closed' disclosure, PoC exploits are not released by the General Technology Note and may well meet the threshold of control under current entries 4.E.1.a. or 4.E.1.c. In cases where a PoC is not released by the GTN, BIS/ECO's guidance presumes that a 'minimal' PoC would provide sufficient information for a vendor to conduct an accurate assessment and determine a course of action.[15] In practice, this is almost never possible.

In order to avoid control as "technology" for the development of "intrusion software", a PoC cannot contain a defeat for 'protective countermeasures' or 'monitoring tools' if it also describes the execution of external instructions. Though this may seem a reasonable threshold for control, it ignores or misunderstands the ubiquity of the technical elements from which it attempts to construct a viable choke point.

[14] One notable exception in this practice is Google's Project Zero.

[15] According to BIS/ECO's guidance, "A bug report that describes a defeat for 'protective countermeasures' and a modification to the standard execution path of a program would be controlled as "technology" if it allowed the execution of external instructions. If instead the only outcome described was to launch a calculator process then this is unlikely to be controlled. [...] If the terms of payment [of a bug bounty program] require a description of how such a proof of concept works then that description could well meet the technology control if the proof of concept met the definition of "intrusion software"." *See* Annex II.

One ‘protective countermeasure’, Address Space Layout Randomization (ASLR), is so ubiquitous that descriptions of its defeat are virtually requisite in any functional PoC on any platform. While sandboxing is not widespread outside of mainstream desktop and mobile platforms, it has achieved ubiquity in that category. Consequently, PoC exploits for mobile frequently describe both defeats for ASLR and the escape or bypass of a sandbox. The net of capture created by these criteria is, then, overly broad. The subsequent criteria of ‘execution of externally provided instructions’ (i.e. arbitrary code execution), does not usefully narrow the scope of capture. On modern platforms, local privilege escalation (LPE) is not normally dependent on an executable component, whether provided externally or internally.[16]

In short, a PoC is all but guaranteed to describe defeats or bypasses of ‘protective countermeasures’ or ‘monitoring tools’, but may or may not describe the ‘execution of externally provided instructions’. There is no possible control derived from these elements (with or without the technically indeterminable ‘modification of [a] standard execution path’) which does not impose an unacceptable burden of compliance on defenders while failing to capture technologies relevant to the entries’ intent.

The proposed amendments are both more comprehensive and more targeted in their capture and control of relevant technologies. By specifying the control only of “technology” ***specially designed or modified*** for the development of “intrusion software”, scope and intent are harmonized such that defenders are relieved of that burden of compliance.

Threat information sharing

Threat information sharing activities among – or within – private sector entities are similarly at risk of control under the existing entries. Excepting the speed with which they are conducted, there is little-to-no practical distinction between ‘threat information sharing’ and ‘closed vulnerability disclosure featuring a PoC exploit’, as described above.

Partnerships among private sector entities in the realms of energy (including nuclear), telecommunications, and other critical sectors, have long been encouraged in support of international peace, security, and stability. A recent United Nations Government Group of Experts (GGE) report on ‘Developments in the Field of Information and Telecommunications in the Context of International Security’ brings a mature strategy of security through cooperation to the world of information and communications technologies (ICTs). However, of the GGE’s findings and recommendations, a plurality are captured – or apparently captured – by 4.A.5., 4.D.4., 4.E.1.a., or 4.E.1.c. as derived from the current definition of “intrusion software”.[17] The GGE notes the importance of “private sector,

[16] This pattern reflects the relatively greater prevalence of kernel over userland exploits; the latter can require an executable to achieve LPE, but this approach is increasingly rare.

[17] *See* Annex III. United Nations, General Assembly, *Report of the Governmental Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International*

academia, and civil society organizations" to confidence and capacity-building activities in ICT security, as well as to programs of mutual assistance throughout the world.[18]

Indications that current WA controls may have a chilling effect on mutual assistance, confidence, and capacity-building activities have already been observed. Mobile Pwn2Own, the mobile-centric edition of a long running hacking contest sponsored by Hewlett Packard's Zero Day Initiative (ZDI), was recently pulled by HP/ZDI from Tokyo's PacSec security conference. Researchers at Pwn2Own events demonstrate novel compromises and disclose threat information (i.e. vulnerability reports and supporting PoC exploits) to affected vendors *through* HP/ZDI. An HP senior manager for threat research stated that HP's own legal and compliance experts were unable to clearly discern when WA-mandated export licenses would be required, how they could be obtained, or how they would be managed.[19] HP/ZDI have indicated concerns over WA controls as the sole motivation for their decision.

WA controls present significant difficulty for this type of multi-stakeholder, multinational disclosure process. While the loss of a hacking contest may not appear significant, one finds the same or very similar disclosure processes in mutual assistance and incident response programs. From financial and security services to nuclear power, telecommunications, and water / sanitation systems, ICT elements are implicated in the security and safe operation of every category of critical infrastructure. The burdens of uncertainty and compliance imposed on threat sharing activities within these sectors by current WA controls are no less unacceptable for being unintended.

Again, threat information sharing activities are currently at heightened risk of capture due to their confidential nature, and to the ease with which they may surpass current thresholds of control. The impact of control on these activities carries potentially catastrophic consequences, particularly for transfers which must occur in real-time (e.g. incident response).

Security, A/70/174 (New York : UN, 22-07-2015), § IV(16)c-d, § IV(17)a, c-e, § V(21), http://www.undocs.org/A/70/174.

[18] *Ibid*., § V(21)g. Notably, in the US, information sharing has been a recent feature of both the Legislative and Executive policy agenda. Two bills in the House of Representatives and a bill in the Senate seek to incentivize cyber threat information sharing. In the Executive branch, Executive Order 13636, Presidential Policy Directive 21, Executive Order 13691, standards and best practices for information sharing and analysis organizations, and the Automated Indicator Sharing Initiative have all been hallmarks of the Obama Administration's cybersecurity policy. These Wassenaar controls would significantly hinder the effectiveness of these other policy initiatives.

[19] Michael Mimoso, "Citing Wassenaar, HP Pulls Out of Mobile Pwn2Own," *Threatpost*, 4 September 2015, https://threatpost.com/citing-wassenaar-hp-pulls-out-of-mobile-pwn2own/114542/.

Malware or rootkit samples

The original phrasing put defensive researchers at risk, as malware samples could easily be classified under “intrusion software” or as software “designed to interact with intrusion software”. The new wording carves out a specific exemption for defensive sharing of software.[20] More work is required to define clear exemptions for the sharing of malware samples, and for defensive work on malware command and control servers.[21]

Unintended release

These are items *not* currently captured by 4.A.5., 4.D.4., 4.E.1.a., and 4.E.1.c., but which are of clear significance to the human rights objectives of these entries.

1. **Malicious or modified smartphone apps**
2. **Attacks that disable encryption functionality on devices for later acquisition**
3. **Rootkits that are hypervisors**

If implemented, the proposed amendments would capture these items and bring them within the scope of control.

Malicious or modified smartphone apps.

The existing entries and definition of “intrusion software” do not catch the simple installation of a backdoored application, or the backdooring of normal applications during their download. Such applications, and systems or software that communicate with them, are captured by the proposed amendments..

Attacks that disable encryption functionality on devices for later acquisition.

Software that is installed with physical access to a device that does not itself extract data, but which retains this data to facilitate later retrieval is not captured by the current definition of “intrusion software”. The proposed amendments capture these attacks, which are a very real threat to users under oppressive regimes.[22]

Rootkits that are hypervisors

The original wording excluded hypervisors too broadly - the sheer fact that something is a hypervisor could have exempted surveillance software under the old ruling. This has been addressed.

---

[20] Defensive sharing is not only helpful in analyzing endpoint infections, but also the command, control, and delivery structures for those infections. In some cases, defenders may be authorized to undertake the location, tracing, analysis and, if applicable, mitigation of control components for “intrusion software” on remote servers. Sharing of this threat information surpasses the threshold for control under the current entries.

[21] *See* n. 3.

[22] *See*, e.g.,

Assessing the current controls

In evaluating the Category 4 controls targeting intrusion and surveillance items, it is instructive to revisit the Wassenaar Arrangement's own 'Criteria for the Selection of Dual-Use Items'.[23] While certain commercial intrusion and surveillance systems certainly qualify as 'major or key elements for the indigenous development, production, use or enhancement of military capabilities,'[24] these items, and the technologies required for their development, are not clear candidates for control as dual-use items. The further criteria specified by the WA against which dual-use items are to be evaluated for selection are

- Foreign availability outside Participating States.
- The ability to control effectively the export of goods.
- The ability to make clear and objective specification of the item.
- Controlled by another regime.[25]

Foreign availability outside Participating States.

Though a particular surveillance *product* may not be available outside of Participating States, that fact has little or no bearing on the foreign development or abuse of surveillance *capabilities*. This is an important point of distinction. While high-profile commercial systems such as FinFisher's FinSpy or Hacking Team's Galileo / RCS have been of predominantly European or North American origin, their role in the oppressive surveillance behaviours WA controls seek to mitigate is frequently misunderstood. These products do not, on their own, impart surveillance capabilities where none have previously existed.[26] Consequently, the question of their control by WA is not a referendum on the provision or denial of surveillance capabilities generally, but rather on the effect of these products to improve the user experience and reliability of targeted access operations (TAO), lowering the barrier to entry for less-skilled operators.

---

[23] *WA-DOC (15) 001 - Basic Documents*, 71. *See* Annex I.
[24] *Ibid.*
[25] *Ibid*.

[26] The regimes identified as having abused these products are regimes which have also compromised all communications infrastructure – nationalised or private – of any value to their security services. Increasingly, this type of backbone or mass surveillance is being leveraged for targeted operations through the introduction of schemes to produce high-fidelity associations between individuals and their devices (e.g. mandatory registration of SIM cards with biometric data). *See* Vincenzo Iozzo, remarks presented at "Real digital security: How to modernize the EU´s export control regime and the trade in zero-day vulnerabilities," meeting convened by MEP Marietje Schaake (Brussels: 30 September 2015), https://drive.google.com/file/d/0B3NL8jkEQKjYcnp5aUtsSVRoQjA/view?usp=sharing; Mara Tam, "ICT surveillance methods in third countries," 28-09-2015, https://drive.google.com/file/d/0B5malB1BoDJ1TWJRQ0ExX1N1dWM/view?usp=sharing.

Relevant to the question of foreign availability is the fact that commercial intrusion and surveillance products are not particularly sophisticated or difficult to develop. Commercial off-the-shelf (COTS) solutions offer convenience, but the restriction of available products is likely to result in proliferation through locally-developed capabilities. Capabilities development outside of WA Participating States is not contingent on the transfer of knowledge or expertise from Participating States to foreign markets.

The ability to control effectively the export of goods.

Effectively controlling the export of commercial intrusion and surveillance items from Participating States is predicated on the revision of existing controls, particularly the WA definition of “intrusion software”. As written, current mechanisms of capture are overly broad and inappropriately targeted. These impose unacceptable burdens of compliance on security practices and tools while permitting a number of highly relevant technologies to escape control.

With adjustments, it is possible that export controls on intrusion and surveillance products could achieve a degree of efficacy without these undesirable side-effects. However, the ability to effectively control the export of these items is not a significant barrier to their proliferation. Local capabilities development of this type will not be responsive to export controls. In these and all cases where significant risk of abuse is present, cooperative measures aimed at reducing dependence on these tools, increasing the transparency of their use, and encouraging responsible State behaviour should be encouraged.

The ability to make a clear and objective specification of the item.

Confusion over the scope of the current Category 4 controls targeting intrusion and surveillance items across a number of implementations indicate that they are not sufficiently clear in their specifications. Paradoxically, this lack of clarity may be a side effect of WA’s traditionally technical (i.e. ‘objective’) criteria for capture and control. This focus on technical attributes has produced effective controls in many categories, but cannot do so in the present case for the simple reason that intrusion and surveillance systems are technically indistinguishable from a wide variety of security, system administrative, and analytic tools.

Controlled by another regime.

Country-specific sanctions and embargoes are among the instruments available to Participating States for the export control of intrusion and surveillance items. Whether or not these measures – or indeed WA itself – are adequately nimble to address changing human rights concerns arising from the deployment of these technologies in destination countries is yet to be determined.

Standards and objectives

A recently-adopted report by the European Parliament's Committee on Foreign Affairs contains further guidance on the scope and impact of export controls targeting "dual-use" ICT products.[27] Among the recommendations of the Report are several excellent standards and objectives for the implementation of export and other controls intended to restrict the transfer of dual-use ICT products.

Do no harm

> 36. [...] calls on the Commission to include effective safeguards to prevent any harm of these export controls to research, including scientific and IT security research;[28]

Recognizing the significant, increasing degree to which ICT elements are responsible for the secure operation and provision of critical infrastructure, policy makers and regulators in this area must ensure that their efforts *do no harm* to the practices and tools vital to ICT security research. ICT security as a discipline is unique in the extent to which leading research is conducted and shared independent of academia or industry. The needs of independent researchers as a class are not well defined. Consequently, these needs are not well understood by regulators. There is much work to be done in this area.

Guard against the chilling effects of ITT controls

> 51. Stresses that any regulatory changes aimed at increasing the effectiveness of export controls of intangible technology transfers must not inhibit legitimate research, or access to and exchange of information, and that any potential measures, such as the use of EU General Export Authorisations for dual-use research, should not have a 'chilling effect' on individuals or SMEs;[29]

Threat information sharing activities, vulnerability disclosures, and research in the area of ICT security must be unambiguously protected from potential chilling effects. Safeguarding "access to and exchange of information" by defenders for the purposes of investigating present and future developments in ICT security must be a priority when formulating regulations in this area.

---

[27] European Parliament, Committee on Foreign Affairs, "Report on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries,'" A8-0178/2015 03-06-2015, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bREPORT%2bA8-2015-0178%2b0%2bDOC%2bPDF%2bV0%2f%2fEN, Hereafter *A8-0178/2015*. *See* Annex III.

[28] A8-0178/2015, 12.

[29] *Ibid.*, 13.

> 52. Calls on the Member States to ensure that existing and future export control policies do not restrict the activities of legitimate security researchers, and that export controls are applied in good faith, and only to clearly defined technologies intended to be used for mass surveillance, censorship, jamming, interception or monitoring purposes, or for tracing and tracking citizens and their activities on (mobile) telephone networks;[30]

Clear, comprehensible regulations and industry outreach by regulators can minimise potential chilling effects. Regulators, SMBs, and independent researchers should work collaboratively to ensure that such outreach activities are responsive to the needs of these demographics.

Encourage ICT security in order to advance human rights

> 57. Underlines the need to avoid unintended consequences, such as restrictions or chilling effects on scientific and other types of bona fide research and development, on the exchange of and access to information, on the development of security knowledge or on the export of technologies that are in the interest of acquiring the requisite digital skills and of advancing human rights;[31]

This report has documented the extent to which "exchange of and access to information" are impacted by the current entries and definition of "intrusion software". Detrimental effects to capacity-building activities in ICT security are likely, and it should be noted that systemic resilience to certain commercial surveillance systems would be significantly impaired as a result. Improvements to ICT security capacity are an indispensable element for the advancement and protection of human rights in third countries; negative impacts in this area should be a source of grave concern.

Realign legislation to reflect the realities of research

> U. whereas the introduction of export controls should not harm legitimate research into IT security issues, or the development of IT security tools, where there is no criminal intent;[32]

"Legitimacy" is a thorny concept in ICT security research. The absence of exclusions for security research in legislation such as the European Computer Programs Directive make it exceedingly easy for researchers to commit statutory violations in the absence of criminal purpose. Tying legitimacy to the absence of criminal intent represents a welcome step forward in the establishment of protections for researchers against specious prosecution and sanctions.

---

[30] *Ibid*.

[31] A8-0178/2015, 14.

[32] *Ibid*., 7-8.

Though the current WA controls on intrusion and surveillance items require adjustment to meet its own high standards, and those of the Participating States, the authors believe that the amendments proposed in this document will achieve that result.

Author Contacts

Thomas Dullien
thomas.dullien@googlemail.com
0xC43901609EA5B0D9
@*halvarflake*

Vincenzo Iozzo
vincenzo.iozzo@gmail.com
0xB64451CE3E642AED
@*_snagg*

Mara Tam
marasawr@gmail.com
0xA4EC11D1CEC8AD26
@*marasawr*

Subject Matter Experts Directory

At every stage in this writing process, the authors have encountered the need for much improved communications on regulatory and policy matters between the information security community and public servants.

In part this is a question of coordinating subject matter experts wishing to engage on these issues with regulators and policy makers. But, equally, it is a question of growing that pool of experts to better reflect the diversity of analysis and opinion within the information security community.

To that end, we invite interested parties to subscribe to and participate on the following mailing lists created in support of this goal.[33]

Regs has been the home for discussions on implementations of the Wassenaar Arrangement 2013 Plenary Agreements since May 2015, but also covers EU-level export control reform.

Subscribe here : https://lists.alchemistowl.org/mailman/listinfo/regs

PolAd was launched in October 2015 to support the US National Telecommunication and Information Administration's (NTIA) multi-stakeholder process on vulnerability disclosure. However, the list is intended to host discussion of policy formation in new areas as they arise.

Subscribe here : https://lists.alchemistowl.org/mailman/listinfo/polad

[33] Though the mailing list format may seem antiquated, in the case of regs@ it has allowed for sustained engagement among a wide variety of participants not limited by geographic location.