Export Controls on Intrusion and Surveillance Items: Noble Sentiments Meet the Law of Unintended Consequences...

By Roszel Thomsen and Philip Thomsen

NOBLE SENTIMENTS

Dateline: March of 2011—the Arab Spring

Place: Government Offices in Cairo, Egypt

A few stray pieces of paper caught the eye of an activist searching the Egyptian State Security Investigations Service's (SSI) Cairo headquarters in March 2011, during the Arab Spring. An invoice and accompanying data sheet described a package of hardware, software, and services that provided SSI with the capability to intrude into targeted computers and mobile devices. Once inside, the software surreptitiously granted the SSI access to email and Skype traffic (unencrypted), and provided full remote access to, and control over, the owner's computer or mobile device.[1]

The invoice and data sheet described "FinFisher" and prominently displayed the logo of Gamma International UK Limited, which at the time owned FinFisher. Human rights organizations quickly began asking questions: How had this powerful tool been acquired by the Egyptian SSI? How many other governments were using FinFisher and similar western technologies to spy on their own citizens?[2]

In April of 2012, evidence that another Middle Eastern government was using western technology to monitor political dissidents came to light. According to a report issued by the University of Toronto, Munk School of Global Affairs' Citizen Lab, activists associated with the organization *Bahrain Watch* received emails with what were purported to be images, but in fact were programs that surreptitiously installed software in order to exfiltrate data from the targeted systems. These programs, masquerading as something innocent yet containing malware, are known as Trojans, reflecting their similarities to the infamous Trojan Horse. Upon closer examination, Citizen Lab discovered references to "FinSpy," the core component of FinFisher, in the memory of an infected device. They also noticed that the exfiltrated data had been sent to IP addresses associated with Batelco, the Bahraini state-owned telecommunications company.[3]

In July of 2012, yet another story broke, this time describing journalists who were the targets of attempted infections in Morocco. The journalists, who recently had received international commendations for their efforts to promote free speech, sent copies of the emails to security researchers who concluded, based on references to "RCS" and the usage of the Italian term "guido," that the origin of the Trojan was the software suite RCS developed by Hacking Team, an Italian company. RCS software is one of the main competitors of FinFisher, and it offers similar capabilities.[4]

Another set of press reports described how western information technology companies had supplied IP network surveillance equipment and expertise to the governments of Syria and Libya.[5]

Software known as Utimaco, owned at the time by the UK-based Sophos Safeware, had been used

Roszel Thomsen *is senior partner in the law firm of Thomsen and Burke LLP and founder of the Alliance for Network Security, a trade association composed of leading Information Technology companies. His practice focuses on international trade issues, including export controls and economic sanctions.* ***Philip Thomsen*** *graduated from the Gilman School in Baltimore, Maryland, and is a prospective concentrator in Computer Science at Harvard College, Class of 2020.*

in the surveillance network assembled by the Asad regime in Syria.[6] In France, public pressure mounted following revelations that Amesys, a subsidiary of the French technology company Bull, had sold surveillance systems to the Gadhafi regime in Libya.[7] Other reports disclosed the use of US computer and communications equipment in the Syrian government's telecommunications network for identification and tracking of political dissidents.[8]

Cumulatively, these stories, describing the use of western countries' technologies by regimes with dubious records on human rights, increased the pressure on US and European governments to take steps designed to restrict access to these intrusion and surveillance technologies.[9] The responses on either side of the Atlantic, however, were quite different.

DISPARATE RESPONSES

President Obama issued Executive Order 13,606, blocking the property of and suspending entry into the United States of certain persons with respect to grave human rights abuses by the governments of Iran and Syria via Information Technology.[10]

The US Department of Justice and the Commerce Department's Bureau of Industry and Security (BIS) promptly launched criminal and civil investigations into the diversion of US origin products to unauthorized destinations. Investigators focused on networks of shady intermediaries in places such as Dubai, an historical free port, where traders operated with impunity.

BIS quickly added a reseller, InfoTech, and its principal, Wassim Jawad, to its Entity List of parties subject to sanctions.[11] Shortly thereafter, Computerlinks FCZO in Dubai, a subsidiary of Computerlinks AG of Germany, paid a civil penalty of $2.8 million to settle charges of having diverted US origin equipment and software to Syria.[12] A freight forwarder, Aramex Emirates LLC, paid a civil penalty of $125,000 to BIS in connection with the same facts and circumstances.[13] An Italian company, Area SpA, agreed to pay a $100,000 civil penalty settling charges that it knowingly sold US origin network monitoring equipment to the Syrian Telecommunications Establishment without the required US Government authorization.[14]

On the European side of the Atlantic, however, there have been several investigations, but fewer penalties, at least to date. Instead, the European governments focused primarily on an hypothetical question. Most of the items of interest, for example software for exfiltration of data, used encryption. Therefore, they already were subject to controls under Category 5, Part 2 on the Wassenaar Dual Use List.[15] What would happen, the European export control authorities speculated, if a company such as Gamma or Hacking Team removed the encryption? Would they then be free to sell intrusion and surveillance technology wherever they wanted, free of export controls?

Based on this concern, European governments submitted proposals to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, seeking to implement multilateral controls on products and technologies of concern. During the Wassenaar Plenary meetings in December of 2013, the participating member states unanimously agreed to adopt controls on Intrusion and Surveillance Items via amendments to the Wassenaar List of Dual Use Goods and Technologies.[16]

The language describing the controls on Intrusion and Surveillance Items is intended to be implemented in the national legislation and regulations of each of the participating member states, so that each of the Wassenaar members would have a common list of items subject to export controls.[17] However, the issuance of export licenses is at the national discretion of each of the participating member states, based on their unique perspectives and interests.[18] This will turn out to be an important loophole in the implementation of a multilateral effort to effectively control the acquisition of Intrusion and Surveillance Items by governments with questionable human rights records.

The remainder of this article references the text of the controls on Intrusion and Surveillance items from the Proposed Rule, published by BIS in the US Federal Register on May 20, 2015,[19] because the text closely tracks the language used in the Wassenaar Dual Use List and has generated the most attention by commentators.

CONTROLS ON INTRUSION ITEMS

The Wassenaar Arrangement's controls on Intrusion Items are nuanced, and must be understood

in the context of other important provisions of the Wassenaar Dual Use List and parallel provisions of BIS' Export Administration Regulations (EAR). These controls have been misconstrued by some commentators.

For example, the Proposed Rule would not directly control Intrusion Software, nor would it control the vulnerabilities that the Intrusion Software is designed to exploit. The Proposed Rule also would not authorize prior restraint on publication by academic researchers. Rather, the Proposed Rule describes a new control on *platforms* for the *delivery* of Intrusion Software, and technology for the *development* thereof.[20]

The controls as published by the Wassenaar Arrangement also have two important exceptions, which become apparent only after a close reading of the related Definitions and Notes. The first exception applies to software and technical data that generally are available to the public, such as open source software. The second exception applies to items that are available via "mass market" distribution channels.[21]

The specific text of the Proposed Rule would amend the Commerce Control List of the EAR by adding Export Control Classification Numbers 4A005, 4D004, and 4E001.c to the Commerce Control List (which is the US implementation of the Wassenaar Dual Use List) that read in relevant part as follows:

> 4A005 "Systems," "equipment," or "components" therefor, "specially designed" or modified for the generation, operation or delivery of, or communication with, "intrusion software".
>
> 4D004 "Software" "specially designed" or modified for the generation, operation, or delivery of, or communication with, "intrusion software".
>
> 4E001.c. "Technology" "required" for the "development" of "intrusion software".[22]

These controls are constrained by the definition of "Intrusion Software" which reads in relevant part as follows:

> Intrusion software. (Cat. 4) "Software" "specially designed" or modified to avoid detection by "monitoring tools," or to defeat "protective countermeasures," of a computer or network-capable device, and performing any of the following:
>
> (a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
>
> (b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.[23]

The controls also include three important exceptions in the definition of "Intrusion Software" which are as follows:

> Notes: 1. "Intrusion software" does not include any of the following:
>
> a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;
> b. Digital Rights Management (DRM) "software;" or
> c. "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.[24]

Additionally, the Proposed Rule includes two important definitions:

> Monitoring tools: "software" or hardware devices, that monitor system behaviors 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.[25]
>
> Protective countermeasures: techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing.[26]

In order to assist the reader in understanding the scope of the control on Intrusion Items, two figures are provided: Figure 1 "Scope of the BIS Proposed Rule on Intrusion Items" on page 25 and Figure 2 "Scope of the BIS Proposed Rule on Intrusion Items: Technology" on page 26.

Figure I

Scope of the BIS Proposed Rule on Intrusion Items:

"Systems," "equipment," or "components" therefor, "specially designed" or modified for the generation, operation or delivery of, or communication with, "intrusion software".

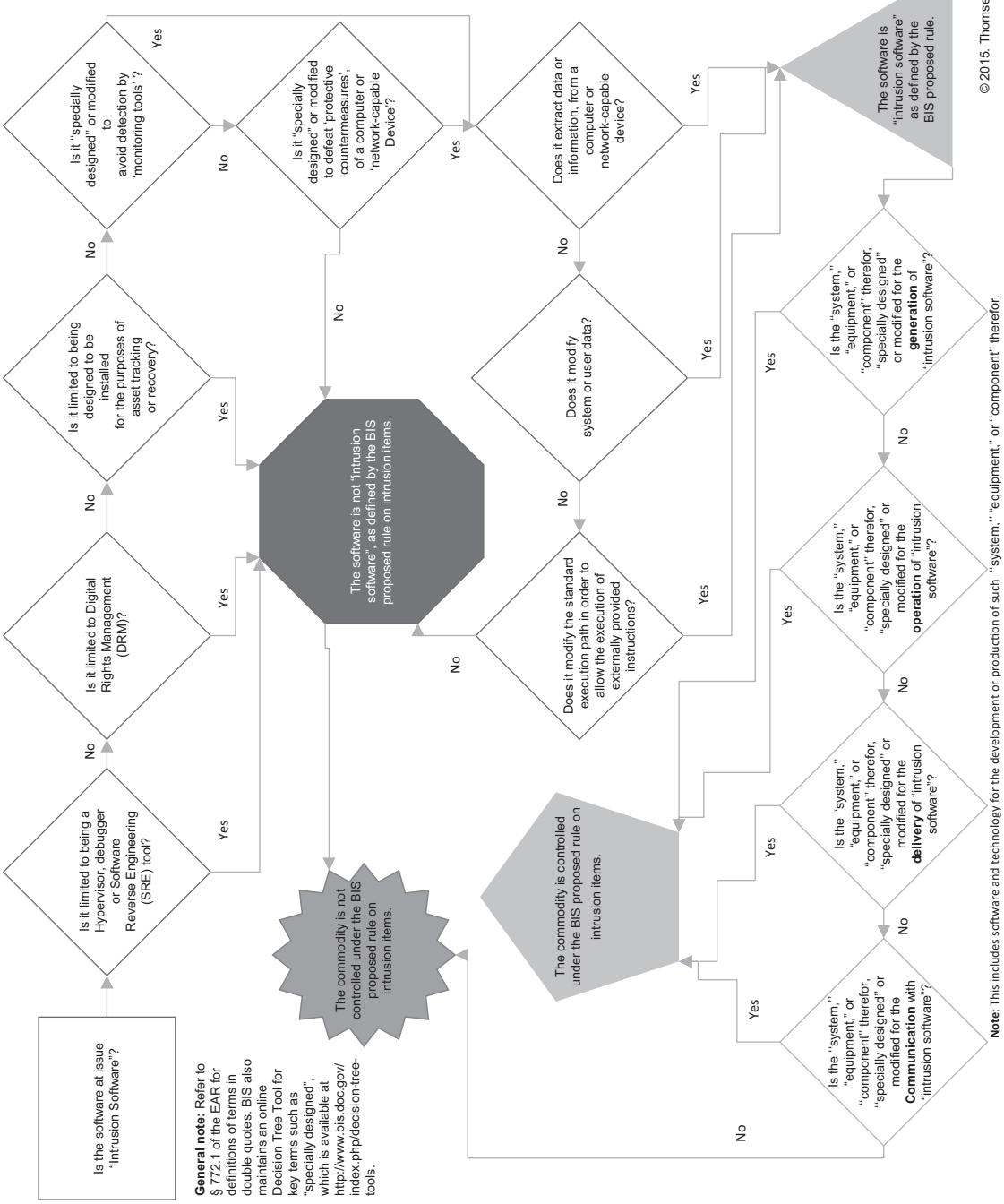
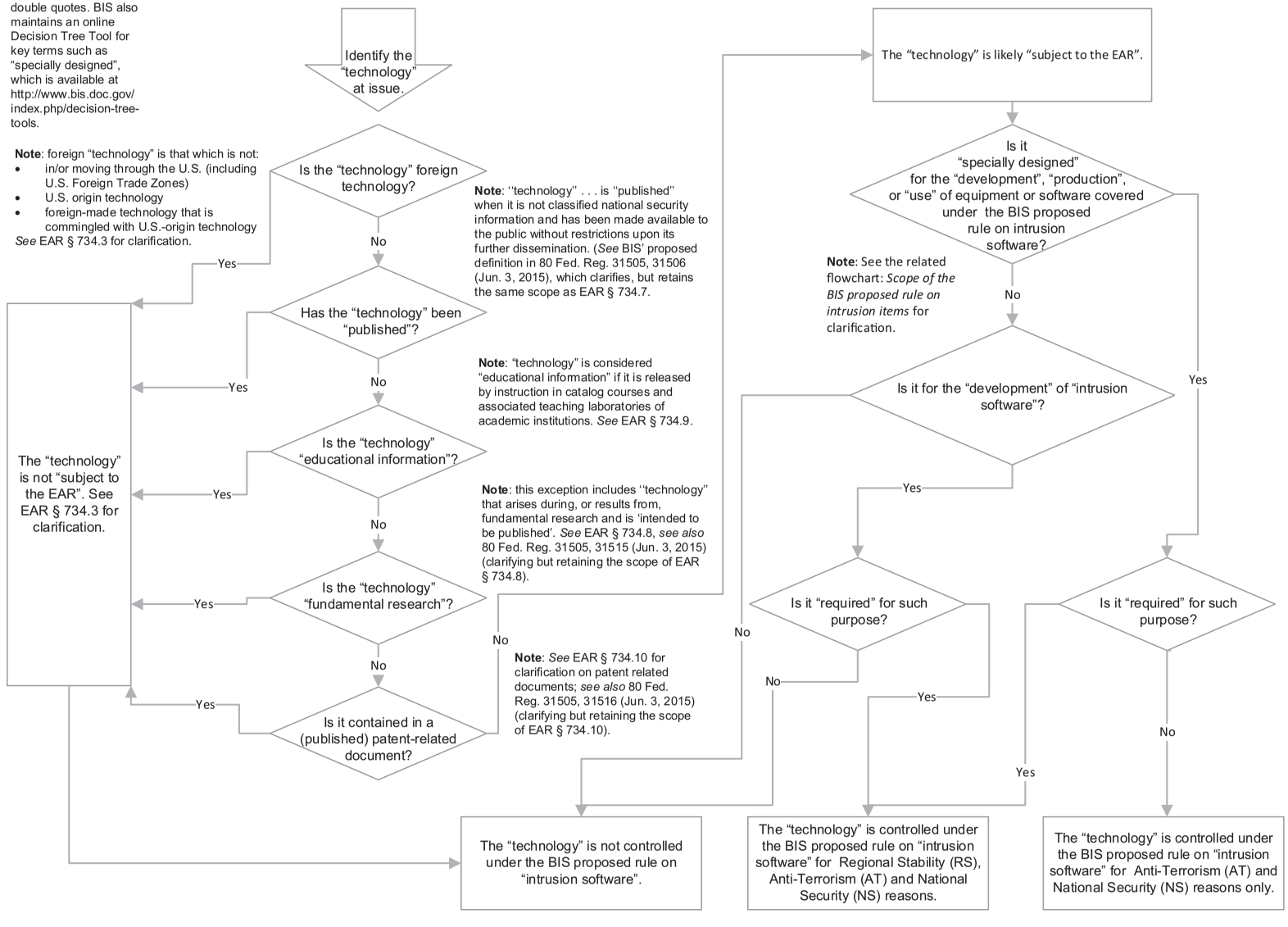


Figure 2

Scope of the BIS Proposed Rule on Intrusion Items: *Technology*



CONTROLS ON SURVEILLANCE ITEMS

The Proposed Rule's controls on Surveillance Items are set forth in the new Export Control Classification Number 5A001.j, which establishes a multi-part test for control eligibility. Only items meeting all parts of the test are subject to control as Surveillance Items. Moreover, there are important exclusion notes and definitions that further limit the scope of this entry. The controls read in relevant part as follows:

> IP network communications surveillance "systems" or "equipment," and "specially designed" components therefor, having all of the following:
>
> j.1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
> j.1.a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498–1));
> j.1.b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
> j.1.c. Indexing of extracted data; and
> j.2. Being "specially designed" to carry out all of the following:
> j.2.a. Execution of searches on the basis of 'hard selectors'; and
> j.2.b. Mapping of the relational network of an individual or of a group of people.[27]

The controls also include the following exceptions in the form of a note:

> 5A001.j does not apply to "systems" or "equipment," "specially designed" for any of the following:
>
> a. Marketing purposes;
> b. Network Quality of Service (QoS); or
> c. Network Quality of Experience (QoE).[28]

These exceptions are preceded by the final component of the control itself, a technical note that reads: "Hard selectors:" data or sets of data, related to an individual (e.g., family name, given name, email, or street address, phone number, or group affiliations).[29]

In order to assist the reader in understanding the scope of the controls on Surveillance Items, there is a figure provided on page 28: Figure 3 "Identifying Coverage Under the New BIS Proposed Rule on IP Network Communications Surveillance".

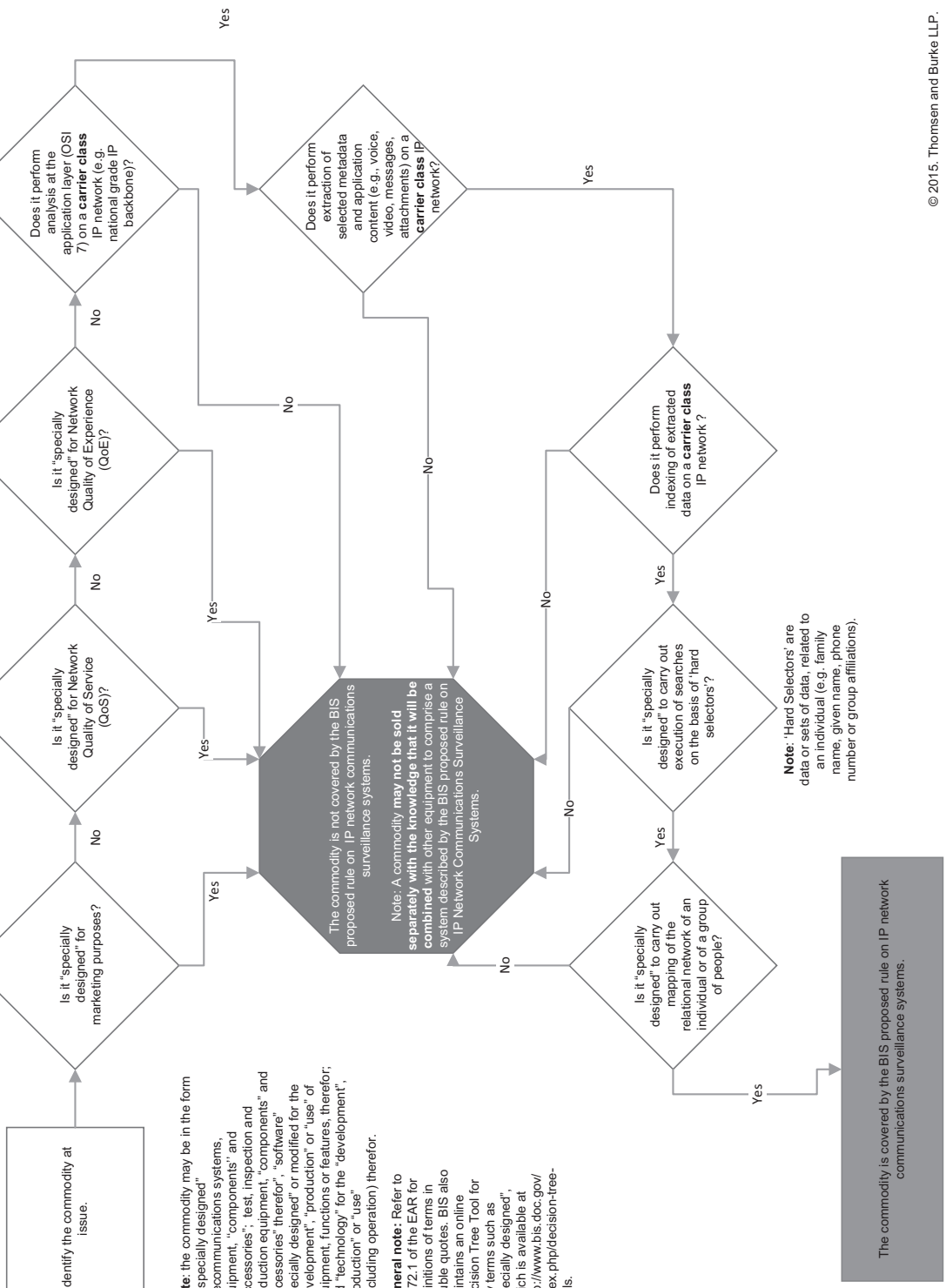
UNINTENDED CONSEQUENCES?

Long before BIS published the Proposed Rule on Intrusion and Surveillance Items, commentators were raising alarms based on their scrutiny of the corresponding Wassenaar text. Some applauded the attempt to control the export of Intrusion and Surveillance Items to regimes that would use them to suppress human rights. Others expressed concerns with respect to the potentially broad reach of the new controls, which could have a chilling effect on cybersecurity research. Many expressed both views.

In a seminal paper, Dartmouth College Computer Science professor Sergey Bratus and his co-authors, DJ Capelis, Michael Locasto, and Anna Shubina, raised two main issues.[30] They criticized use of the term, "modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions" in the definition of Intrusion Software.[31] Even the term of limitation, requiring that the modification must be done in conjunction with avoiding detection of "monitoring tools" or defeating "protective countermeasures," they argued, was overly broad and would cause non-malicious programs to fall under the rubric of Intrusion Software.[32] They offered as their primary example Microsoft's Detours software library which, according to Microsoft, "intercepts Win32 functions by re-writing the in-memory code for target functions."[33] They asserted that many programs use this library as a way to deliver live updates to programs.[34] Because the memory must be located and adjusted in order for the updates to be delivered, Detours must effectively "defeat 'protective countermeasures'" as described in the proposal, specifically Address Space Layout Randomization (ASLR).[35]

Bratus and his co-authors further asserted that "defeating 'protective countermeasures'" as they are defined could encompass many other programs, such as jailbreaks, and described a sandbox as an example.[36]

Figure 3
Identifying Coverage Under the New BIS Proposed Rule on IP Network Communications Surveillance



They asserted that there are many legitimate reasons to "defeat 'protective countermeasures.'"[37] Their paper also described Automated Exploit Generation (AEG), a relatively new idea in computer science, which involves the automated discovery and testing of vulnerabilities in programs, allowing for automated generation of test exploits as they are developed to determine the severity of discovered bugs.[38] This technique is very new, and the authors alleged that new control on Intrusion and Surveillance Items significantly would retard the growth of what could become an important software verification tool, almost akin to a debugger.[39]

On the other hand, support for a narrow construction of the regulations has been offered by experts such as Collin Anderson. In his paper, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies," Anderson asserted that the Wassenaar text is indeed narrowly tailored enough, given a proper interpretation, to target the intended mass surveillance support products.[40] He acknowledged the time and effort devoted to defining the proper scope of the Wassenaar text by its negotiators. He further explained how large scale surveillance systems require technical assistance and training, and suggested that controls on such *services* might be a more logical approach to not only limit the potentially overbroad application of the controls themselves, but also potentially to avoid some of the cases in which, "non-controversial software may be modified for the purpose of delivering Intrusion Software."[41]

Anderson also examined the exemptions enumerated in the Wassenaar text, agreeing that in the short term they did not appear susceptible to potential misuse by companies seeking to relabel products in order to avoid the controls. He also stressed "that export control authorities [must] maintain an expectation about how exempted devices should operate in order to achieve the strict definition of a legitimate objective."[42] Anderson also described why certain companies, such as FinFisher and Hacking Team, who do have products that would appear to clearly fall under this classification, are different from products such as Metasploit and jailbreaks, which are often open source or considered "mass market"[43] and hence would not be controlled under the Wassenaar text.[44]

How, then, would BIS address these issues in the Proposed Rule? It would take almost 18 months to find out.

WASSENAAR CONTROL LIST TEXT AND BIS PROPOSED RULE COMPARED

When BIS published the Proposed Rule, it strayed beyond the Wassenaar text, in some important and restrictive ways. BIS' subsequent attempts to clarify the scope of its Proposed Rule through FAQs on its Web site raised still more questions about the intended scope and impact of the Proposed Rule.[45]

One important difference between the Wassenaar text and the Proposed Rule is that the Wassenaar text is tempered in its scope by the exclusion of publicly available and mass market items.[46] For example, mass market and open source software, such as Metasploit, often are used by security researchers and private security consultants alike. Neither version is subject to control under the Wassenaar Dual Use List.

The Proposed Rule, however, takes a different approach, excluding open source software from control, while retaining controls on mass market software. For example, by all appearances, whereas Metasploit Framework, the open source, free version, would not be controlled, the premium version of the software, Metasploit Pro, would be controlled. This is a particular problem because many companies and security researchers use this and other similar tools to protect their networks.

Neither the Wassenaar text, nor the Proposed Rule, purports to control the vulnerabilities, themselves. Therefore, so-called Zero-Day (previously unknown) vulnerability vendors are not covered by the Proposed Rule, provided that they are selling simply the vulnerability. However, the question arises whether academic research could fall under the control on "technology" "required" for the "development" of Intrusion Items. While this does not appear to be the case, the confusion among many researchers, compounded by their reluctance to contend with export controls with which they have little prior knowledge or experience, could lead to a decline in cooperation on security research, which could have a chilling effect on information security worldwide. Efforts on the part of BIS to clarify the scope through FAQs on its Web site have led to additional concerns, particularly with respect to definitions of terms used in the FAQ that have no counterparts in the text of the Proposed Rule.[47]

Additional concerns with respect to the scope and intent of the controls under the EAR are raised by the language in the Supplementary Information Section under the subheading, Scope of the New Entries, which reads as follows:

> Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices.[48]

Similarly, BIS decided to implement controls on Surveillance Items that are more extensive than the controls imposed by the other Wassenaar members. The BIS stated:

> However, such equipment [(meaning equipment that does not meet all 5 requirements)] may not be sold with knowledge that it will be combined with other equipment to comprise a system described in new paragraph ECCN 5A001.j.
>
> [T]he Export Administration Regulations (EAR) also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry.[49]

These sentences concern many companies because they open the door to the possibility that every single piece of networking equipment, such as a general purpose router or switch, could fall under this control if it is deemed that a company knew it would be used in such a system as defined under ECCN 5A001.j.

While the BIS has stressed that this is not meant to be an end use control, the Proposed Rule arguably is transformed into an end use control, based on the possible incorporation of an item into a larger network that includes somewhere within it some other equipment that may meet the definition of a Surveillance item.

Viewed from a different perspective, there is a legitimate question whether the definition of Surveillance Item is an "empty box."[50] That is, none of the products available in the marketplace today meets this definition. In his paper, Anderson points out that the control only targets systems that would examine all traffic on the IP carrier class network, perhaps inadvertently omitting any smaller scale products that are meant to target individuals.[51] Anderson also points out that such a massive surveillance system as would be required to analyze the entirety of traffic on the IP network backbone would not be supplied by a single company.[52] Instead, it likely would be an amalgamation of one product that collects all the data, which by itself would not be controlled, another product that stores the data, which also would not be controlled by itself, combined with yet another, separate product that would be used to analyze a large amount of data, which again by itself would not be controlled.[53]

Does BIS really intend to control all network equipment that might be incidentally deployed in a network that somewhere has surveillance capabilities described in the Proposed Rule? The export licensing implications of such an interpretation are potentially vast.

PUBLIC COMMENTS ON THE PROPOSED RULE

The Proposed Rule generated an extraordinary number of public comments from diverse constituencies including civil society groups, trade associations, and affected companies, and even Members of Congress. As of August 4, 2015, 264 comments have been submitted.[54]

Some of the commenters appear to be anonymous persons with residual animus from the so-called crypto wars of the 1990s. Others seem to be individuals and organizations that quite simply do not understand the Wassenaar text in the context of Section 734 of the EAR, the General Technology and Software notes, and the definitions published in Part 772 of the EAR. However, there were enough prescient warnings

about the damage the Proposed Rule might do to legitimate cybersecurity activities, that within a week the Deputy Secretary of Commerce, Bruce Andrews, announced BIS would be issuing a second proposed rule, taking into consideration the issues raised in the public comments.[55]

The views of civil society are perhaps best expressed in the comments submitted by Privacy International of the United Kingdom, and a group of US organizations including Access, the Center for Democracy and Technology, Collin Anderson, the Electronic Frontier Foundation, Human Rights Watch, and New America's Open Technology Institute. Both comments recognize the noble sentiments behind the Proposed Rule, but criticize its unintended consequences.[56]

Certain segments of the affected industry filed comments that are not too dissimilar from those expressed by civil society. Examples include the comments submitted by the Alliance for Network Security, and several of its members including Google, Microsoft, and Symantec.[57]

THE SOLUTION? IT'S COMPLICATED...

Regardless of whether one adheres more closely to the views expressed by the anonymous commenters, or by civil society, or by industry, it is abundantly clear that the fear, uncertainty, and doubt surrounding the scope and effect of the Wassenaar text, as adopted in 2013, and its articulation in the Proposed Rule in particular, has resulted in an unfortunate reduction in the reporting of security vulnerabilities to companies, which affects their ability to identify and fix flaws in the products that make the Internet function.

BIS could address this in part by educating the affected constituencies on provisions of the Export Administration Regulations governing published information, information resulting from fundamental research, and educational information set forth in Section 734.7, Section 734.8, and Section 734.9 of the EAR. BIS also could, and should, continue posting FAQs on its Web site, addressing specific techniques of concern, like it did with "fuzzing" in FAQ #4.[58]

In addition, a clarification, (preferably in the form of a Commodity Interpretation published in the EAR) on the question of whether network penetration testing tools, rootkits, and zero-days are controlled as Intrusion Items, would be very helpful. Explicit definitions for these terms would be helpful to further clarify the breadth of the controls. BIS also could alleviate some of the concerns expressed by commentators through creation of new license exceptions or extensions of existing authorities such as the General Software Note and License Exception ENC to exports of Intrusion and Surveillance items.

Another area deserving of attention is that the terms used to describe the list of Surveillance Items subject to control are not technical in nature. For example, terms such as "carrier class IP network," "group of people," and "relational network" are subject to interpretation and essentially meaninglessness from a technical perspective.

These clarifications are particularly important, because the cybersecurity research community has relatively limited prior experience with export controls. Some members of the community also experienced the "crypto wars" of the 1990s and retain a lingering suspicion that the language of the EAR is deliberately obtuse, with stealth "gotchas" as snares for the unwary.[59] If BIS is going to impact such a large community of previously unregulated companies and researchers, it is incumbent on the agency to do so in a regulation that is simple in its language and susceptible of implementation by persons who are not necessarily deeply steeped in export compliance minutiae.

There also is an overriding concern that the fundamental approach of trying to define an Intrusion Item is misguided because it does not distinguish between attack platforms and legitimate defensive penetration testing products. This was a prominent theme in the panel discussion at the Center for Strategic and International Studies, for example, but the companies refrained from recommending ways to differentiate between offensive and defensive products and technologies.[60]

One solution proposed by Bratus and his co-authors was to re-focus those controls on the exfiltration of data rather than on the intrusion itself. This might help to differentiate between offensive and defensive software, ideally allowing for the security research community to be confident in its ability to perform research without fear of violating export control laws and regulations.[61]

Alternatively, Anderson suggested a distinction be made between design and development. In his conception, design (*e.g.*, research) would not be controlled. By comparison, development of a product that meets the definition of an Intrusion Item would be controlled.[62] He further suggested that, "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," as these are primarily limited to the large scale surveillance technologies.[63]

Another potential solution would be a fundamentally different approach to the problem of western companies selling Intrusion and Surveillance items to odious regimes. Rather than focus on the tools and technologies themselves, it may be possible to impose sanctions on the "bad actors." The United States adopted this approach as long ago as April of 2012, in Executive Order 13,606. In April 2015, the President issued Executive Order 13,694, which is not directly applicable because it focuses on critical infrastructure, but provides a comparable framework for a similar sanctions regime.[64] Although it largely has been relegated to the sidelines, as the international focus has shifted to export controls, it may be appropriate to reconsider whether sanctions would be more effective than export controls.[65]

Arguably, the number of companies having not only the tools and technologies to conduct intrusion and surveillance, but also the trust of the host governments of concern, is a fairly small group. If this assumption is accurate, then it should be possible to issue an Executive Order and implement regulations prohibiting transactions with such companies and governments, where the end result is suppression of human rights, similar to the approach in Executive Order 13,606.[66]

Most of these proposals, however, would require (a) deferring implementation of a control that was agreed to in 2013, and (b) returning to the Wassenaar member states suggesting that the existing definitions of Intrusion and Surveillance Items should be eliminated or, at least, reviewed. There may be some (understandable) reluctance to do so.

Indeed, before doing so, the US government should seriously consider whether the Wassenaar Arrangement is the right forum in which to implement this kind of export control. The Wassenaar Arrangement's Initial Elements say nothing about human rights.[67] The organization's mission is to prevent destabilizing accumulations of conventional arms. Granted, there are no other regimes that seem particularly suited to this mission (certainly not Nuclear Suppliers Group, the Missile Technology Control Regime, or the Australia Group).[68] Some aspects of the Wassenaar Arrangement also suggest that it is not the right forum within which to address this particular set of issues.

The Wassenaar Arrangement's membership is one of the reasons that it may not be the ideal forum for addressing these issues. Conspicuous by its absence in the Wassenaar Arrangement is China,[69] which, according to some, has Intrusion and Surveillance Items of the highest order. How can a multilateral export control on Intrusion and Surveillance items hope to be effective if China does not participate?

Furthermore, the Wassenaar Arrangement only provides a list of items that its members should control under their national legislation. All licensing is performed by the member countries at their national discretion.[70] As evidenced by the recent documents exposed by activists targeting Hacking Team, Italy has granted a broad authorization for the company to operate in 46 countries, some of which have questionable records with respect to the protection of human rights.[71] Such a license grant surely would seem to be inconsistent with the noble sentiments that originally inspired the members of the Wassenaar Arrangement to adopt multilateral export controls on Intrusion and Surveillance Items.

CONCLUSION

Perhaps, after the initial storm of controversy has abated, allowing commentators and government officials to re-read the existing control text in light of the public comments, they may reach a common understanding that the existing language is indeed narrowly focused on a small handful of companies and technologies. In support of this narrow construction of the Wassenaar text, it is interesting to note that there has not been nearly the same level of concern expressed in the other Wassenaar member countries as has been the case in the United States.

In Sir Arthur Conan Doyle's famous detective story, *Silver Blaze*, Sherlock Holmes focuses on a

crucial piece of evidence: "the curious incident of the dog in the night-time":

> Gregory (Scotland Yard detective): "Is there any other point to which you would wish to draw my attention?"
> Holmes: "To the curious incident of the dog in the night-time."
> Gregory: "The dog did nothing in the night time."
> Holmes: "That was the curious incident."[72]

Although the United States may have the largest single concentration of security researchers and firms, there are plenty of very competent security researchers in other Wassenaar member countries. Is the absence of a similar outcry outside the United States evidence that the other Wassenaar member governments do not share the same broad reading of the controls that has given rise to concerns in the United States? (A note published by the UK's Export Control Organization within the Department for Business, Innovation and Skills, for example, supports a narrower understanding of the Wassenaar text than some US critics of the Proposed Rule have claimed.)[73] The State Department should immediately demarche the other Wassenaar member governments to determine whether this supposition is correct.

Perhaps, Bratus and his co-authors are correct, and there really is a way to revise the existing language of the controls on Intrusion and Surveillance Items to address concerns expressed in the public comments. BIS should work closely with its Technical Advisory Committees, industry, and civil society to determine whether amendment of the existing language would make it possible to differentiate between offensive versus defensive technologies.

Perhaps, the public comments that posit that there is no meaningful distinction between offensive and defensive technologies are accurate. If this is the case, then the existing list-based controls on Intrusion and Surveillance Items should be abandoned, in favor of an alternative approach or approaches.

If alternatives are considered, either as a replacement for, or in addition to, the list-based approach, then BIS should consider, among other options, the suggestions made by Anderson and others to focus on the technical assistance and training provided by the operators of Intrusion and Surveillance Items. These and other approaches argue in favor of sanctions, as opposed to export controls, as the primary mechanism for implementing such a policy.

In conclusion, at minimum, as it prepares the second proposed rule, BIS should consider the following:

- Whether the Wassenaar definition of Intrusion and Surveillance Items describes items that truly warrant being subject to export controls? Stated differently, is the ecosystem of offensive and defensive technologies so inextricably intertwined that it is simply infeasible to differentiate between the two?
- Whether the licensing policy expressed in the Proposed Rule strikes the right balance? For example, the Proposed Rule attempts to control Intrusion and Surveillance Items that the Wassenaar text would decontrol under the mass market note. Is it even feasible to control items that are readily available in the marketplace?

Finally, the United States and all the Wassenaar member nations should be asking whether there are better ways to accomplish the noble sentiments of protecting human rights without the attendant adverse consequences for cybersecurity researchers and vendors.

NOTES

1. *See* Kevin McVeigh, "British Firm Offered Spying Software to Egyptian Regime—Documents," *The Guardian*, Apr. 18, 2011, *http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher*.
2. *Id.*
3. Morgan Marquis-Boire *et al.*, "From Bahrain with Love: FinFisher's Spy Kit Exposed," *The Citizen Lab*, Jun. 25, 2012, *https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/*.
4. *Id.*
5. *See, e.g.*, Paul Sonne & Margaret Coker, "Firm Aided Libyan Spies," *The Wall Street Journal*, Aug. 20, 2011, *http://www.wsj.com/articles/SB10001424053111904199404576538721260166388*; John Riberio, "HP Says its Products Sold Unknowingly to Syria by Partner," *CIO*, Nov. 26, 2012, *http://www.cio.com/article/2390177/hardware/hp-says-its-products-sold-unknowingly-to-syria-by-partner.html*; John Hudson, "Meet the U.S. Companies Helping Censor the Arab Web," *The Wire*, Mar. 28, 2011, *http://www.thewire.com/technology/2011/03/meet-corporate-enablers-helping-censor-arab-web/36134/*.
6. "Police State: Is Syria Monitoring Protestors with German Technology?," *http://www.spiegel.de/international/world/police-state-is-syria-monitoring-protesters-with-german-technology-a-796510.html* (Nov. 8, 2011, 12:19PM EST).
7. Ryan Gallagher, "French Company that Sold Spy Tech to Libya Faces Judicial Inquiry Amid New Allegations," *Slate*, Jun. 19,

2012, *http://www.slate.com/blogs/future_tense/2012/06/19/amesys_facing_inquiry_in_france_over_selling_eagle_surveillance_technology_to_qaddafi_.html*.

8. "Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma," *The Citizen Lab*, Nov. 9, 2011, *https://citizenlab.org/2011/11/behind-blue-coat/*; and Hudson, *supra* n.5.
9. *See* Ryan Gallagher, "How Government-Grade Spy Tech Used a Fake Scandal to Dupe Journalists," *Slate*, Aug. 4, 2015, *http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html*.
10. Exec. Order No. 13,606, 77 Fed. Reg. 24571 (Apr. 22, 2012).
11. Press Release, Bureau of Industry and Security, "BIS Adds Two Parties to Entity List for Sending Internet Filtering Equipment to Syria," (Dec. 15, 2011) (available at *http://www.bis.doc.gov/index.php/about-bis/newsroom/archives/press-release-archives/65-template/press-release/233-bis-adds-two-parties-to-entity-list-for-sending-internet-filtering-equipment-to-syria*); 76 Fed. Reg. 78146 (Dec. 16, 2011).
12. Press Release, Bureau of Industry and Security, "Bureau of Industry and Security Announces $2.8 Million Civil Settlement with Computerlinks FZCO for Charges Related to Unlawful Exporting of Technology to Syria," (Apr. 25, 2013) (available at *https://www.bis.doc.gov/index.php/about-bis/newsroom/press-releases/102-about-bis/newsroom/press-releases/press-releases-2013/524-bureau-of-industry-and-security-announces-2-8-million-civil-settlement-with-computerlinks-fzco-for-charges-related-to-unlawful-exporting-of-technology-to-syria*).
13. Press Release, Bureau of Industry and Security, "U.A.E. Freight Forwarder Agrees to Pay $125,000 Penalty in Connection with Export and Reexport of Monitoring Devices to Syria," (May 20, 2014) (available at *https://www.bis.doc.gov/index.php/about-bis/newsroom/107-about-bis/newsroom/press-releases/press-release-2014/683-u-a-e-freight-forwarder-agrees-to-pay-125-000-penalty-in-connection-with*).
14. Press Release, Bureau of Industry and Security, "Italian Company Agrees to $100,000 Penalty for Unlawful Technology Export to Syria," (Sept. 17, 2014) (available at *https://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*).
15. The Wassenaar Arrangement on Export Control for Conventional Arms and Dual-Use Goods and Technologies (The Wassenaar Arrangement) is a multilateral export control regime with 41 participating countries. The Wassenaar Arrangement on Export Control for Conventional Arms and Dual-Use Goods and Technologies, *www.wassenaar.org* (last updated Jun. 18, 2015). The Wassenaar Arrangement maintains a commodity control list, The List of Dual-Use Goods and Technologies and Munitions List, which forms the basis of the participating countries' export controls on such items. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, List of Dual-Use Goods and Technologies and Munitions List, WA-LIST (14) (Mar. 25, 2015) [hereinafter the Wassenaar Dual Use List] (the List organizes controlled commodities into categories, Category 5, Part 2, is reserved for "information Security" commodities).
16. Public Statement, the Wassenaar Arrangement, 2013 Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Dec. 4, 2013).
17. The BIS maintains this list in the EAR as the Commerce Control List. 15 C.F.R. Part 730 *et. seq.*, Supp. No. 1.
18. Public Statement, the Wassenaar Arrangement, What is the Wassenaar Arrangement (2006) ("All measures undertaken with respect to the Arrangement are in accordance with member countries' national legislation and policies and implemented on the basis of national discretion.").
19. Wassenaar Arrangement 2013 Plenary Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28853 (proposed May 20, 2015).
20. *Id.* at 28853.
21. The Wassenaar Dual Use List, *supra* n.15 at 86.
22. Wassenaar Arrangement 2013 Plenary Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28854.
23. *Id.* at 28858.
24. *Id.*
25. *Id.*
26. *Id.*
27. Wassenaar Arrangement 2013 Plenary Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28861.
28. *Id.*
29. *Id.*
30. Sergey Bratus, *et al.*, "Why Wassenaar Arrangement's Definition of Intrusion Software and Controlled Items Put Security Research and Defense at Risk and How to Fix It," (2014).
31. *Id.* at 2; Wassenaar Arrangement 2013 Plenary Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28858.
32. Bratus, *supra* n.30 at 2; Wassenaar Arrangement 2013 Plenary Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28858.
33. Microsoft, Detours—Microsoft Research, *http://research.microsoft.com/en-us/projects/detours/* (last visited Aug. 4, 2015).
34. Bratus, *supra* n.30 at 3.
35. *Id.*; Wassenaar Arrangement 2013 Plenary Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28858.
36. Bratus, *supra* n.30 at 9; Wassenaar Arrangement 2013 Plenary Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28858.
37. Bratus, *supra* n.30 at 3.
38. *Id.* at 10.
39. *Id.*
40. Collin Anderson, Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies, at 4 (2015).
41. *Id.*
42. *Id.* at 7.
43. *See* The Wassenaar Dual Use List, *supra* n.15 at 86 (items sold via "mass market" distribution channels are exempted from the controls).
44. Anderson, *supra* n.40 at 11-12.
45. *See* BIS Frequently Asked Questions, *http://www.bis.doc.gov/index.php/policy-guidance/faqs* (last visited Aug. 4, 2015).
46. *See* The Wassenaar Dual Use List, *supra* n.15 at 86.
47. *See* BIS Frequently Asked Questions, *supra* n.45 (*e.g.*, "hacking").
48. Wassenaar Arrangement 2013 Plenary Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28854.
49. *Id.*
50. Teleconference, Bureau of Industry and Security, Intrusion and Surveillance Items Proposed Rule (Cyber Rule) for Implementation of the Wassenaar Arrangement 2013 Plenary Agreements (May 20, 2015) (BIS did identify "only 5 [or] 6 systems that would fall under the Network Surveillance Control").
51. Anderson, *supra* n.40 at 14-16.
52. *Id.*
53. *Id.*
54. Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items, *http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0001* (last visited Aug. 4, 2015) [hereinafter Wassenaar Public Comments]. *See also* Amendment

to the Cybersecurity Information Sharing Act (CISA), S.Amdt. 2612 to S. 754, 114th Cong. (2015) (Sen. Wydner introduced a bill to amend the Cybersecurity Information Sharing Act, a bill which would allow the US government access to Internet traffic information received by technology companies. The amendment, which did not specifically address the Proposed Rule, highlighted the importance of public awareness "regarding cybersecurity risks and voluntary best practices for mitigating and responding to such risks".).

55. Tom Risen, "U.S. Reboots Plan to Halt Tech Sales to Foreign Hackers," *U.S. News*, Aug. 4, 2015, *http://www.usnews.com/news/articles/2015/07/30/us-reboots-wassenar-anti-surveillance-trade-plan*.
56. *See* Wassenaar Public Comments, *supra* n.54.
57. *See id*.
58. BIS Frequently Asked Questions, *supra* n.45.
59. History of the First Crypto War, *https://www.schneier.com/blog/archives/2015/06/history_of_the_.html* (Jun. 22, 2015, 13:35 EST).
60. Stewart Baker, Katie Moussouris, Cristin Goodwin, Laura Galante & Michael Maney, Panel Discussion on the BIS Proposed Rule for Intrusion Software Platforms (Jul. 24, 2015).
61. Bratus, *supra* n.30 at 4.
62. Anderson, *supra* n.40.
63. *Id*.
64. Exec. Order No. 13,694, 80 Fed. Reg. 18077 (Apr. 1, 2015).). Additional examples of sanctions used to address similar issues can be found in Exec. Order 13288—Blocking Property of Persons Undermining Democratic Processes or Institutions in Zimbabwe, 68 Fed. Reg. 11457 (Mar. 6, 2003), Exec. Order 13348—Blocking Property of Certain Persons and Prohibiting the Importation of Certain Goods from Liberia, 69 Fed. Reg. 44885 (July 22, 2004) and Exec. Order 13619—Blocking Property of Persons Threatening the Peace, Security, or Stability of Burma, 77 Fed. Reg. 41243 (July 11, 2012). A contrary view that multilateral export controls remain preferable to unilateral sanctions is expressed by Mailyn Fidler in Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis, *http://moritzlaw.osu.edu/students/groups/is/files/2015/06/Fidler-Second-Review-Changes-Made.pdf* (last visited Aug. 4, 2015)
65. Exec. Order No. 13,606, *supra* n.10.
66. *Id*.
67. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Guidelines & Procedures, including the Initial Elements (Jul., 2014).
68. *Id*.
69. Participating States, *http://www.wassenaar.org/participants/* (last visited Aug. 4, 2015).
70. *See supra* n.18 and accompanying text.
71. David Gilbert, "Hacking Team Hacked: Spy Tools Sold to Oppressive Regimes Sudan, Bahrain and Kazakhstan," *Int'l Bus. Times*, Jul. 6, 2015, *http://www.ibtimes.co.uk/hacking-team-hacked-spy-tools-sold-oppressive-regimes-sudan-bahrain-kazakhstan-1509460*. *See also* "Hacking Team Table of Anticipated Destinations for Italian Licensing," available at *https://drive.google.com/file/d/0B2q69Ncu9Fp_MzhYTGJuNjJLWUdVazkzam0xZVdNOVdqRm5R/view?pli=1* (last visited Aug. 14, 2015).
72. Sir Arthur Conan Doyle, Silver Blaze (1892).
73. Export Control Organization, Guidance on Intrusion Software Controls, 2015 (available at *http://blogs.bis.gov.uk/exportcontrol/files/2015/08/Intrusion-Software-Tools-and-Export-Control1.pdf* (last visited Aug. 10, 2015).

September/9900502670