CONSIDERATIONS ON

WASSENAAR ARRANGEMENT CONTROL LIST ADDITIONS FOR SURVEILLANCE TECHNOLOGIES

Authored by Collin Anderson

TABLE OF CONTENTS

ACKNOWLEDGEMENT

We would like to thank the numerous reviewers for their constructive feedback on earlier versions of this paper, including Jochai Ben-Avie, Peter Harrell, and Sarah McKune. This does not imply their endorsement of the recommendations, only our appreciation for their willingness to critical challenge this lengthy work.

DISCLAIMER ON LEGAL ADVICE

The export controls agreed upon within the Wassenaar Arrangement are implemented at the national level, and methods or interpretations of controls may vary among states. Moreover, export control regulations depend heavily on the particular technical characteristics of the item for export. This document provides the author's perspective on the applicability of the cited language to the apparent functionality and features of certain technologies, and related policy issues. Moreover, several states maintain additional controls pertinent to such technologies, which are not discussed in this document. It is neither exhaustive nor conclusive, and does not constitute legal advice. Those seeking legal advice on the application of this language to particular exports should consult local legal counsel and their national export authorities.

EXECUTIVE SUMMARY

In December 2013, Wassenaar Arrangement member states agreed to implement export controls related to "Intrusion Software" and "IP Network Surveillance Systems."[1] While the announcement garnered attention from civil society organizations and export control professionals for its connection to human rights concerns, the new controls align with a deeper history of national regulation of similar technologies within member states, and is not the first round of privacy-related controls within the Wassenaar Arrangement Control List. Through a review of these two new controls, based on technical documentation of existing products, we find both to be narrowly-tailored to address a subset of technologies that have no purpose other than for support of surveillance regimes. Differences exist between the two on the level of specificity in their definition and necessary precautions in practice. Therefore, we extend this analysis to include recommendations on their implementation and note areas where authorities can ensure that export controls do not create an unintended chilling effect in pursuit of commonly agreed upon human rights objectives.

Both the United States and the European Union have imposed targeted sanctions against Iran and Syria regarding the proliferation of "sensitive technologies," equipment instrumental to Internet censorship and surveillance,[2] and the United Kingdom has controlled the sale of at least one Intrusion Software product based on its use of cryptography.[3] Moreover, legislative bodies in both regions have previously called for increased restrictions on surveillance and offensive intrusion equipment.[4] The additions also follow the inclusion of mobile interception equipment, otherwise known as IMSI catchers, in the Control List during the 2012 plenary session. [5]

The Intrusion Software and IP Network Surveillance controls represent two distinct types of definitions under different sections of the Control List, with the former under Category 4 (Computers) and the latter Category 5 Part 1 (Telecommunications). The Wassenaar Arrangement's language on Intrusion Software is a more broadly-defined control than IP Network Surveillance and others within the Computers category, which are often more precisely defined by quantitative performance metrics.

Based on a review of sales brochures, public accounts, and technical documentation, we find that both rules apply to a narrow subset of systems, rather than a broad suite of surveillance technologies; namely, those that are specifically marketed for support of intelligence activities, including:

1 http://www.wassenaar.org/publicdocuments/2013/WA%20Plenary%20Public%20Statement%202013.pdf
2 http://www.treasury.gov/resource-center/sanctions/Programs/Documents/13606.pdf
Council Regulation 36/2012, (enacted on the 18 January 2012) and Council Regulation 264/2012 (enacted 23 March 2012)
3 https://web.archive.org/web/20140816043703/https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma
4 http://www.gpo.gov/fdsys/pkg/BILLS-113s1197pcs/pdf/BILLS-113s1197pcs.pdf
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0470+0+DOC+XML+V0//EN
5 https://www.federalregister.gov/articles/2013/06/20/2013-14644/wassenaar-arrangement-2012-plenary-agreements-implementation-commerce-control-list-definitions-and#h-24

Intrusion Software:
- Systems and Equipment [4. A. 5.]: *FinFisher FinFly ISP and FinFly Net, HackingTeam Network Injector Appliance, FinFisher FinIntrusion Kit and FinFisher Tactical Network Injector, FinFisher FinUSB and FinFireWire*
- Software [4. D. 4.]: *FinSpy Agent and RCS Console, FinFisher FinFly Web, FinSpy Master and RCS Server*

IP Network Surveillance:
- Systems and Equipment [5.A.1.j.]: *ETI Group's EVIDENT Investigator, SS8 Communications Insight (Intellego), Area SpA MCR Studio, Amesys's EAGLE GLINT (Nexa Technologies SAS), AMECS's Analys, Narus nSystem, Vastech ZEBRA, Group 2000's Lawful Monitoring Centre, Glimmerglass CyberSweep Sapience, ATIS Klarios Monitoring Centre, Siemens Intelligence Platform, Verint Systems, AQSACOM Aqumen, Nice Systems.*

The Wassenaar Arrangement controls on systems, software, and technology related to Intrusion Software have proven to be controversial and poorly understood, in part due to the separation of the definition of Intrusion Software from the actual list of items controlled. FinFisher (formerly Gamma Group) and HackingTeam's catalogues and manuals provide illustrative examples of products targeted under the new rules, describing the relationship between the definition and the actual controls. Both companies develop software for remote access to computers and mobile devices – programs specially designed[6] to avoid monitoring and security measures in order to extract data and execute externally-provided instructions – Intrusion Software as per the Wassenaar Arrangement definition. These software products would not themselves be subject to export controls. Instead, the rule applies to the products designed to facilitate their use, including those as basic as the software for the administration of their Intrusion Software and the infrastructure for their operations. Similarly controlled would be the products designed to facilitate infection of targets, such as those that allow their customers to tamper with Internet downloads, create fake versions of popular websites, and take advantage of physical access in order to compromise devices. These infection systems, which are tightly integrated into specific remote access software and administration platforms, would be considered equipment specially designed for the delivery of Intrusion Software.

Neither control was designed to solve the totality of threats to privacy and national security. While a wide array of network management and surveillance equipment conduct analysis of Internet traffic, the ability to map relationships based on intercepted content, a requirement under the IP Network Surveillance control, is a highly sophisticated function that denotes a specialized product. Contrary to some expectations, there is no indication that the Wassenaar Arrangement language would apply to the deep packet inspection (DPI) equipment or lawful interception systems that have routinely evoked controversy when exported to countries that violate human rights. The narrowness of the IP Network Surveillance definition may be reflective of the uncertainty that export control authorities face in asserting administrative burdens on the sale of dual use network equipment. While such devices are frequently used for censorship, the same products are also commonplace in networks for caching of content, mitigating security threats and other purposes, even in countries with human rights challenges. Broad definitions pose the challenge of potential increasing licensing burdens for network equipment manufacturers, in a market where telecommunications vendors in non-Wassenaar Arrangement members states provide ample foreign competition with less self-restraint. More work will be necessary to construct controls that differentiate the misuse of DPI from legitimate deployments within telecommunications networks.

6 'Specially designed' in the Wassenaar Agreement defined term that cover items that as a result of their development have properties peculiarly responsible for achieving or exceeding the description within the control. Essentially, this raises the threshold for control, and therefore technologies that might have incidental use for a controlled purpose are less likely to be covered. **See Appendix for more.**

Moreover, due to the nature of the Wassenaar Arrangement's General Software Note, which exempts software that is publicly-available without the need for substantial support from the vendor, these controls will not regulate the open market for commonplace spyware sold in a near retail manner to individuals attempting to monitor children, spouses and others, though in the United States and other countries the sale of such software is regulated under other statutes. Both controls limit themselves to highly-professionalized systems of surveillance that are often only provided to government agencies and telecommunications companies, with little legitimate use outside of law enforcement and intelligence mandates.

The effectiveness of both Intrusion Software and IP Network Surveillance systems are dependent on their invisibility and unavailability to the general public, especially to avoid the reach of the security and antivirus research communities that might interfere with their operations. Manufacturers of both types of equipment also avoid sales that may run afoul of wiretapping statutes and restrict access to information on their use to only government customers. However, law enforcement intrusion and surveillance systems are also highly dependent on supplier support, including for integration into telecommunications networks, after sales service, and continuing updates. The enforcement benefit of this pre- and post-sales dependency is that these systems should bear less transshipment or reexport risk than most controlled items, as vendors will have the means to follow changes in customer needs, network placement, ongoing communications with update servers, and the ability to "know their customer,"[7] if encouraged by export control authorities.

The scope and section of the new controls are important factors in light of concerns within the computer security community on their potential to chill research, concerns that are motivated by negative experiences with cryptography restrictions. Notably, neither control relies on the use of encryption in products – neither are listed within the section that covers cryptography, Category 5 Part 2 (Information Security) – and the conflation of these technologies would be extremely ineffective to achieving either set of controls' ultimate objectives.[8] There is indication that special care was taken to limit potential overreach in the drafting of the Intrusion Software control. For example, the definition attempts to mitigate over-broadness through defining a set of exemptions, as well as not directly controlling Intrusion Software itself. Additionally, while the majority of the Wassenaar Arrangement's Controls for Technology[9] cover the 'development, production, or use' of controlled systems, the Intrusion Software's Technology controls only covers 'development' [4. E. 1. c.].

The design of Intrusion Software does not constitute a highly sophisticated or exclusive field of knowledge, and thus it would not benefit the objective of the control to regulate research that is not performed for the sole purpose of deployment of a commercial product. Moreover, we do not believe that the exploit or vulnerability market is covered under the definition of Intrusion Software. While exploitation is a common mechanism for the circumvention of protective and monitoring measures, it is not concomitant to intrusion nor is vulnerability research necessarily Intrusion Software development. Whether or not particular tools are appropriated by malicious actors, it remains in the interest of export control authorities to promote the availability of information security tools and not chill their development. Instead, the primary focus for export control authorities in the application of the Technology classification should be oversight of the consultative services that are rendered prior to or in support of the deployment of Intrusion Software.

7 https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment

8 **For more on this topic, see Recommendations for the Implementation of the 2013 Wassenaar Arrangement Changes Regarding "Intrusion Software" and "IP Network Communications Surveillance Systems" (May 2014)** http://oti.newamerica.net/blogposts/2014/human_rights_and_technology_organizations_submit_joint_recommendations_to_the_us_gove

9 Technology in the Wassenaar Arrangement is a defined term that covers a broad range of technical data and development assistance, **see Appendix for more.**

The exemptions under both Intrusion Software (for debuggers, software reverse engineering, digital rights management, and asset recovery) and IP Network Surveillance (marketing and network management) appear to be narrowly-defined and are unlikely to present significant short-term risk of relabelling by companies that may want to apply avoid scrutiny. For example, asset tracking, which most closely resembles the tracking function of Intrusion Software software, implies ownership of the device. It should not require the opaque behavior that necessitates bypassing security countermeasures or evasion of antivirus applications. Similarly, marketing equipment generally maintains an active presence on the network with limited inspection of content, inserting tracking code for the purpose of advertising, as opposed to passive interception and retention of all Internet traffic. In order to avoid the possible misuse of exemptions, it is important that export control authorities maintain an expectation about how exempted devices should operate in order to achieve the strict definition of a legitimate objective.

As export control authorities consider license applications and industry education, it is incumbent on them to ensure that these new regulations are narrowly applied to control equipment, software, and technologies that are substantially designed for surveillance, while not chilling research and work that is fundamental to the promotion of Internet security. In the process of determining the applicability of the control language in licensing determinations and pursuing enforcement actions, export control authorities should:

- Refrain from considering broad interpretations of Intrusion Software that might lead to attempts to regulate exploits or the vulnerability market;
- Issue specific guidance outlining the forms of scientific research and "Technology" covered by the Intrusion Software control;
- Consider consultations and post-sales support requirements within Intrusion Software and IP Network Surveillance license applications;
- Maintain technical expectations about how exempted systems should operate in order to achieve legitimate and narrowly-defined objectives;
- Review items not only based on their technical specification, but also their advertising material, integrations, partnerships, customers, network placement, passive operations, and end use;
- Promote standard red flags that employ the technical characteristics of network-connected products to mitigate transshipment risks, such as changes in customer needs, network placement, and ongoing communications with update servers;
- Consult with industry and civil society to promote implementation of "know your customer" policies that will reduce the potential for approved, or otherwise permissible, exports to misappropriated for the abuse of human rights.

The new Wassenaar Arrangement controls represent the recognition of an increasing need for export control authorities and private industry to limit the proliferation of sensitive technologies to bad faith actors. Clearly defined and well enforced Intrusion Software and IP Network Surveillance controls can lay the groundwork for a constructive and expansive role for export controls in the promotion of human rights and cyber security goals.

I. INTRUSION SOFTWARE

A. CONTROL LANGUAGE

WHAT IS INTRUSION SOFTWARE?

"Intrusion software" is software that is specially designed[1] to avoid detection by security monitoring tools (such as antiviruses or firewalls) or to defeat protective countermeasures (namely the memory protection functions of operating systems) in order to *(a)* extract or modify data of the device, or *(b)* allow the execution of externally provided instructions.

Intrusion Software **does not** include debuggers and software reverse engineering tools, digital rights management systems, or asset recovery software that is installed by manufacturers, administrators, or users.

Intrusion Software is not an item controlled under the Wassenaar Arrangement by itself. Rather, this control focuses on items that have a specified relationship with Intrusion Software, as follows:

WHAT IS CONTROLLED?

Does the item maintain the quality and relationship of being:

- equipment *[4. A. 5.]* or software *[4. D. 4.]* specially designed or modified to be used for the generation, operation, or delivery of, or communication with Intrusion Software?; or,
- 'technology,' such as technical schematics or technical assistance, necessary for the **development** of an Intrusion Software product. *[4. E. 1. c.]*?[2]

WHAT IS EXEMPTED FROM CONTROLS?

1. **For Software [4. D. 4.]:** Software that is generally available to the public (is available for free or purchase through unrestricted retail-style sales and does not require substantial support from the seller). ***[General Software Note]***
2. **For Technology [4. E. 1. c.]:** Technologies that are in the public domain or constitute basic scientific research **(see Appendix for more information)**. ***[General Technology Note]***

1 'Specially designed' in the Wassenaar Agreement defined term that cover items that as a result of their development have properties peculiarly responsible for achieving or exceeding the description within the control. Essentially, this raises the threshold for control, and therefore technologies that might have incidental use for a controlled purpose are less likely to be covered. **See Appendix for more.**

2 Technology in the Wassenaar Arrangement is a defined term that covers a broad range of technical data and development assistance**. See Appendix for more.**

WASSENAAR LANGUAGE (CATEGORY 4, COMPUTERS)

[From Wassenaar Arrangement Definitions]

Cat 4 "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.

NOTES

"Intrusion software" does not include any of the following:

- Hypervisors, debuggers or Software Reverse Engineering (SRcE) tools;
- Digital Rights Management (DRM) "software"; or
- "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery;
- Network-capable devices include mobile devices and smart meters.

TECHNICAL NOTES

'Technology,'[3] such as technical schematics or technical assistance, necessary for the development of an Intrusion Software product. [4. E. 1. c.]?

- **'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

[From Wassenaar Arrangement Control List]

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".
…
4. E. 1. c. "Technology" for the "development" of "Intrusion Software".

3 'Specially designed' in the Wassenaar Agreement defined term that cover items that as a result of their development have properties peculiarly responsible for achieving or exceeding the description within the control. Essentially, this raises the threshold for control, and therefore technologies that might have incidental use for a controlled purpose are less likely to be covered. **See Appendix for more.**

B. PRODUCT CONSIDERATIONS

PRODUCTS COVERED BY INTRUSION SOFTWARE DEFINITION

- **FinFisher FinSpy and HackingTeam RCS –** Software for surreptitious access to Internet-connected devices.

PRODUCTS COVERED BY CONTROL

- **FinFisher FinFly ISP and FinFly Net, HackingTeam Network Injector Appliance [4. A. 5.] –** Systems for the delivery of Intrusion Software over a network;
- **FinFisher FinIntrusion Kit and HackingTeam Tactical Network Injector [4. A. 5.] –** Systems for the delivery of Intrusion Software over a network;
- **FinFisher FinUSB and FinFireWire [4. A. 5.] –** Equipment for the delivery of Intrusion Software to a locally connected device;
- **FinFisher FinFly Web [4. D. 4.] –** Software for the delivery of Intrusion Software over a network;
- **FinFisher FinSpy Master, FinSpy Proxy and FinSpy Relay, and HackingTeam RCS Server [4. D. 4.] –** Software for the communication with Intrusion Software; and,
- **FinFisher FinSpy Agent and HackingTeam RCS Console [4. D. 4.] –** Software for the operation of Intrusion Software.

PRODUCTS NOT COVERED BY CONTROL

- **Metasploit (General Software Note) –** Penetration testing software that maintains the ability to use exploits to gain remote access to a device;
- **Private Exploitation Research (Not Intrusion Software, General Technology Note) –** Research in support of discovering vulnerability in systems;
- **Black Ice, Antivirus Products (Not Intrusion Software) –** Personal security software;
- **IDA Pro, Fuzzers (Debuggers) –** Software for the discovery of vulnerabilities and to conduct research on systems;
- **Jailbreak Software (General Software Note) –** Mechanisms for users to gain more privileged access to a system in order to install software and modify their own device in a manner that may be restricted by the vendor; and,
- **DarkComet RAT, Blackshades and other commercially-available spyware (General Software Note) –** Software that is openly sold in a retail manner to spy on other computer users.

C. DISCUSSION

The Wassenaar Arrangement's language on Intrusion Software represents a more broadly-defined control than others under the "Computers" category, which are often defined precisely by quantitative performance indicators rather than the operational behaviors found in the definition. This ambiguity has provoked fears that the controls regulated commonplace research, instead of concerns about missed technologies. The definition attempts to manage potential issues of over-broadness through defining a set of exemptions for software development tools, digital rights management, and asset tracking, as well as not directly controlling Intrusion Software itself. Notably, the Intrusion Software control does not rely on the use of cryptography, nor would such a strategy be effective. While the control's technical notes to the terms 'monitoring tools' and 'protective countermeasures' provide illustrative examples, their focus on memory protection and antivirus software also suggests that Wassenaar is primarily interested in

end-host security. The control is not designed to solve the totality of threats to information security and privacy, for example, it does not regulate the ample market for commercial malware that is sold to the general public. It also does not attempt to holistically control the broad range of software that may be used to compromise user data, such as tools designed to obtain user credentials via brute force attacks or to conduct forensics on seized devices. Finally, we do not believe the exploitation or vulnerability market is covered under the definition of Intrusion Software, and encourage export control authorities to refrain from misapplying the control to do so.

In recent years, security firms have marketed highly-professionalized systems of intrusion or remote control software to law enforcement and intelligence agencies. These products have catered to fears that criminals and other targets are "going dark," that they are less susceptible to traditional forms of surveillance due to increased use of encryption software and their mobility across networks or borders. As one such company argued, "if communications are encrypted, governments should use spyware-based wiretapping technologies (that is, offensive technologies) to foil tech-savvy criminals communications."[1] On review of sales material, user manuals and journalistic accounts, we find Intrusion Software items that align with the Wassenaar Arrangement definition provided by: ***FinFisher (formerly Gamma Group), HackingTeam, DigiTask, AGLAYA, RCS Lab, Gr Sistemi (Dark Eagle), Clear-Trail Technologies (QuickTrail), Stratign (Spy Phone), SS8 (Interceptor), iPS (ITACA).***

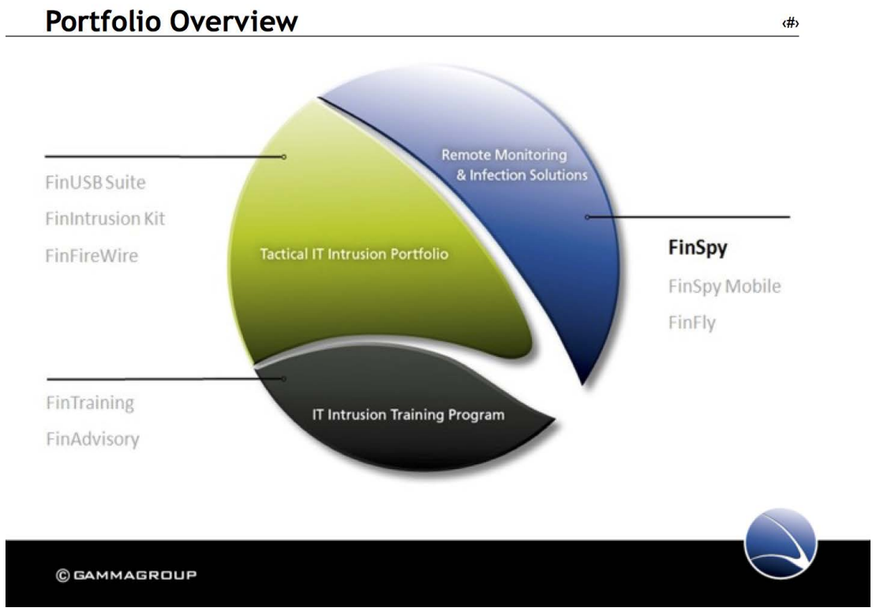
While the commercial products BlackShades and DarkComet have been used by state-affiliated actors to target dissidents and individuals abroad, the effectiveness of these products generally stems from the attackers' persistence and security failures on the part of the victims. 'Law enforcement' products bear striking differences from off-the-shelf counterparts, most significantly their highly-specialized support infrastructure to facilitate intrusion and avoid detection. In a sales presentation, HackingTeam claimed that Remote Control System (RCS), its line of Intrusion Software, "cannot be detected by any bugged computer user" and that "antivirus, antispyware, anti-key-loggers cannot detect our bug."[2] Commercial products may attempt to hide their presence through obfuscation of binaries and modification of system files, however, law enforcement systems go to greater lengths to ensure that infection agents cannot be detected after installation or during the extraction of information.[3] As documented by Citizen Lab,[4] prominent government-grade Intrusion Software vendors include features not found elsewhere, such as the use of unpublished exploits provided by partners (pertinent to the 'protective countermeasures' clause) and through proxy-chain exfiltration networks (evasion of 'monitoring tools'). HackingTeam even includes modules that allows the software to go silent when it detects that the host is engaging in monitoring that may disclose its presence, such as locally capturing outgoing network traffic.

The effectiveness of law enforcement Intrusion Software is also dependent on its unavailability to the general public, especially the security research community. The less that is known about such software, the more effective the product is at evasion of protective countermeasures and monitoring tools. Its efficiency is strongly correlated to the time between the release of a version of Intrusion Software to customers and when it is detected by antivirus products. Seeking to preserve legitimacy in a legally-challenging field, such companies also need to avoid sales that may run afoul of wiretapping statutes that regulate the use and sale of interception devices.[5] In its customer policy, HackingTeam states:

1 https://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf
2 https://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf
3 http://www.symantec.com/security_response/writeup.jsp?docid=2012-062906-4932-99&tabid=2
4 https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/
5 http://www.law.cornell.edu/uscode/text/18/2512

"We provide our software only to governments or government agencies. We do not sell products to individuals or private businesses."[6]

FinFisher makes the same claim, that its products "are sold to governmental agencies only," adding that they only target "individual suspects and can not be used for mass interception."[7] This differs from commercial malware products that are frequently made available in an unrestricted manner through a near-retail process that accepts mainstream electronic payment methods. The differing customer bases and services bear a price tag to match: whereas BlackShades costs $40 for unlimited use,[8] FinFisher requires a license for every target, at a cost of at least €1,170 per device.[9] This distinction between commercial and law enforcement intrusion products is pertinent to the General Software Note, which provides exemptions for products that are sold without restriction and without requiring significant support.



FinFisher and HackingTeam's product catalogues and user manuals,[10] made available late last year by transparency advocates, provide the most public documentation of the relationship between Intrusion Software and the types of products to be controlled under the Wassenaar Arrangement Control List. FinFisher's primary means for remote access to computers and mobile devices is its software agent

6 http://www.hackingteam.it/index.php/customer-policy
7 http://www.finfisher.com/FinFisher/products_and_services.html
8 http://www.symantec.com/connect/blogs/blackshades-coordinated-takedown-leads-multiple-arrests
9 https://www.wikileaks.org/spyfiles/docs/DREAMLAB-2011-FinFPric-en.pdf
10 **FinFisher:** https://wikileaks.org/spyfiles4/
HackingTeam: https://firstlook.org/theintercept/2014/10/30/hacking-team/

FinSpy. HackingTeam provides a suite of evidence collection software under the RCS brand with names such as *Galileo* and *DaVinci*. FinSpy and RCS qualify as Intrusion Software – programs specially designed to avoid monitoring and security measures in order to extract data and execute externally-provided instructions. As per the structure of the control, these software products would not themselves be subject to export restrictions despite being licensed on a per instance basis to an exclusive customer base. We can then elaborate on the systems and software designed to interact with this Intrusion Software in order to identify what is likely to be controlled under the new regime.

These remote access products are administered by the applications *FinSpy Agent* and *RCS Console,* which provide an administrative interface to the system that lists infection targets, displays collected analysis, and facilitates the creation or configuration of the Intrusion Software. FinSpy Agent and RCS Console would therefore qualify under all the characteristics laid out within Control 4. D. 4., as software "specially designed for the generation, operation or delivery of, or communication with, Intrusion Software."

To facilitate infection of targets, the primary hurdle to gaining access. FinFisher and HackingTeam offer a diversity of products that take advantage of different vectors, including network injection, mimicry of other websites, and physical access to target devices. While these tools are often built with off-the-shelf hardware, including name-brand USB storage devices and standard server equipment, they are specifically-modified for the purpose of staging the delivery of Intrusion Software. On their own, unmodified, these devices would not be controlled. However, these products are integrated as components of the intrusion system through proprietary means, which limits their potential legitimate use cases; as a part of an Intrusion Software system, they therefore encounter controls.

Amongst the most sophisticated staging platforms are FinFisher's *FinFly ISP* and HackingTeam's *Network Injector Appliance*, which are network devices that are placed within Internet Service Providers to insert Intrusion Software into normal files as they are downloaded. As HackingTeam's patent application describes this class of product:

"In many situations it can be useful to be able to install applications on networked remote terminals, or to modify applications being downloaded and installed from a network, even transparently to the users of such terminals. Consider, for example, the installation of control devices, capable of performing monitoring and notification of the operations performed at the terminal, ***in particular in the context of lawful interception activities*** *or the insertion of customized advertising content in applications downloaded by the user. For this purpose, devices are known which allow to modify network traffic on-the-fly: these devices are based on code injection techniques. These techniques allow to intercept and modify data packets in transit on the network during download on the part of the user who uses the terminal onto which one wishes to install the application, generally referenced as the target terminal."*[11]

(*FinSpy Proxy* and *FinSpy Relay*) and RCS provide 'anonymizing proxy' software dedicated to mask the nature and end destination of exfiltrated traffic (software specially designed for communication with Intrusion Software [4. D. 4.]).

11 http://worldwide.espacenet.com/publicationDetails/originalDocument?CC=CA&NR=2807011A1&KC=A1&FT=D&ND=4&-date=20120209&DB=worldwide.espacenet.com&locale=en_EP

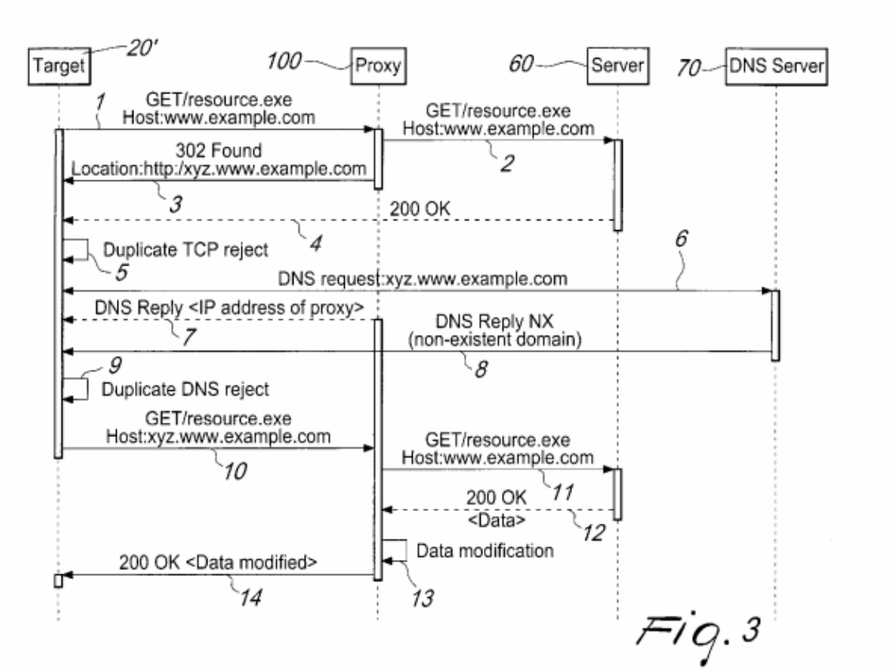
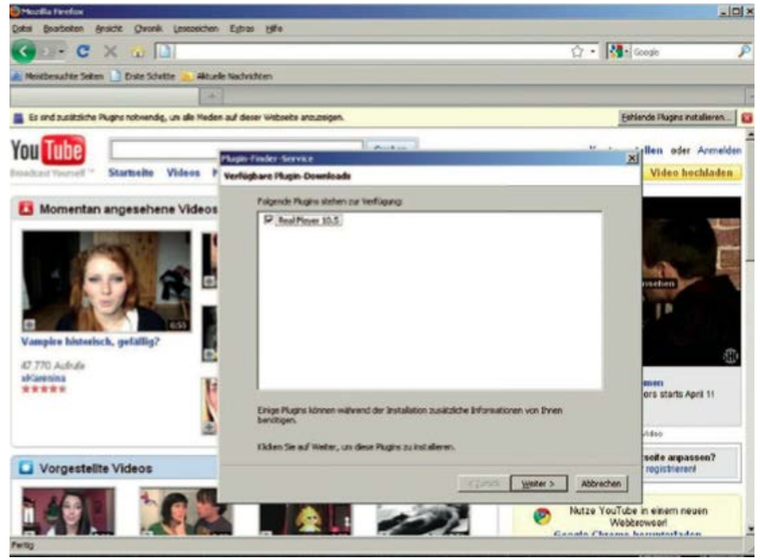


Fig. 3

In addition to assurances of invisibility and restrictions on customers, law enforcement intrusion systems are highly dependent on supplier support, complementing the Intrusion Software with tailored delivery mechanisms, after sales service and continuing updates. This is a product of the complexity of the systems for controlling and delivering Intrusion Software, economic incentives to the vendor that encourage ongoing support contracts, changing needs connected to the evolving environments they operate in, and challenges posed to their activities by antivirus software and security researchers. In June 2010, FinFisher (then Gamma) and Dreamlab Technologies AG negotiated to provide an entity in Oman with the development services and hardware necessary to install the FinFly ISP infection proxy system.[12] This contract included 45 billable days of network analysis, project management, documentation, installation and on-site training services, rendered by Dreamlab. Gamma was to provide two maintenance sessions, one annual coordination meeting onsite, and one year of bug fixes, updates, and new system releases. Publicly-disclosed FinFisher proposals to security agencies in Turkmenistan and EFinFisher offers different versions of this infection system based on required performance characteristics, covering environments ranging from small private networks (*FinFly Net*) to the entire customer base of Internet Service Providers (FinFly ISP). In Turkmenistan, FinFly ISP was installed to provide authorities access to the entirety of international Internet traffic, covering every user in the country. For more targeted intrusion, such as modification of local wireless traffic, both offer specially-equipped laptop units, called *FinIntrusion Kit* (FinFisher) and *Tactical Network Injector* (Hacking Team). All of these examples constitute equipment and systems specially designed for the delivery of Intrusion Software [4. A. 5.].

12 https://www.wikileaks.org/spyfiles/docs/DREAMLAB-2010-OMPurcOrde-en.pdf

Alternatively, for remote targets, *FinFly Web* provides a platform to create fake sites that pose as legitimate software updates or web plugins, but in actuality contain FinSpy. The customer of FinFly Web would then send these links to the target in order to deceive them into installing the Intrusion Software. This product appears to be offered as an application, and would therefore be software specially designed for the delivery of Intrusion Software, thus subject to control [4. D. 4.].



FinFly Web poses YouTube to provide a fake update to a web plugin that infects the target with FinSpy.

When physical access to the target is available, *FinUSB* and *FinFireWire*, vendor-provided USB and Firewire devices, automate infection through the exploitation of vulnerabilities or insecurities in the host's operating system. Both would fall under equipment specially designed for the delivery of Intrusion Software and therefore also subject to control [4. A. 5.].

Further examples of Intrusion Software systems that could fall under the Wassenaar Arrangement language might include those that:

- enumerate potential vulnerabilities in a remote or locally-connected target device in order to insert Intrusion Software into a host; or,
- facilitate the compromise of a locally-connected device through the delivery of an alternative bootloader that exploits operating system or firmware vulnerabilities.

The open source security project Metasploit, the commercial tool Nessus, and software for phone jailbreaking were initially raised out of concern that they might fall under these controls. However, those specific examples would fall under the General Software Note as they are available to the public, often in the public domain as open source software, and are designed for installation without further substantial support by the supplier. Since the Intrusion Software market is highly opaque, these products provide illustrative examples of the form that potentially-controlled systems might take. The objective of the

control should not be to control all 'hacking tools,' instead it should be narrowly-applied to control equipment, software, and technologies that are substantially oriented toward the proliferation of Intrusion Software marketed for surveillance purposes.

Lastly, the operation of FinSpy and RCS requires backend infrastructure for communications and tracking of intrusions. *FinSpy Master* and *RCS Server* act as central data collectors from infected hosts and provide administrative services for the customer. The system for the operation of Intrusion Software may be provided as a hardware solution [4. A. 5.] or a software package [4. D. 4.]. Additionally, both FinFisher gypt reinforce that installation and usage support from the vendor and partners is core to the provision of law enforcement Intrusion Software. In the case of FinFisher, this service is provided under the name *FinLifeline* at a cost of up to hundreds of thousands of dollars. The enforcement benefit of this pre- and post-sales support dependency is that Intrusion Software likely bears less transshipment risk than most controlled items, as vendors will have the means to follow changes in customer needs, network placement, and ongoing communications with update servers.

Export control authorities must bear in mind that control of Intrusion Software remains a point of contention within the computer science field given that the definition bears more than a passing resemblance to normal information security activities. These fears have been exacerbated by debates on surveillance practices, calls from public officials for more regulation of cryptography, and computer fraud enforcement actions unrelated to the new rules. Since this community has little access to legal support for parsing complex export control regulations, lack of clarity has already threatened to impose a chilling effect. Despite the separation of end controls from the Intrusion Software definition, there remain concerns whether exploitation and vulnerability research would fall under the rubric of the new language.[13] This is in part due to the resemblance of the Intrusion Software definition to proof of concepts for vulnerabilities and various types of security tools, as well as lack of clarity over deemed exports (intangible technology transfers) and what constitutes a controlled Technology. Exploitation is not concomitant with Intrusion Software nor is vulnerability research necessarily Intrusion Software development. Information security research, even when it includes the professional sale of vulnerabilities, is a distinct activity from Intrusion Software development, and the field is critically important to ensuring the protection of networks and communication systems. Despite the appropriation of exploits in Intrusion Software products, and clear examples of vulnerability brokers maintaining close affiliations with Intrusion Software vendors, exploitation is at most only a characteristic of some Intrusion Software products, as a mechanism for the circumvention of protective and monitoring measures. Its usefulness in Intrusion Software does not lead it to be automatically controlled. Here the distinction between the definition of Intrusion Software and the actuals controls is important – exploits do not play a role in the operation of Intrusion Software administration systems and it is not the delivery mechanism itself, the intended targets of the control. Therefore, it would not fall within the scope of the Wassenar Arrangement.

Security researchers may demonstrate the existence of a vulnerability through the release of proof-of-concept code. A proof-of-concept may perform exploitation to bypass countermeasures, such as the escape of a sandbox, and then execute externally provided instructions in order to demonstrate the extent of the vulnerability. Security researchers will need to consider the pertinence of any export laws

13 See, 'Why Wassenaar Arrangement's Definitions of "Intrusion Software" and "Controlled Items" Put Security Research and Defense At Risk' by Sergey Bratus, Michael Locasto, and Anna Shubina https://www.usenix.org/publications/login/august14/bratus_wassenaar

to their work, since proof of concepts and vulnerability information may be reported to international vendors, offered for bug bounties or privately sold to vendors – in addition to the longstanding issues of collaborative research with foreign nationals seen in other fields. This situation would run contrary to the intended scope of the definition and pose a challenge to protecting information security, and should not be the outcome of the controls.

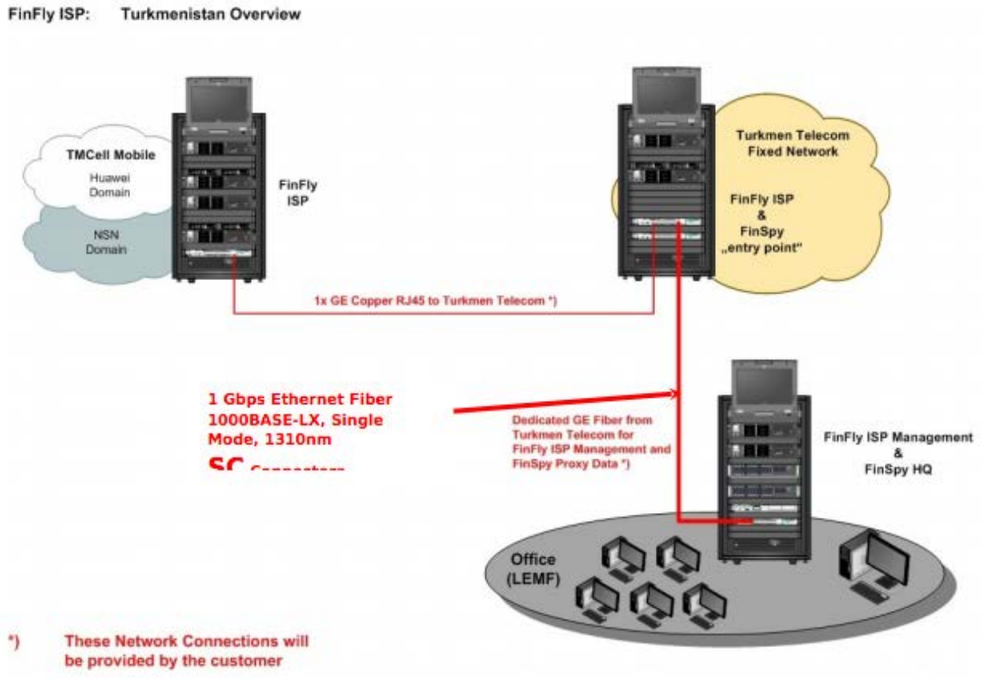
An interpretation of Intrusion Software that includes standalone exploits or proof of concepts would stifle computer security research, particularly given the wide net that could be cast by the Technology control or deemed export rules. These concerns are heightened by past experiences with controls on encryption, including instances where cryptography controls were used to regulate products now considered Intrusion Software.[14] Reasonable individuals with similar intentions to combat unlawful violations of privacy continue to differ on the best approach for regulating exploit markets. The Wassenaar Arrangement language was not presented publicly as an attempt to address this issue, and may not be properly equipped to handle the nuances associated with the matter. It is incumbent that export control authorities refrain from considering broad interpretations of Intrusion Software that might lead to attempts to regulate exploits or vulnerability sales.

It is worth noting that while the majority of the Wassenaar Arrangement's controls for Technology cover the development, production, or use of controlled systems, the Intrusion Software's Technology controls only cover development [4. E. 1. c.]. The Wassenaar Arrangement clarifies under its definitions that "development" is:

> *related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.*

Therefore, it appears that user training and post-sales support services like FinLifeline would not be covered under the control. The design of Intrusion Software does not constitute a highly sophisticated or exclusive field of knowledge, and thus it would not benefit the objective of the control to regulate research for purposes other than deployment of a commercial product. Instead, the primary focus for export control authorities in the application of the Technology classification should be control of the consultative services that are rendered prior to or in support of the deployment of Intrusion Software. The preinstallation consultations provided by Dreamlab for the Omani and Turkmen governments demonstrates the role of needs assessments and integration design in the process of providing Intrusion Software infrastructure, requiring advanced mapping of the network topology of the customer and points of integration prior to installation. This would have the added benefit of catching cases where non-controversial software may be modified for the purpose of delivering Intrusion Software, and mitigate some of the concerns of the computer security community.

14 FinFisher was reportedly controlled by the UK on the basis of the use of encryption in 2012. http://www.exportlawblog.com/archives/4347



Preinstallation consultation of the potential placement of FinFly ISP appliances in Turkmenistan.

If government agencies are concerned about the widespread availability of commercial spyware or hacking tools, the case of StealthGenie demonstrates that the U.S. and other governments maintain other means of pursuing vendors responsible for their distribution, on the grounds of possession or distribution of interception devices.[15] Software vendors or foreign parties may reappropriate common defensive security or network management tools in order to deliver Intrusion Software or execute provided instructions. Products that fall within this theme, such as Metasploit and Nessus, are heavily used by security professionals to perform intrusion for audits. While most would qualify as generally available under the General Software Note, access to these tools may be restricted to security professionals in order to minimize their misuse. Thus far, it is easy to differentiate the Intrusion Software products of FinFisher and HackingTeam from security auditing tools, as none of latter companies' products have any conceivable, legitimate use in strengthening information security. Defensive tools may also require less direct support from vendors, outside of updates. Therefore, export control authorities may differentiate information security products from intrusion support based on whether an item is integrated into Intrusion Software agent, whether such integration constitutes their primary usefulness, and whether the product would have legitimate uses in promoting network security. Whether or not particular security audit software are appropriated by malicious actors, it remains in the interest of export control authorities to promote the availability of information security tools and not chill their development.

15 http://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine

The exemptions offered to debuggers, software reverse engineering tools, digital rights management systems, or asset recovery software are narrowly-defined and do not appear to present significant risk of relabelling by companies that may want to apply avoid controls through misappropriating exemptions. For example, asset tracking, which most closely resembles the tracking functionalities of surveillance software, implies ownership or legitimate access to the device. It should not require the opaque behavior that necessitates circumvention of security countermeasures or evasion of antivirus applications. The effectiveness of Intrusion Software is directly interrelated to its invisibility to the targeted user to the extent that both FinFisher and HackingTeam appeared to produce regular reports on what was detected by specific antivirus products.[16] This obsession with invisibility is counter to the spirit of the exemptions provided. There is little overlap between the vendors of Intrusion Software and the exempted activities, and thus far, there is little ambiguity in the intent of products that we have identified. Moreover, the specially designed or modified restrictions of the control are not onerous to the objective. For example, while FinFly ISP appears to use mobile network identification probes in order to perform selection of targets, the probes themselves would continue to be considered general network equipment, and we would not expect them or related technologies to qualify as specially designed Intrusion Software equipment. We do not expect there to be a great deal of grey area, or that those products would be the most in need of control.

We believe that the most ambiguity for vendors and export control authorities under the new rules may arise on whether an item constitutes a specially designed product for the delivery of Intrusion Software. As we have noted, the line between cybersecurity products is blurred when Intrusion Software vendors use the same means, even the same source code (e.g. FinFisher's FinTrack is based on the open source security auditing tool BackTrack), to stage the delivery of remote access systems. Such companies may also have a broader portfolio of product offerings that includes security trainings and audits. Intrusion Software has thus far been highly controlled by vendors for the sake of charging users on a per-seat basis and avoiding scrutiny from protective products. In order to provide for sophisticated and reliable operations, the systems for the generation and operation of Intrusion Software are likely to be similarly confidential, proprietary, and tightly integrated into the functionality of the remote agent. These relationships and technical qualities provide for guidance on the primary purpose of the product, and narrow the likelihood that such equipment could incur ambiguities about legitimate dual use. For example, there is little functional difference between some network advertising technologies, such as those exempted under the IP network surveillance rules, and network injection appliances like FinFly. However, FinFly is tightly integrated into the delivery of the FinSpy software and administrative platform provided by FinFisher, and the equipment could provide nearly no functionality on a network other than the delivery of Intrusion Software. Furthermore, while the use of exploitation should not be sufficient to determine whether an item should be controlled, it may serve as a significant indicator of the primary use of the equipment.

Therefore, we encourage export control authorities to consider items not only based on their technical specification, but also their advertisement and end use. Such factors might include whether:

16 **FinFisher:** (Excel Document) https://wikileaks.org/spyfiles4/documents/Anti-Virus-Results-FinSpy-PC-4.51.xlsm
HackingTeam: (PDF) https://s3.amazonaws.com/s3.documentcloud.org/documents/1347999/invisibility-report-9-0-final.pdf

the system is specially suited for integration with particular Intrusion Software packages or control systems;

the exporter maintains partnerships with Intrusion Software vendors;

pertinent patents or sales material make reference to lawful interception or surveillance use cases;

the technical characteristics and deployment in the case of exemption claims matches legitimate objectives, such as if the stated purpose of the technology should normally require user consent, if they could be performed effectively with the awareness of the user, and if the equipment could have significant use outside of the delivery of Intrusion Software;

the system is sold as a package with Intrusion Software and whether any Intrusion Software product is reliant on the system or operation in question for operation;

the product is primarily marketed to, or only sold to, law enforcement or intelligence agencies;
the end recipient is a law enforcement or intelligence agency, or an entity with known relationships to such sectors, and the possible use cases for such customers;

the platform maintains the ability to employ exploitation or mimic legitimate resources in order to perform non-consensual operations against the user;

the primary placement or capabilities of the device would enable its end recipient the ability to tamper with public access networks.

More detailed suggestions on a "Know Your Customer" regime appropriate for censorship and surveillance technologies has also been articulated by the Electronic Frontier Foundation.[17] The United Nations Guiding Principles on Business and Human Rights offer recommendations regarding corporate responsibility to respect human rights, and the European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights provides a supporting institutional framework.[18]

17 https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment

18 "UN Guiding Principles on Business and Human Rights" http://www.businesshumanrights.org/Documents/UNGuidingPrinciples European Commission "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" http://www.shiftproject.org/publication/european-commission-ict-sector-guide

II. IP NETWORK SURVEILLANCE

A. CONTROL LANGUAGE

WHAT IS CONTROLLED?

Does the network surveillance equipment, or specially designed[1] component to such a system, provide all of the following functionalities:

1. Process large volumes of Internet traffic (compared to, for example, a home or business network) *[§1]*,
   - capable of application-layer content inspection, otherwise known as deep packet inspection *[§1.a]*, and
   - extract and index metadata and application content (such as emails or telephony information) from this traffic *[§1.b, §1.c]*;
2. Search indexed information based on data related to an individual (such as names or email addresses) *[§2.a and Technical Note 'Hard selectors']*; and,
3. Map the relationships between individuals based on collected data. *[§2.b]*.

In addition to the primary equipment control outlined in [5. A. 1. j.], the Wassenaar Arrangement includes controls on:

- software specially designed or modified for the "development", "production" or "use" of equipment that would fall under the control *[5. D. 1.]*; or,
- 'technology,' [2]namely technical data or technical assistance, specific information necessary for "development", "production" or "use" of equipment or software that would fall under the control *[5. E. 1.]*.

WHAT IS EXEMPTED FROM CONTROLS?

- Devices whose primary purpose is to perform marketing. *[Note to 5.A.1.j.].*
- Devices whose primary purpose is to perform Quality of Service (QoS) or Quality of Experience (QoE) functions on the network *[Note to 5.A.1.j.]*.

WASSENAAR LANGUAGE (CATEGORY 5, PART 1, TELECOMMUNICATIONS)

[From Wassenaar Arrangement Control List]

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

1 'Specially designed' in the Wassenaar Agreement defined term that cover items that as a result of their development have properties peculiarly responsible for achieving or exceeding the description within the control. Essentially, this raises the threshold for control, and therefore technologies that might have incidental use for a controlled purpose are less likely to be covered. **See Appendix for more.**

2 Technology in the Wassenaar Arrangement is a defined term that covers a broad range of technical data and development assistance. **See Appendix for more.**

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.

Note 5.A.1.j. does not apply to systems or equipment, specially designed for any of the following:

1. Marketing purpose;
2. Network Quality of Service (QoS);or
3. Quality of Experience (QoE).

TECHNICAL NOTE

- **'Hard selectors':** data or set of data, related to an individual (e.g., family name, given name, e-mail, street address, phone number or group affiliations).
- **5. D. 1. "Software" as follows:**
    - "Software" specially designed or modified for the "development", "production" or "use" of equipment, functions or features, specified by 5.A.1.;
- **5. E. 1. "Technology" as follows:**

"Technology" according to the General Technology Note for the "development", "production" or "use" (excluding operation) of equipment, functions or features specified by 5.A.1. or "software" specified by 5.D.1.a.;

B. PRODUCT CONSIDERATIONS

PRODUCTS COVERED BY CONTROL

IP network communications surveillance systems or equipment [5. A. 1. j.]

- Amesys EAGLE[3]
- SS8 Communications Insight[4]
- ETI Group[5]
- Narus nSYSTEM[6]
- Vastech ZEBRA[7]

PRODUCTS NOT COVERED BY CONTROL

- **Quality of Service:** QOSMOS IxMachine[8]
- **No Relationship Mapping:** Blue Coat, Sandvine or UTIMACO[9]
- **Marketing Exemption:** Phorm, NebuAd or Frontporch[10]

3 https://www.wikileaks.org/spyfiles/files/0/95_AMESYS-CRITICAL_SYSTEM_ARCHITECT.pdf
4 http://go.ss8.com/notebooklet
5 https://www.wikileaks.org/spyfiles/docs/ETIGROUP-2011-Evid-en.pdf
6 http://narus.com/images/pdf/Narus_nSYSTEM_brochure.pdf
7 https://www.wikileaks.org/spyfiles/files/0/285_VASTECH-ZEBRA2.pdf
http://www.documentcloud.org/documents/711299-brochure484.html#document/p5
8 Overview: https://www.wikileaks.org/spyfiles/docs/QOSMOS-2011-CasestudNetw-en.pdf
QOSMOS ixEngine: https://www.wikileaks.org/spyfiles/docs/QOSMOS-2011-iXEngiDPI-en.pdf
Qosmos ixMachine LI Edition: https://www.wikileaks.org/spyfiles/docs/QOSMOS-2011-ixMaLIEdit-en.pdf
9 https://www.wikileaks.org/spyfiles/docs/UTIMACO-2010-UtimLIMSLawf-en.pdf
https://www.wikileaks.org/spyfiles/docs/FROSTSULLIVAN-LawfInteA-en.pdf
10 http://web.archive.org/web/20080713030851/http://www.juniperamspmarketing.com/NebuAD.htm
http://www.frontporch.com/brochure/FP-Brochure-072512.pdf

C. DISCUSSION

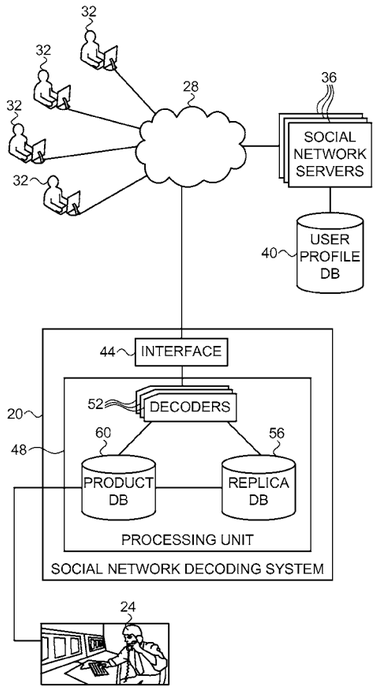
The Wassenaar Arrangement language on IP Network Surveillance is extremely narrow, and does not serve as a catch-all for the broad spectrum of network technologies that could be employed for repressive purposes. Contrary to some expectations, there is no indication that the Wassenaar Arrangement language would directly apply to the deep packet inspection (DPI) equipment (such as those manufactured by Blue Coat Systems or Qosmos) or interception systems that have routinely evoked controversy when found to have been exported to countries that restrict freedom of expression. The most constraining factor of the definition appears to be subsection 2, particularly part B, which requires the characteristic of being specially designed to carry out mapping of the relationship network of an individual or of a group of people.[11] In practice, this characteristic of mapping differentiates platforms designed for "lawful interception" of communications from those marketed as mass surveillance of Internet traffic for intelligence purposes. The new control seeks only to regulate only the latter equipment, and in doing so focuses on a high specialized function that does not appear to be commonplace or likely incur dual use scenarios. As export control authorities begin to make determinations on license applications and educate telecommunications equipment manufacturers, the primary areas of controversy may be grey lines between surveillance and cyber security functionalities, such as those advertised by high-profile vendors Narus and Glimmerglass.

While a wide array of technologies purport to conduct high performance analysis of Internet traffic, and a large subset of those include the ability to monitor for personally-identifying information, the correlation of traffic data for mapping of relationships is a sophisticated function that denotes a specialized product. Publicly-available information on the analytical capabilities of any specific device is scarce, and more often originates from journalistic accounts of their implementation in the surveillance regimes of repressive states. A review of technical specifications and marketing material of equipment believed to be subject to the new controls reinforces that the new rules apply to a narrow selection of systems and technologies; namely, those that are specifically marketed for intelligence activities, rather than the broad suite of network surveillance equipment.

One relevant patent, granted to Verint for "passive decoding of social network activity using replica database" describes the collection of information on social relationships from surveillance of traffic to sites such as Facebook and Twitter:

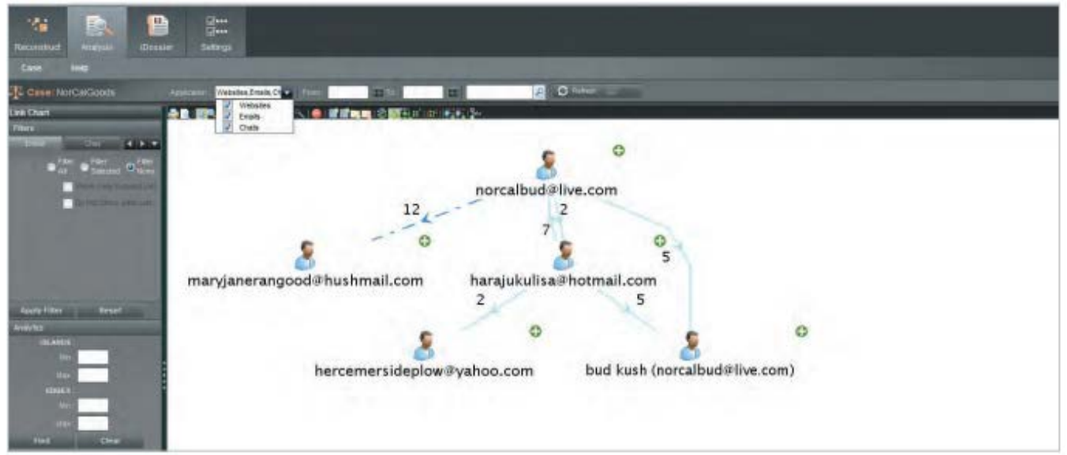
> *Methods and systems for obtaining reconstructing activities of target users in social networks, such as for decoding and displaying social network sessions held by a target user, or identifying other users who are associated with the target user. This analysis is typically carried out based on passive monitoring of network traffic. A social network decoding system constructs and maintains a replica database, which mimics a portion of the user profile database maintained by the social network servers. The social network decoding system monitors network traffic between users and social network servers. Based on the monitored traffic, the system gradually constructs a replica database that attempts to replicate a portion of the social network user profile database, relating to one or more predefined target users. Using the replica database, the system is able to correlate loosely-coupled information objects, events and interactions between the target users and social network pages.*[12]

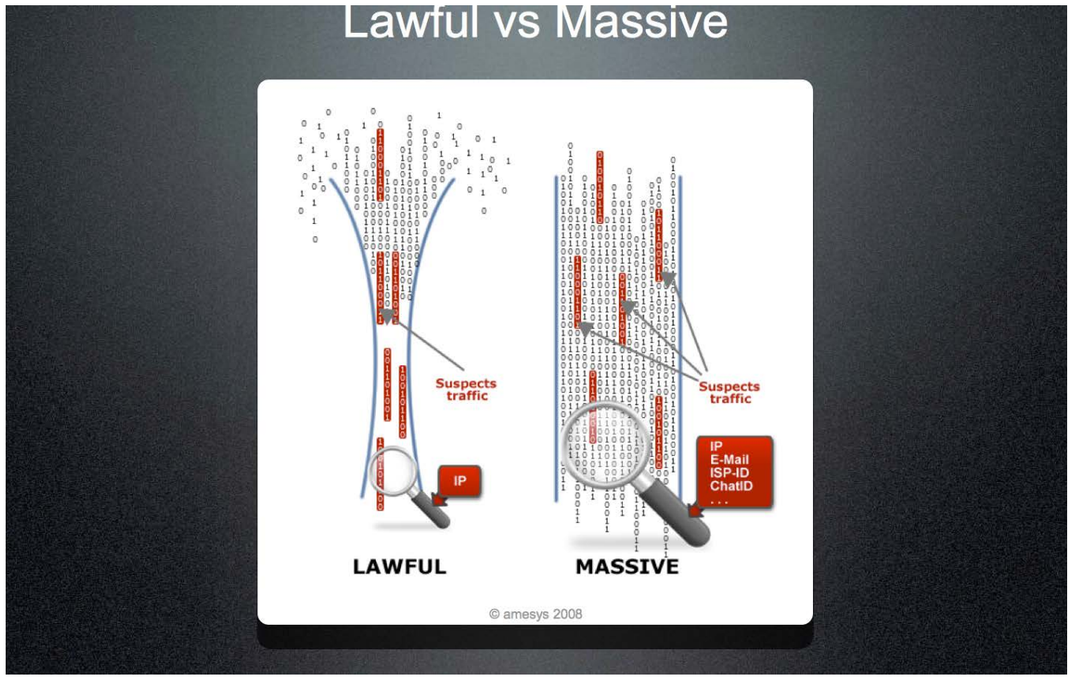
11 Examples of such analysis can be found in industry literature, such as: http://www.ss8.com/sites/default/files/SS8_SNA_Features_Sheet.pdf
12 http://www.google.com/patents/US20140095700



We identified the following systems and components as warranting heightened scrutiny under the IP Network Surveillance controls: ***ETI Group's EVIDENT Investigator,[13] SS8 Communications Insight (Intellego),[14] Area SpA MCR Studio,[15] Amesys's EAGLE GLINT (now Nexa Technologies SAS),[16] AMECS's Analys,[17] Narus nSystem,[18] Vastech ZEBRA,[19] Group 2000's Lawful Monitoring Centre,[20] Glimmerglass CyberSweep Sapience,[21] ATIS Klarios Monitoring Centre,[22] Siemens Intelligence Platform,[23] Verint Systems, AQSACOM Aqumen, Nice Systems.[24]***

13 Page 28, https://www.wikileaks.org/spyfiles/docs/ETIGROUP-2011-Evid-en.pdf
14 http://www.ss8.com/sites/default/files/SS8_Intellego_Brochure.pdf
15 http://s3.documentcloud.org/documents/810665/76-area-brochure-mcr-studio.pdf
16 https://www.wikileaks.org/spyfiles/files/0/99_AMESYS-EAGLE-GLINT-Operator_Manual.pdf
17 https://www.wikileaks.org/spyfiles/docs/AMECS-2011-A30Excein-en.pdf
18 http://narus.com/images/pdf/Narus_nSYSTEM_brochure.pdf
19 http://www.documentcloud.org/documents/711299-brochure484.html#document/p5
20 www.group2000.com/solutions/intelligence_services/monitoring_centre/
21 https://www.wikileaks.org/spyfiles/files/0/55_201110-ISS-IAD-T1-GLIMMERGLASS.pdf
http://www.glimmerglass.com/news-events/press-releases/glimmerglass-demonstrates-latest-release-of-cybersweep-sapience-at-iss-world-asia-2014/
22 http://www.atis-systems.com/klarios-2-0-mc.html?&L=1
23 https://wikileaks.org/spyfiles/files/0/15_200702-ISS-DXB-SIEMENS.pdf
24 https://www.documentcloud.org/documents/815869-996-nice-systems-brochure-nicetrack-horizon.html





All of these devices in their marketing material share a stated purpose of surveillance of telecommunications networks for intelligence operations and monitoring centers, frequently using language such as "acquiring actionable information" and "target development." These technologies can take the form of components to enhance an existing lawful interception infrastructure, or constitute complete platforms to handle the full process from the collection of traffic to the production of actionable intelligence information. As one American company, SS8, describes their product,

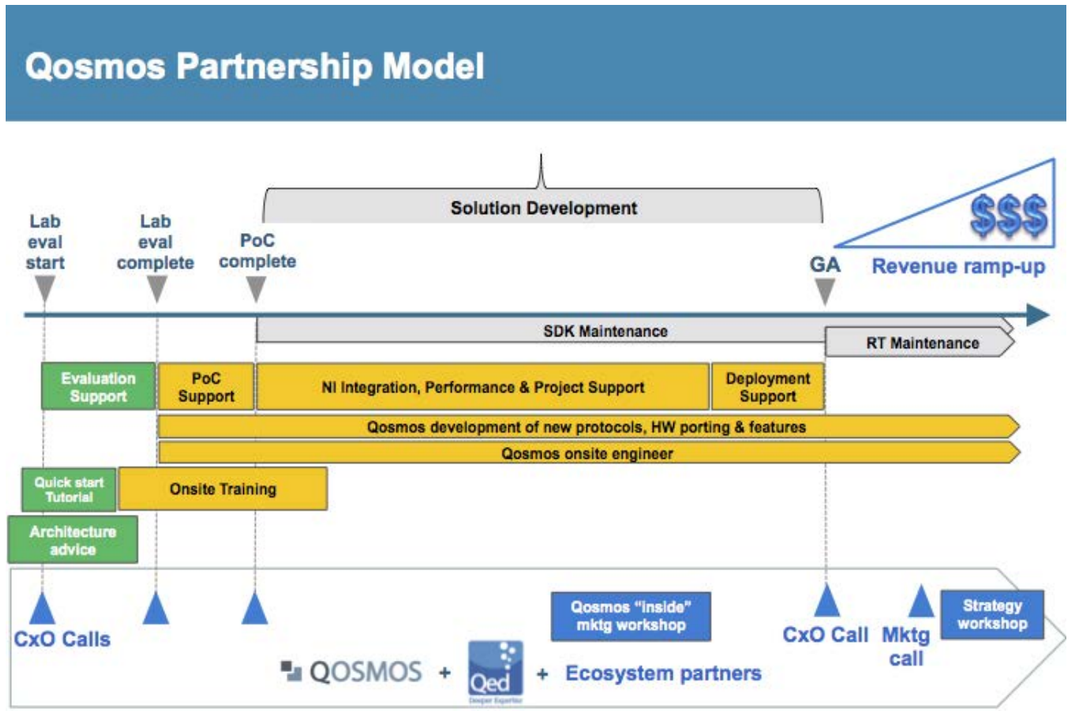
We've created a true "end-to-end" solution that not only includes the sensor technology required in the network, but also the next generation of criminal investigation and national security intelligence analysis tools. We integrate Social Network Analysis (SNA) across our applications to effectively and efficiently monitor and capture relevant intelligence on threats to your society, community, or network.[25]

Alternatively, and perhaps more commonly, the items now controlled can appear as specific components for placement in an interception system built or maintained by different vendors. The language of the control does not suggest that the controlled systems need to be the primary collector of traffic from the network or handle target signaling from the monitoring center themselves. This is important since such systems have different devices for the collection of communications from network logging devices. As ATIS notes in one sales presentation to a Tunisian client,[26] implementation of interception and monitoring regimes requires "adaptation of individual customer requests" and "intensive customer support (pre-sales consultancy and technical services)." All of these services exceed the bounds of the Wassenaar Arrangement's General Notes on software and technology, and represent technical design data to be controlled [5. E. 1.].

Network monitoring regimes are built on a suite of technologies, most of which are not specially designed for lawful interception or intelligence-related surveillance. Qosmos, whose sophisticated traffic analysis equipment was a component of the surveillance system offered to Syrian authorities, provides an illustrative example. Under normal conditions, the Qosmos ixMachine is advertised as an off-path network device that offers "application-based billing, cyber security, traffic optimization, policy management, and many more."[27] However, Qosmos announced an "LI Edition" version of the ixMachine in November 2009 at the security trade show Milipol.[28] The LI Edition purports to allow law enforcement to use "Qosmos Network Intelligence technology to more easily detect, mitigate and prevent illicit and criminal activity." By most accounts, the LI Edition appears to only be a specifically tailored ixMachine, and Qosmos had advertised the use of ixMachine in lawful interception regimes long before the introduction of a specialized product.[29] Qosmos has also maintained a highly-promoted relationship with the Sophos-subsidiary company Utimaco, in order to provide standard interfaces between the ixMachine's logging functions and Utimaco's "Lawful Interception & Monitoring Solutions" (LIMS).[30]

While Qosmos and Utimaco's products appear to be useful to Internet surveillance, ixMachine, LIMS, and Utimaco's Data Retention Suite (DRS) do not appear to fully match the specifications of the IP Network surveillance control. These products may inspect or record the application-layer content of Internet traffic in order to catalogue the communications of the target, but it is not clear that they provide for search and mapping of relationships based on personally-identifying information within that content. Moreover, Utimaco's product literature promotes the ability to export data to third party products, such as IBM i2 Analyst's Notebook, as a solution relationship mapping – not a native function or vendor-provided solution.[31] Based on documentation and accounts from elsewhere, holistic monitoring capacity envisioned by the control often appears to be offered as a custom solution designed per customer, with products like ixMachine and LIMS as backend infrastructure.

25 http://www.ss8.com/sites/default/files/nonprotected/0553-04FA3%20SS8_Corporate%20Overview_WEB_0.pdf
26 https://www.wikileaks.org/spyfiles/docs/ATISUHER-ATISPres-en.pdf
27 https://www.wikileaks.org/spyfiles/docs/QOSMOS-2011-ixMa-en.pdf
28 http://www.businesswire.com/news/home/20091109006202/en/Qosmos-Enables-Network-Intelligence-Lawful-Interception-Applications#.VKco94rUvfZ
29 http://www.prweb.com/releases/qosmos/network/prweb1009744.htm
30 https://www.wikileaks.org/spyfiles/docs/QOSMOS-2011-CasestudNetw-en.pdf
31 Page 8, https://lims.utimaco.com/fileadmin/assets/brochures_datasheets_whitepapers/UTIMACO_DRS_BROCHURE_EN.pdf

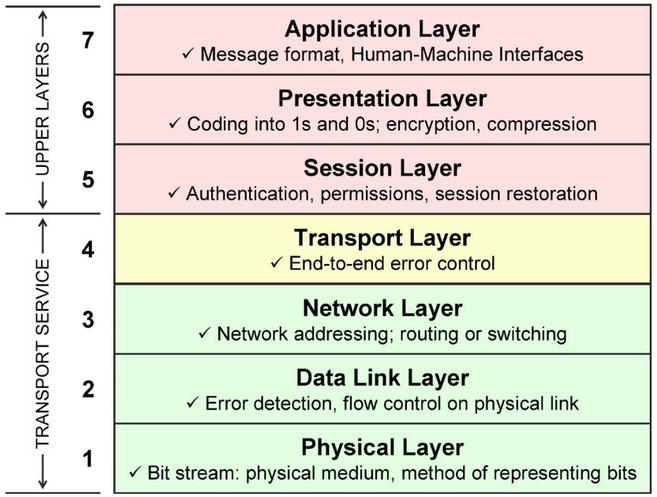


Several ixMachines were procured by Utimaco as a part of the data retention platform that was to be provided to Syria by the Italian company Area SpA. Area's platform allowed Syrian authorities the ability to monitor not only IP traffic, but mobile subscriber data as well. Area's contribution to Qosmos and Utimaco's platform was the analysis components to the monitoring center, including the MCR System. While ixMachine devices provide high performance traffic analysis, they were merely collection agents with LIMS as the backend datastore. MCR Studio, a component of the MCR System, advertises itself as a turnkey service for "finding out both direct and indirect relationships among subjects, identifying behavioral models."[32] The Wassenaar Arrangement language does not appear to require the equipment to do interception itself, only analysis and extraction. Therefore, the most likely product to be controlled within installations similar to Syria's would be MCR Studio, as a specially designed component that matches the criteria for analysis, extraction, indexing, and mapping.

The focus on Layer 7 of the OSI model[33] in the IP Network Surveillance specification reinforces that the control is only interested in surveillance that is conducted through analysis of the content of Internet communications. This does not include monitoring of statistical information on the use of particular applications, blocking of sites, or tracking what IP addresses a user exchanges traffic with. It is noteworthy that, while the discussion of the Wassenaar Arrangement language has thus far focused on traditional Internet communications such as web and email, the control also provides for further enforcement

32 http://www.documentcloud.org/documents/815928-80-area-product-list-mcr-tracer-mcr-captor-mcr.html
33 More on the OSI model can be found at: http://www.webopedia.com/quick_ref/OSI_Layers.asp

opportunities on the more traditional communications that are increasing being provided as "over-the-top" services. The control should cover interception of telephony conducted using voice over Internet Protocols (VoIP), which is the communications transport for next generation networks and constitute normal application content on an IP network. This overlap is incidentally reinforced by the fact that the predominant discussion on the performance requirements of the "carrier-class IP networks" term used in the specification has thus far focused on the replacement of traditional telephony infrastructure with VoIP.[34]



The IP Network Surveillance control maintains exemptions for systems and equipment that are specially designed for marketing, Network Quality of Service (QoS), and Quality of Experience (QoE) purposes. While the exemptions have been met with some skepticism, we find less ambiguity or suggestion of dual use in a review of the marketing material for potentially exempted devices. The largest source of concern has arisen from the premise that DPI equipment, such as ixMachine, perform traffic classification for the purpose of assessing the performance of end-user connectivity based on the same mechanisms as its lawful interception functions. This dual use risk applies equally to other technologies that have been linked with censorship and surveillance regimes in repressive states, such as Blue Coat's proxy equipment.[35] Legitimate quality of service and quality of experience functionalities, however, should have more narrow needs for traffic inspection and data retention, rarely maintaining awareness of network connections past decisions on how to classify the traffic or collect statistical information. If deep packet inspection devices lack relationship mapping capabilities, and thus already fall outside of the IP Network Surveillance rules, this concern about rebranding and dual use appears less pressing.

The marketing exemption appears primarily to apply to products offered by companies such as Phorm, NebuAd, and Frontporch, which perform deep packet inspection for tracking in highly-targeted advertisements. While these devices pose their own dangers to privacy, they are less likely to act as passive devices, or produce the social relationship map of a specific user that is accessible to the

34 http://www.itweb.co.za/index.php?option=com_content&view=article&id=18366
35 http://www.itweb.co.za/index.php?option=com_content&view=article&id=18366

network administrator. These devices bear a different marketed purpose with a different consumer base and a divergent economic model from surveillance products. Given their proprietary nature, despite the similarity in objectives they are unlikely to be easily modified to perform comprehensive network surveillance. They are also unlikely to provide the capacity to connect with warrant mediation systems. It is difficult to imagine that vendors such as Narus or Vastech could convincingly brand their surveillance devices as marketing technologies since their passive interception and wholesale retention of traffic data is unnecessary for legitimate marketing purposes.

In order to avoid the possible misuse of such an exemption, it is important that export control authorities maintain an expectation about how Frontporch-like devices should operate in order to achieve a strictly marketing objective (similar considerations could be held for network management exemptions as well).[36] Such expectations might include design considerations such as:

active presence on the network, inserting cookies, HTTP headers or HTML code for the purpose of user tracking or display of advertisements, as opposed to passive interception;

limited inspection of traffic, in terms of types of applications, length of data retention and extensiveness of data collected,

focus on themes of content rather than the collection of personal identifiers and evaluation of linkages between hard selectors; and,

isolation from lawful interception and network account management operations, including restricted access to subscriber information held by the network operator, constraints on direct access to the data retained on specific users, and lack of warrant mediation functionality.

Finally, IP network surveillance technologies maintain a hallmark property of being specifically marketed to governments and telecommunications companies, with substantial restrictions on even information regarding their operation or capabilities. Based on public accounts of Area SpA's activities in Syria[37] and Amesys in Libya, these systems are highly customized to fit the design requirements and infrastructure environment of their government customers. It is therefore highly unlikely that development of such systems would qualify under either General Note as being generally available or scientific research. These dependencies also provide indication of the intent and location of the system's deployment for export licensing and compliance purposes.

This distinction between exempted activities and network surveillance equipment is reaffirmed by differences in patterns in branding and specifications. The technologies identified as necessitating heightened scrutiny advertise themselves strongly in terms of national security, intelligence production, and interception compliance, and include design elements such as warrant mediation and data retention that bear little resemblance to legitimate network management or advertising needs. Therefore, similar to Intrusion Software, export control authorities should consider not only technical specifications, but also their marketing and end use. Such factors might include whether:

36 http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf
37 www.bis.doc.gov/index.php/about-bis/newsroom/press-releases/107-about-bis/newsroom/press-releases/press-release-2014/643-italian-company-agrees-to-100-000-penalty-for-unlawful-technology-export-to-syria

- the system is specially suited for integration with particular interception, monitoring, or surveillance systems;
- the exporter maintains partnerships with vendors of products for lawful interception and mass surveillance;
- pertinent patents or sales material make reference to surveillance use cases;
- the primary placement or capabilities of the device would enable its end recipient the ability to perform analysis of the traffic of public access networks, rather than home or small business premises;
- the product is marketed to, or only sold to, law enforcement or intelligence agencies;
- the end recipient is a law enforcement or intelligence agency, or an entity with known relationships to such sectors, and the possible use cases for such customers;
- the equipment maintains components for integration within warrant mediation systems or lawful interception data retention platforms;
- the stated activities of the system could be performed with the awareness of the user and still be effective.

A few concerns remain. Export control authorities should provide greater clarity on the meaning of "carrier class IP network," which parenthetically offers the example of "national grade IP backbone" but is otherwise an ambiguous term. The suggestion of a national grade backbone might be informed by the experiences of Iran, Libya, or Syria, where interception occurs at scarce international transit points, which is often a result of a state-owned or affiliated monopolies on core infrastructure. However, demands for increasing bandwidth challenge this network design, and states have sought to move surveillance and censorship away from international points of transit and nearer to the access ISP for performance reasons. The deployment models offered by Qosmos and others encourage the positioning of traffic interception closer to the user. Additionally, the Blue Coat installation in Syria demonstrates that countries may appropriate devices that are meant for smaller networks and pool equipment to scale up to cover larger networks. Therefore, export control authorities should take care to define carrier class IP networks in terms of capacity, type of connectivity, and operational nature that are within the range of consumer access ISPs, rather than solely long-haul transit networks. For the time being, differentiating consumer access networks from small business connectivity or other limited, private networks that do not bear the same level of human rights risk, appears to be feasible. The equipment previously identified markets substantially to governments and telecommunications vendors, based on national security interests and compliance requirements, which are less common in a corporate environment.

Lastly, while these network surveillance products tend to self-identify as national security or lawful interception equipment, a point of uncertainty remains on the specially designed language in the face of certain systems that include cybersecurity in their portfolio. Companies such as Narus and Glimmerglass have marketed similar technology to private enterprises for detection of attacks on networks, identification of insider threats, and other forensics. This security-oriented traffic analysis equipment engages in similar functions as IP network surveillance equipment: the interception of application-layer traffic correlated across connections in order to discern information on the user's behavior. These types of security appliances remain IP Network Surveillance systems specially designed to conduct indexing and mapping of relational data, regardless of the potential use in or monitoring of non-public environments. Export control authorities should take particular note as to whether the design of equipment renders it useful for covered surveillance, even if it may also have rare dual use deployments, and exercise intensive scrutiny given the already narrow scope of the control's specification.

III. CONCLUSION AND RECOMMENDATIONS

Clearly defined and well enforced Intrusion Software and IP Network Surveillance controls can lay the groundwork for a constructive and expansive role for export controls in the promotion of human rights and cyber security goals. As export control authorities consider license applications and industry education, it is incumbent to ensure that these new regulations are narrowly applied to control equipment, software, and technologies that are substantially designed for surveillance. The objective should not be to control all hacking tools or other illicit activities online, and regulators should not take expansive interpretations that would chill legitimate research. Whether or not particular tools are appropriated by malicious actors, it remains in the interest of export control authorities to promote the availability of information security tools and not chill their research or development. The Control List can and should be later revisited to address systems not covered presently.

Additionally, in the process of determining the applicability of the control language, handling licensing determinations and pursuing enforcement actions, export control authorities should:

- Refrain from considering broad interpretations of Intrusion Software that might lead to attempts to regulate exploits or the vulnerability market;
- Apply the technology classification of Intrusion Software narrowly to control the consultative services rendered prior to or in support of the deployment of Intrusion Software;
- Issue specific guidance outlining the forms of scientific research and technical data that are covered by the Intrusion Software control;
- Consider pre-consultations and post-sales support requirements within Intrusion Software and IP Network Surveillance license applications;
- Promote standard red flags that employ the technical characteristics of network products to mitigate transshipment risks, such as changes in customer needs, network placement, and ongoing communications with update servers;
- Maintain technical expectations about how network advertising and quality of services devices should operate in order to achieve a legitimate and narrowly-defined objectives, such as active presence on the network and limited inspection of traffic;
- Differentiate information security products from intrusion support systems based on their integration into particular Intrusion Software agents, and whether such integration constitutes their primary usefulness;
- Consider Intrusion Software and IP Network Surveillance items not only based on their technical specification, but also their advertising material, system integration, partnerships, customer base, network placement, passive operations and end use; and,
- Consult with industry and civil society to promote implementation of "know your customer" policies that will reduce the potential for approved, or otherwise permissible, exports to misappropriated for the abuse of human rights.

Whether or not the Wassenaar Arrangement's language on Intrusion Software and IP Network Surveillance controls the limited range of privacy-invasive technologies identified here, the United States and other countries still maintain unilateral controls related to communications intercepting devices or surreptitious listening devices. These are defined as equipment that "can be used for interception of wire, oral, or electronic communications if their design renders them primarily useful for surreptitious listening even though they may also have innocent uses," language that is an exact copy of federal laws on the possession or production of wire and electronic communications interception equipment.[1] Export enforcement on surreptitious listening devices has fallen behind domestic prosecutions. In late 2014, the FBI began to pursue the developers and users of spyware products (commercially-available Intrusion Software) such as Mobistealth, StealthGenie, and mSpy under charges of possession of illegal interception devices, the latest in a history of prosecutions for such software under wiretapping laws. Despite these similarities, Intrusion Software does not appear to have been controlled by the Department of Commerce's Bureau of Industry and Security until the new rules. Governmental agencies could review the disparities in enforcement between wiretapping statutes and export controls to achieve greater parity on privacy violating technologies.

Finally, the Area contract with the Syrian Telecommunications Establishment reinforces the fundamental argument offered by human rights organizations: rarely does any particular component or vendor provide the totality of a system for invasive surveillance to facilitate the violation of fundamental human rights. Whether or not partners seek to end contracts after public disclosure of wrong-doing, once shipped, such equipment remains accessible to actors for illicit uses forever. Moreover, environments change and can change quickly. FinFisher, Area, and Amesys all entered into contracts at times when relationships between Egypt, Syria, and Libya were positive and improving. Absent stronger regulation of components than appears possible or desirable, it is not clear that the Wassenaar Agreement language would cover the Area installation if the relationship analysis functionalities provided by MCR Studio were omitted. Successful fulfillment of the objectives of the both controls will be heavily reliant on export control authorities paying particular attention to marketing, support, risks and end-use of the systems under consideration, and then reviewing progress for future Wassenaar Arrangement Plenary Sessions.

1 http://www.law.cornell.edu/uscode/text/18/2512

APPENDIX

CONTROL LISTS

Wassenaar Arrangement 2014
http://www.wassenaar.org/controllists/2014/WA-LIST%20%2814%29%201/WA-LIST%20%2814%29%201.pdf

UK Strategic Export Control Lists
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/392470/strategic-export-control-consolidated20141231.pdf

WHAT DOES "SPECIALLY DESIGNED" MEAN?

An "item" is "specially designed" if:

1. as a result of "development" it has properties peculiarly responsible for achieving or exceeding the performance levels, characteristics, or functions in the relevant ECCN or U.S. Munitions List (USML) paragraph; or
2. it is a "part," "component," "accessory," "attachment," or "software" for use in or with a commodity or defense article 'enumerated' or otherwise described on the CCL or the USML.

http://www.bis.doc.gov/decisiontools/specialdesigntool/Specially%20designed%20decision%20tool%20for%20sending%20to%20BIS%20programmers.4.15.13_files/docs/specially_designed_decision_tool_glossary.pdf

WHAT IS "TECHNOLOGY"?

Specific information necessary for the "development", "production" or "use" of a product. The information takes the form of 'technical data' or 'technical assistance'. Controlled "technology" for the Dual-Use List is defined in the General Technology Note and in the Dual-Use List.

Technical Notes

1. 'Technical data' may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.
2. 'Technical assistance' may take forms such as instruction, skills, training, working knowledge, consulting services. 'Technical assistance' may involve transfer of 'technical data'.

WHAT IS "BASIC SCIENTIFIC RESEARCH"?

Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

THE GENERAL SOFTWARE NOTE

For non-Information Security items, therein application to the Intrusion Software controlled items as Computer (Category 4) items, the Wassenaar List does not control "software" which is any of the following:

1. Generally available to the public by being:
   - Sold from stock at retail selling points without restriction, by means of:
     i. Over-the-counter transactions;
     ii. Mail order transactions;
     iii. Electronic transactions; or
     iv. Telephone call transactions; and
   - Designed for installation by the user without further substantial support by the supplier;
2. "In the public domain"; or
3. The minimum necessary "object code" for the installation, operation, maintenance (checking) or repair of those items whose export has been authorised.

THE GENERAL TECHNOLOGY NOTE

The export of "technology" which is "required" for the "development", "production" or "use" of items controlled in the Dual-Use List is controlled according to the provisions in each Category. This "technology" remains under control even when applicable to any uncontrolled item.

Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) or repair of those items which are not controlled or whose export has been authorised.

Controls do not apply to "technology" "in the public domain", to "basic scientific research" or to the minimum necessary information for patent applications.