Malware Counter-Proliferation and the Wassenaar Arrangement

Trey Herr
Belfer Center’s Cyber Security Project
Harvard Kennedy School
Cambridge, M.A., USA

Abstract: Can states control malware? It is a radical asymmetry: the power of a modern nation-state arrayed against a few hundred thousand bytes of code and its creators, but an imbalance whose counterintuitive nature impacts the security of citizens, corporations, and governments alike. This paper evaluates export controls found in the Wassenaar Arrangement targeting malware in the context of the research into the malicious software ecosystem. The article highlights that export controls place burdensome restrictions on research and commercial information security efforts. Looking at the market for malicious software, incentivising the discovery of new vulnerabilities to reduce their availability to attackers would be more effective in curtailing malicious activity.

Keywords: foreign policy, proliferation, cyber crime, malware market, Wassenaar Arrangement, export controls

1. INTRODUCTION

The malicious software ecosystem is built on a set of interlinked markets where a combination of exploits, payloads, and more developed services like botnets are bought, sold and rented. Unlike more traditional illicit goods markets, the principle content of these products is information. The value of goods in the malware market is thus often derivative of their secrecy, as each can be replicated without marginal cost.

Government’s interaction with these markets and the application of state power to restrict the flow of goods into and out of this malware ecosystem has been a public policy issue for many years. However, international efforts to curtail the deployment of malware and its growth in sophistication have yielded limited success. The controversy over changes to the Wassenaar
Arrangement, while an intriguing illustration of state-civil society relations and the nature of malware, obscures a deeper misunderstanding of the threat environment.

This paper leverages previous research into malicious software markets and a review of internal documentation from intermediaries and broker firms in this ecosystem. These different sources are combined to present a picture of the malware market’s structure and its interaction with state power. By evaluating this market against the malware-specific language of Wassenaar, this paper highlights three key limitations in the export control approach to counter-proliferation – harm to beneficial research activity, minimal impact on malicious activity, and the challenge of creating multilateral coordination regimes. Increasing the clarity of national policy goals around malicious activity and creating better incentives for vulnerability research represents a more effective path forward.

2. THE WASSENAAR ARRANGEMENT

The Wassenaar Arrangement was signed in 1996 from a desire to revise the Cold War era arms export control process and to integrate former Soviet bloc states into an international forum to restrict the flow, dissemination and proliferation of potentially dual-use technologies to terrorist groups and states of concern (Dursht, 1997). Wassenaar is not an enforceable legal regime or a treaty, but rather a means for participating states to coordinate their respective domestic policies. It is intended to prevent regulatory arbitrage, where businesses relocate their activities to the least restrictive jurisdiction. This arbitrage can undermine export controls and pose a particular challenge for information security (Farrell, 2006).

In December 2013, the British and French governments proposed, with the support of other member states, to change the Arrangement’s language and add new rules to cover the tools and technology associated with malicious software (Anderson et al., 2015). One goal for the new controls was to restrict the sale of malware to repressive governments that used technology to monitor journalists and political dissidents. Evidence of this pervasive surveillance industry involved a host of companies in countries like Egypt, Bahrain, and Pakistan (Marquis-Boire et al., 2013; Gamma International, 2013; Hypponen, 2011). The original intent of the new controls was to target firms such as Hacking Team and Gamma Group, which were selling these surveillance tools to these states.

These modifications to Wassenaar created a new restricted product, ‘intrusion software’, which referred to the tools designed to bypass defences, gain access to computers, and extract data from them. Rather than target these products directly, the Wassenaar language provides for controls on the supporting infrastructure used to generate, deploy, or communicate with this intrusion software (Wassenaar Arrangement, 2015). The controls discussed here are a subset of the broader Wassenaar changes that include separate restrictions on IP network surveillance tools intended for the collection and analysis of large volumes of network traffic. These products are distinct from malware and thus not considered here.
There are additional subtleties around the construction and use of these malware components that are not detailed here. Exploit development, for example, involves a discovery and testing process to advance from knowledge of a vulnerability to an exploit suitable for use on a target system, not just a basic proof of concept. This process takes time, talent, and a not insignificant measure of luck. The persistence of these components, a feature that may differentiate state from non-state group’s code, tends to originate in the design of the respective payloads and propagation methods and deserves a more comprehensive treatment than is possible here.

The malware specific changes to Wassenaar were not directly instigated by the United States, but much of the ensuing controversy was provoked by their implementation in American export control law which broadens the original language (Bureau of Industry and Security, Department of Commerce 2015). In May 2015 the US Department of Commerce issued a draft rule which expanded the rules to require source code submission with license applications and proposed to apply a policy of ‘presumptive denial’ for products which integrated zero-day vulnerabilities (Fidler, 2015). These controls attempted to replicate the sort of restrictions US export law placed on cryptographic tools, targeting their sale rather than use.

3. THE MARKET FOR MALWARE

A. What is malware?
There are a host of different ways to talk about malicious code and categorise its various functions and features; perhaps too many, as competing definitions and naming schemes abound. To focus the discussion, this paper employs the PrEP framework which describes malicious software tools as sharing three fundamental components: a propagation method, exploits, and a payload (Herr, 2014).

The propagation method is a means of transporting code from its origin to the target computer. Anything that can hold or transmit data can propagate malware, be it an email attachment or USB memory stick. Exploits are code designed to take advantage of software flaws and enable attackers to compromise a computer system; they support both the propagation method and payload. The payload contains the malware’s key functionality: software delivered to a computer to achieve some specific goal, such as pilfering intellectual property or causing physical damage. The botnet infrastructure employed as a propagation method in spear phishing attacks, for example, is quite different from the payload these attacks distribute, and they are often bought and sold separately. It is important to note that while this framework can be a useful conceptual tool, it is not intended for direct adoption as a legal construct.

B. Why a market?
The market is a well-studied phenomenon in social science. Using the models and language of a marketplace allows us to tie in existing scholarship and to structure an analysis of how malicious actors might respond to different policy interventions. The price a state is willing to pay for a certain vulnerability may set the market for other players. This could then encourage new suppliers to develop exploits for the vulnerability and potentially price out relatively
‘friendly’ actors such as a responsible software vendor. The National Security Agency (NSA) bidding on a vulnerability for Google’s Chrome browser might block it from being sold to Google directly and patched.

The existence of a market-like apparatus for the exchange, purchase, and sale of malware components is not a novel idea, with previous work looking at aspects of pricing (Ablon, Libicki, and Golay, 2014) and the commoditisation process (Grier et al., 2012), as well as larger economic structures (Huang et al., 2015). The buyers and sellers are individuals, firms, and even governments (Fung, 2013). Specialisation has become nearly a de-facto standard with one paper observing that ‘the underground economy has evolved into a complex ecosystem with commoditised services’ (Huang et al., 2015).

Understanding the functioning of this market is important to evaluate how export controls may be applied to limit the type of goods offered and curb the behaviour of participants. This market is largely a notional one – the interactions of vulnerability discoverers, exploit brokers, and buyers occur in a variety of forms and fora across time and space (Motoyama et al. 2011). Employing the framework of a marketplace is made possible by the competition between different sites and suppliers to attract business and generate revenue. Buyers look across a variety of sources to find commodities and services and sellers will concentrate expertise into particular products to improve economies of scale.

C. Market forces

(i) Supply

There is a tremendous variety in the underground forums where buyers select malware components and related services, but also a clear distinction between the supply and demand relationships for vulnerabilities. Demand is determined by buyers with an interest in purchasing and deploying malware. The source of supply varies by malware component. Vendors’ software is the primary source of new vulnerabilities, for example. Propagation methods are numerous; an example is the herds of infected computers known as botnets. Marshalling these machines and renting them is not a trivial process and may depend on the skill and pre-existing resources of the seller. Payloads are largely developed by individuals or small groups and may be purchased, modified, or even stolen. The variation in their purpose means that groups with different skill levels may be unsuccessful at adapting the tools of others or creating their own for complex tasks.

Malware components, and in particular payload, may be reused but adapting payloads may require a high degree of engineering effort. Adapting highly specific payloads, like Stuxnet, is difficult. Code written for a more general purpose is easier. A prominent example of this is Zeus, a popular malware family used to target banks and financial institutions, whose source code was leaked online in 2011 without cryptographic protection (Fisher, 2011). Less than six months later, several new malware families had integrated some or all of the Zeus code and saw sales growth as a result (Damballa, 2011).
Malware sales may be for single components or for several assembled into a service like an exploit kit, which combines propagation methods and one or more exploits (Clarke, 2013). The Angler exploit kit, for example, appears to have integrated the Cryptowall payload with great success (Mimoso, 2015a). Groups may also supply fully operational tools like the GammaGroup’s FinSpy surveillance package (Anderson, 2015).

(ii) **Demand**

The determinants of demand vary, as some groups appear to select targets based on the tools available to them while others find tools to satisfy strong preferences about targets. The implications for tool-focused groups are that demand is shaped by the security posture and configuration (e.g. vulnerabilities present and unpatched) of the potential victims. Targets are selected based on the tools available, making these attacks more opportunistic. A different calculus reigns where the potential target is more important than the tool employed. Target focus implies a willingness to develop or to purchase and modify components to fit the needs of a narrowly defined target set. Being target-focused may require groups to dedicate greater resources to develop appropriate code.

(iii) **Reputation and trust**

How do you establish trust in a den of thieves? Reputation mechanisms are the means by which two parties in a transaction establish a basis of trust on which to guarantee the desired exchange of goods or services for compensation (Yip, Webber and Shadbolt, 2013). Understanding the potential for fraud in any given transaction, buyers must evaluate the relative quality and character of the good being purchased. There are means to overcome this natural information asymmetry. Independent crowd sourced mechanisms can be used to provide evaluations and customer feedback, like the star based ratings systems found on mainstream e-commerce sites such as Amazon and eBay (Holt, 2012).

In the malicious software market, some forums allow users to post information about the quality of code and services received, to complain about poor customer support, or to call out fraudulent transactions or failure to receive the promised product. There are also systems relying on an interpersonal ‘vouching’ protocol, not unlike friend of friend chains in other illicit environments, which allows existing trusted networks to add nodes at the edges by brokering introductions between previously disconnected parties (Motoyama et al., 2011). Prolific suppliers can use this as a tool to enhance their legitimacy in new environments or even help suppress the sales of competitors as their reputation precedes them.

**D. Supply side actors**

(i) **Malware components and service vendors**

Supply side actors are firms and organisations hawking particular malware components, such as a payload focused on the extraction of user credentials or exploit kits. Suppliers in the high end of the market form a highly fragmented ecosystem of skilled individuals who focus on the development and sale of new exploits for well secured software or high value targets. Companies selling exploits, like ReVuln and Exodus Intelligence, generally operate on
a subscription service model comparable to a data plan for a cellphone (Constantin, 2012). In these programmes, governments and other intermediaries pay a certain amount every year in exchange for a fixed number of exploits. By one estimate, in the entire marketplace there are at least half a dozen such firms capable of selling more than 100 new exploits a year to both governments and non-state actors, with an average list price ranging from $40,000 to $160,000 (Frei, 2013).

Suppliers at the low end of the market sell basic malware components like payloads and propagation methods as well as vulnerabilities. Rarely if ever does this low end market see sales of vulnerabilities unknown to the vendor (zero-days). These suppliers also offer services like click fraud, intended to drive visitor traffic through particular ads, and pay-per-install (PPI), where threat groups can pay according to the vendor’s success at infecting different users (Team Cymru, 2011). Interaction tends to take place via Internet relay chat (IRC) or through a shifting collection of forums like Agora, Darkode, and Abraxas.

(ii) Supply side intermediaries
Supply side intermediaries are firms with a legitimate business presence who sell malicious software components to buyers, generally states. These groups may participate directly in the market as buyers in order to expand their wares, but also function as suppliers to at least a portion of the market. These intermediaries resell more developed products intended largely for states, but which may also involve some more sophisticated criminal groups. This mix is interesting as some state organisations may be less capable than non-state actors. The canonical state threat, America’s NSA or Israel’s Unit 8200, is generally accorded a high degree of technical capability. Others, like intelligence bodies of the Republic of Sudan and Ethiopia, appear to be lacking even the skillset required to operate Hacking Team’s products without potentially glaring errors and remedial training (Currier and Marquis-Boire, 2015).

Hacking Team, a prominent Italian company whose internal email system and documentation were leaked onto the web in May 2015, uses a regular stream of new exploits to support its core malware called Galileo RCS or Remote Control System (Anderson, 2015). This malware can be used to spy on a variety of desktop and mobile phone operating systems. Customers can then purchase a licence to increase the number of computers and phones they collect information from at any given time. Companies even offer training, customisation and maintenance features for more developed users.

E. Demand side actors

(i) States
States are highly resourced actors with specific objectives beyond just affecting information systems. States are capable of employing, and have demonstrated interest in, destructive payloads. They also have the human capital and time to develop components internally rather than exclusively through purchase or reuse. The capabilities of the most advanced states are moving ahead of the market and the increasing frequency with which they use malicious software creates a proliferation challenge (Herr and Armbrust, 2015). This proliferation disseminates more sophisticated components to other threat actors where they can be discovered
and potentially re-engineered. Nevertheless, this again remains a challenging task depending on the code obtained (Moshe and Keith, 2015).

**(ii) Non-state actors**

Non-state actors are the canonical information security threat – criminal groups, gangs and malicious individuals. Varying levels of resources and capability mean that a common decision-making process for these groups is difficult to generalise, but they almost certainly have access to fewer human or material resources than states. Non-state groups’ interactions are rarely overt, but their goals are generally oriented around financial gain. This category may include organisations with a political or otherwise ideological agenda, but the sophistication of the tools employed tends to be lower. For example, non-state groups will often use distributed denial of service (DDoS) attacks for their disruptive and propaganda benefits.

**(iii) Demand side intermediaries**

Demand side intermediaries are groups that contribute to victim security. This may be through providing information assurance resources or managed security services. These intermediaries could also be involved in directly purchasing vulnerabilities like Verisign’s iDefense Vulnerability Contributor Program (VCP), which buys vulnerability and exploit information with the intent of disclosing it to vendors (Frei, 2013). This disclosure only takes place after a delay, sometimes substantial, in which subscribers to the iDefense program have exclusive access to the information. These defensive firms participate in the market and affect the stock of goods by disclosing vulnerabilities back to vendors after a delay. There is also a small industry of companies who, for a fee, will conduct mock attacks on organisations’ networks to pinpoint weaknesses. These penetration testing firms employ exploits in the same manner as a criminal or state attacker, and often have an interest in the latest research in order to be most effective but can purchase exploits more cheaply since they do not require exclusive access.

**(iv) Software vendors**

Vendors may also be buyers in the market through vulnerability purchase programmes (VPPs), not participating directly but affecting the incentives of potential suppliers and the available price and quality of goods. These take a variety of forms and many reward more than standalone vulnerabilities; compensation is also given out for novel attack and defence techniques. Firms such as Google and Facebook organise ‘bug bounties’ (also known as Vulnerability Reward Programmes), designed to encourage researchers to disclose vulnerabilities directly in return for prestige and a cash reward (Popper, 2015). Some companies, like HackerOne and BugCrowd, sit in between organisations and vulnerability researchers, managing these bounty programs for software firms (Ellsmore 2013).

There are also competitions where researchers are given set amounts of time to find vulnerabilities in major commercial software, and to prove their effectiveness with a rudimentary exploit. In 2015 Pwn2Own, a competition held in Canada, paid out prizes totalling more than $400,000 for vulnerabilities in the Chrome, Safari, Internet Explorer, and Firefox browsers as well as other software (Goodin, 2015). However, the sponsor of a similar competition in 2016, Hewlett Packard, pulled out after concerns that changes to Wassenaar might impose penalties or unmanageable legal costs on the event (Mimoso, 2015b).
4. ANALYSIS

Wassenaar’s impact on the malware market affects few supply side actors and generally only those demand side actors contributing to enhanced software security. The Arrangement’s language takes an overbroad, and thus largely ineffective, approach to disrupting the global flow of malicious software. It does little to affect the existing malware markets, it harms security research, and its export controls are weak in the face of the difficulties of effective international coordination.

A. Missing the mark

The Wassenaar’s language defines ‘intrusion software’ as:

‘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 (Wassenaar Arrangement, 2015)

The Wassenaar controls do not target this ‘intrusion software’ directly. Instead the controls focus on supporting components which are any software, systems, equipment, components, or technology used to generate, operate, deliver, or communicate with intrusion software. In effect, Wassenaar targets the means by which intrusion software is built, deployed, or communicated with (Dullien, Iozzo, and Tam, 2015).

One of the major sources of innovation on non-state-authored malicious software comes from state-built code. Duqu, a likely state-built espionage platform discovered in 2011, used an exploit in the Windows operating system to escalate privileges on a target machine and enable payload execution (Bonfante et al., 2013b). Less than a year after the announcement of its discovery, the same exploit was integrated into two major exploit kits and used in attacks against a range of targets by criminal groups (Wolf, 2013). This reuptake of the originally state-authored package drove renewed interest in kernel level exploits to the point where Microsoft was forced to more frequently publish patches to this and related vulnerabilities for more than a year afterwards (Mimoso, 2013). Wassenaar fails to affect state actors responsible for some of the latest malware components, especially exploits.

Wassenaar’s controls also appear to miss supply side intermediary sales. VUPEN, a French company which sold customised exploits to clients, announced that it would restrict products and sales because of the changes to Wassenaar but although the firm was subsequently removed from the national business registry, the founder and others have gone on to create a new company...
with a similar business model (Granick, 2014). It is not yet clear if any substantive change to the type of malware components being offered or their end use has taken place. In addition, Hacking Team’s surveillance malware has a command and control infrastructure, RCS Console, which meets the definition of supporting technologies for intrusion software (Anderson 2015). However, even after Italy implemented new export rules in line with the Arrangement, the firm experienced only a brief interruption in operation (Internet Association, 2015).

**B. Collateral damage**

Wassenaar’s language poses the risk of considerable collateral damage as it might be most effective in targeting organisations contributing to software security and standard software development practices. A vulnerability can be used for ill, by malicious actors, or for good, to patch and improve software security (Shepherd, 2003). There are a variety of actors searching daily for new vulnerabilities, contributing to what has become an arms race of sorts between these researchers and vendors trying to secure their software. Many vulnerabilities are found and quietly fixed through code review by teams housed within giant software vendors like Google, Microsoft, and Adobe. Smaller security firms, academic groups, and independent security researchers play a crucial role as well. These groups often bring new vulnerabilities to light through independent audits, hacking competitions, and bug bounty programs.

Exploits are not intrinsically malicious and thus have limited effectiveness as a signal of the user’s intent. They have an array of potential uses in the security industry, and are the principle means by which software vendors are made aware of holes in their products that need to be patched. As with restrictions on cryptography, export controls on malware not only struggle to achieve their goal of restricting the flow of malicious tools around the world, but also create challenges to legitimate users and security research. This is especially true under the current wording of technology for the development of intrusion software (Wassenaar Arrangement, 2015).

**FIGURE 1: VULNERABILITY DISCOVERY AND DISCLOSURE**

![Vulnerability Discovery and Disclosure Diagram](image)
Bypassing protective counter-measures, those so effective as to have become commonplace, is a standard part of security research and experimentation, and exactly the manner in which more secure software is developed. This chilling effect of Wassenaar on research could be substantial as ‘nobody can confidently state that he knows how this will be interpreted in practice’ (Dullien, 2015). Figure 1 presents a waterfall diagram showing the potential disclosure path of a vulnerability. The Wassenaar rules do as much (if not more) to disrupt the flow of vulnerability information to the patching process as to the malware market.

The Arrangement’s language also captures too many potential software tools and security processes to be of any use without creating an untenably complex rule with loopholes and endless exceptions. It isn’t that the definition of intrusion software found in the Arrangement will not encompass malware payloads or exploits, but that so much more is swept up at the same time. ‘Modification of a standard execution path…’, for example, could also include patches from a software vendor to improve user’s security, or software plugins like Firefox’s Add-ons, which, ‘interleave externally provided instructions with the main Firefox code logic’ (Bratus et al., 2014). The controls are written in such a blunt manner as to cover quotidian software engineering and security tools, the same sort of broader negative effects on cryptographic tools that began in the 1990s.

C. Challenges to multilateral counter-proliferation

The use of export controls for counter-proliferation of information products has substantial limitations. For both cryptographic tools and malware, one of the key obstacles to successful regulation is that all states party to an agreement must collaborate to prevent regulatory arbitrage. The lack of a standard enforcement mechanism as part of Wassenaar makes this collaboration more unlikely, as different countries may be unable to overcome resistance from domestic constituencies without external inducement (Shehadeh, 1999). Wassenaar also lacks a rule forbidding undercutting, where one state grants export licenses for a product denied by another. There is a provision for notification in these instances, but it does not compel corrective action so a company can choose to export from the most permissive jurisdiction without penalty. While Wassenaar’s membership is still broader than that of CoCom, its predecessor, the Arrangement still excludes a majority of countries including the United States, United Kingdom, Germany, France, Estonia, and Russia (Lipson, 1999). This includes information security hubs like Israel, limiting the effective scope of regulation.

Stepping back from the Arrangement, any successor multilateral approach has to consider reporting requirements for specific controls, licensing activity, and violations. Such an international agreement must also include means of maintaining compliance and must cover all states with current or potential information security research programmes. The difficulty in designing an institution along these lines is substantial. Such an agreement would need to include effective reporting and compliance mechanisms and have as members all states likely to be home to research and commercial activity of interest. Even if such an agreement was in place, the Internet has provided more than enough capability for individuals involved in producing, reselling, or brokering malware components to live and work almost anywhere.
5. A WAY AHEAD

Export controls are likely not the best vehicle to target the malicious software ecosystem. Targeting the transmission of these goods and services across national jurisdictions is a near hopeless task, and imposing strong production and research limitations is just as certain to curtail beneficial security efforts. The clearest indication of a tool’s potential application is in the design of the payload. Security research or penetration testing services do not need to disrupt the integrity of data on target machines or cause physical damage to demonstrate their efficacy. The canonical testing payload initiates the calculator application on target machines, demonstrating the ability to achieve access and execute successfully. Where payloads may be harder to distinguish, the use of large scale propagation methods, such as distribution through a botnet, could also be indicative of a malicious activity (Herr and Rosenzweig, 2015). The exercise of state power over malicious software will continue to be a substantial policy issue, but there are two particular lessons to take from the current debate.

First, what are the goals of using export controls to target malicious software? The discussion around the 2013 changes to Wassenaar have at times embodied human rights concerns while more recently settling on the national security issue (Maurer and Kehl, 2014). The larger discussion of what counter-proliferation looks like in cyber security, or how best to build institutions to facilitate it, has yet to take place. Understanding what the goals of different states are, limiting state to state proliferation or the use of certain tools against particular groups such as political dissidents is one example of an as yet poorly debated trade-off. More can be done to specify goals and match means to those ends.

Second, existing legal tools may be of a limited use when applied to criminal markets and information products. While policymaking is a process of selecting suitable rather than ideal solutions, the gap between these two has grown wide with the debate around malware. Policy practitioners would benefit from a concerted effort to broaden the discussions specific to Wassenaar towards the larger question of how national policy can positively affect efforts to improve citizens’ information security and combat crime. This would be complimented by more systematic engagement with the technical security community and civil society whose insight into the malicious ecosystem can help target policy interventions. A balance of interests is optimal, but some form of state action is inevitable. Continued exchange of common knowledge and language between policymakers and the technical community should not stop with export controls.

An alternative to directly restrict the demand for or use of malware is to target exploits and shrink the supply available for use by states and criminal organisations. In terms of reducing the scale and sophistication of malware, pushing resources and talent towards the goal of finding and patching vulnerabilities would help drive this information to defenders as fast as, or faster than, to those with malicious intent. The community of information security firms and independent researchers responsible for discovering and disclosing a large portion of vulnerabilities every year labour under uncertain legal frameworks that vary between countries. Provisions of the US Digital Millennium Copyright Act (DMCA), for example, can target the analysis of vendor’s
products required to find and prove the existence of bugs, enabling lawsuits to prevent this discovery and discouraging security research (Samuelson, 2001; Adams, 2015). In Belgium, similar laws protecting digital rights management (DRM) systems provide restrictions on the form and content of information that can be disclosed about software systems (Biancuzzi, 2008). A temporary security exemption to the DMCA was passed in 2015, but it will not come into effect for a year (Ellis, 2015). The exception protects the work of researchers looking for vulnerabilities in consumer electronic devices, automobiles, and medical equipment from criminal prosecution under the DMCA.

Changes like the DMCA exception could incentivize greater disclosure to software vendors and would help curtail the supply of vulnerabilities to malicious actions. This emphasis on discovering and patching vulnerabilities would also side-step the tricky question of how to directly restrain state behaviour (like purchasing) in these markets. Vulnerabilities are just information so they can exist in multiple places at once. Aggressively identifying and patching bugs in software is not just a way to secure systems, but a means to limit the lifespan of malware in use by states and non-state actors.

6. CONCLUSION

There are a host of problems with the Wassenaar Arrangement’s application to malicious software. In the larger analysis of counter-proliferation, export controls targeting malware are likely to prove a poor tool. Additionally, understanding the nature of the underlying technology is important in crafting policy but the operation of a system is not deterministic on the manner in which it is regulated. This shortfall, expecting that laws should map directly onto the nature of a software tool or the process of its development and use, has made security researchers’ interaction with the policy process more difficult.

While limited changes to existing law are a positive step, it would be potentially more useful to further revise these protections for research and, importantly, harmonise their application and interpretation across the international community. Vulnerability research is an international enterprise with a bevy of conferences, academic outlets, and competitions taking place across the world. Encouraging security research and growing the pool of individuals looking to discover and disclose vulnerabilities to vendors, would help shrink the pool available to states and criminal groups. Enabling this research through a clear legal framework across states would encourage broader participation and make it easier for vulnerabilities to be disclosed rather than sold on the malicious software market.

The malicious software market is a collection of actors buying, trading, and sometimes stealing from each other. Of the various goods in question, exploits play a key enabling role. However, this level of importance is true of both defensive efforts to engineer secure software and malicious behaviour to compromise it. Exploits are indistinguishable; they do nothing to signal intent. Export controls, as currently constructed in Wassenaar, target these goods as much as any overtly malicious tool. The diversity of demand side actors in this market, and the relatively low
barrier to entry for the supply side make it a difficult environment to restrict with production- or sales-related regulation. Incentivising research could help drain the pool of vulnerabilities for malicious actors.

Wassenaar’s changes targeting malware fail to adequately affect malicious actors, place a harmful burden on security researchers, and expose the limits of multilateral approaches to restrict malware proliferation. Improving the clarity of policy goals on combating crime and enhancing incentives for vulnerability research and disclosure are likely to be more effective than continued application or revision of export controls. The diversity of government, commercial, and civil-society interests in this discussion demands a careful balance, but there remains as yet under-exploited opportunities for crossover engagement and dialogue.

ACKNOWLEDGEMENTS

Thank you to Allan Friedman, Lance Hoffman, Paul Rosenzweig, Katie Moussouris, Eric Armbrust, Tyler Moore, Paulo Shakarian, Ryan Ellis, Andi Wilson, and Jordan McCarthy for their advice and input.

REFERENCES


