REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 7 NÚM. 1 (2018) • PÁGS. 61-78 • DOI 10.5354/0719-2584.2018.48828
RECIBIDO: 29/3/2018 • APROBADO: 9/5/2018 • PUBLICADO: 30/6/2018

DOCTRINA

Control a las exportaciones de cibertecnologías: Un análisis del Arreglo de Wassenaar y sus implicancias para la ciberseguridad

Export control on cybertechnologies: An analysis of the Wassenaar Agreement and its implications for cybersecurity

Camila Hernández Sánchez

Investigadora independiente, Chile

RESUMEN Este artículo busca analizar las diferentes posturas y reacciones que ha generado la incorporación de cibertecnologías a una de las listas de control de exportaciones del Arreglo de Wassenaar. A partir de esto, se pretende reflexionar hasta qué punto es factible y conveniente regular la transferencia de este tipo de tecnologías de la información y, sobre todo, hacerlo a través de un régimen que tiene como objetivo esencial el combate de la proliferación de armas. Es finalmente la diferencia en la naturaleza en los bienes —cibertecnologías contra armas tradicionales—, las características de las definiciones incorporadas y la falta de consenso y normas en torno a la ciberseguridad lo que ha generado oposición a la enmienda y problemas en su implementación.

PALABRAS CLAVE Cibertecnologías, proliferación, control de exportaciones, uso dual, software de intrusión.

ABSTRACT This article seeks to analyze the different positions and reactions emanating from the incorporation of cybertechnologies into the Wassenaar Arrangement list. On that basis, it is intended to reflect to what extent it is feasible and convenient to regulate the transfer of this type of information technology, and especially, perform it through an international regime that has as an essential objective the fight against the proliferation of weapons. It is finally the difference in the nature of goods —cybertechnologies vs. traditional weapons—, the characteristics of the definitions incorporated and the lack of consensus and norms around cybersecurity which has generated opposition to the amendment and problems in its implementation.

KEYWORDS Cybertechnologies, proliferation, export control, dual use, intrusion software.

Introducción

El año 2013, los países miembros del Arreglo de Wassenaar decidieron por consenso incorporar en una de sus listas de control de exportaciones, tecnologías relacionadas a la ciberseguridad, también llamadas cibertecnologías, como ítems sujetos a licencias. Desde ese entonces, ha existido un extenso debate internacional acerca de la utilidad, efectividad y posibles consecuencias negativas que tiene el poner límites a la transferencia internacional de este tipo de herramientas. En tal contexto, este artículo tiene como objetivo analizar las diferentes posiciones y reacciones que ha generado esta inédita incorporación, con la intención de entender hasta qué punto es posible —y deseable— regular este tipo de tecnologías bajo los marcos tradicionales de los regímenes de control de exportaciones.

Para esto, el artículo describirá en primer lugar el concepto de régimen de control de exportaciones, los motivos por los cuales surgen en el sistema internacional y las principales características de los acuerdos que son parte de los esfuerzos para prevenir la proliferación de armas de destrucción masiva. Luego, se expondrá el contexto en que se incluyeron las cibertecnologías en el Arreglo de Wassenaar como productos a controlar por sus países miembros, el detalle de las definiciones incluidas y, en específico, los ítems que en la práctica deberían estar sujetos a licencias o autorizaciones para cruzar una frontera. En tercer lugar, se presentarán las diferentes posiciones y recomendaciones de gobiernos, expertos y empresas en torno al caso, principalmente en relación con los problemas que se han desencadenado a la hora de su implementación y a las consecuencias negativas atribuidas para el sector de la ciberseguridad.

Finalmente, se hará un análisis crítico acerca de la factibilidad, utilidad e implicancias que trae la incorporación de tecnologías de la información a listas centradas tradicionalmente en la no proliferación de armas. Se concluye que la diferencia en la naturaleza de los bienes, la falta de consensos y normativa internacional respecto de la ciberseguridad, sumado al tipo de definiciones que se plasmaron en las listas, son las raíces fundamentales de los obstáculos que se presentan para su implementación.

Regímenes multilaterales de control de exportaciones

El control de las exportaciones se materializa a través de diferentes acciones, ya sea en la restricción de transferencias, impuestos al comercio de productos específicos o la emisión de licencias para exportar, y puede cumplir con objetivos tanto económicos como de seguridad (Bonarriva, Koscielski y Wilson, 2009: 3). En el contexto de este análisis, el concepto de «control de exportaciones» se definirá como las iniciativas y legislación de los gobiernos para regular la transferencia o comercio internacional de ciertos productos militares y artículos, los cuales se puedan usar para producir o entregar armas de destrucción masiva y sus elementos relacionados, a través de listas

de control y el otorgamiento de licencias (Beck y otros, 2002: 5; Pyetranker, 2015: 158). Es así como una autoridad de gobierno es la encargada de revisar, aprobar y denegar la exportación de los bienes que el país ha decidido controlar.[1]

La existencia de los sistemas de control se relaciona con el hecho de que una gran variedad de bienes, tecnologías y materias primas necesarias para fabricar armas de destrucción masiva y sus medios de distribución tienen aplicaciones legítimas en otras áreas. En la literatura este tipo de productos son conocidos como bienes de «doble uso» o «uso dual», los cuales pueden ser utilizados tanto para propósitos civiles como militares o de armas de destrucción masiva (Fuhrmann, 2008: 633).

Un ejemplo simple e ilustrativo de este tipo de productos es el «transductor de presión», elemento que convierte presión en señal eléctrica analógica. Su uso industrial se observa en sistemas de calefacción, refrigeración o ventilación. Por su parte, su uso relacionado con las armas de destrucción masiva consiste en la medición de presión de gas dentro de las centrifugadoras en cascadas para enriquecer uranio. Existe evidencia de que países como Irán y Pakistán utilizan una gran cantidad de transductores en sus plantas nucleares que han podido adquirir en el mercado internacional, a pesar de que su comercialización esté controlada por muchos países.[2]

Es así como, mientras la capacidad para producir este tipo de armas y programas estuvo concentrada en un inicio en las manos de un selecto grupo de países, el fenómeno de la globalización y la dinámica del sistema financiero internacional han llevado a la emergencia de innumerables proveedores secundarios. Actualmente, la mayoría de los elementos que un país o actor no estatal necesita para estos fines se encuentran disponibles y pueden ser adquiridos en los mercados internacionales.

En esta línea, la regulación del comercio de estos bienes es parte de los esfuerzos internacionales para combatir la proliferación de armas de destrucción masiva. Este fenómeno ha sido descrito en la literatura como la propagación de armas o tecnologías relacionadas desde entidades o Estados hacia otros Estados o actores no estatales, la llamada «proliferación horizontal». Por su parte, la «proliferación vertical» se puede observar cuando Estados poseedores de armas de destrucción masiva aumentan cuantitativamente sus arsenales, realizan mejoras cualitativas en las tecnologías o desarrollan nuevas armas (Sidel y Levy, 2007: 1.589). A pesar de que los sistemas de control intentan afectar el fenómeno como un todo, se vincula de mayor manera cuando las transferencias son horizontales.

A través de los años, este tipo de controles al comercio se ha ido estructurando

1. Tim Maurer, «Exporting the right to privacy», *Slate*, 15 de mayo de 2017, disponible en https://slate.me/2xPouX5.

2. David Albright y Andrea Stricker, «Case study: Chinese salesman arrested in pressure transducer case», Institute for Science and International Security, 18 de agosto de 2013, disponible en http://bit.ly/2xShUPp.

y enmarcando a nivel internacional a través de regímenes como acuerdos multilaterales informales y voluntarios entre Estados, los cuales aplican controles a bienes estratégicos a partir de normativa común no vinculante. Actualmente existen cinco cuerpos de este tipo a nivel global, cada uno con su foco de control y alcance en particular. Nacen como un complemento a los tratados internacionales más importantes en la materia, como por ejemplo el Tratado de No Proliferación Nuclear, la Convención sobre las Armas Químicas y la Convención sobre Armas Biológicas y Toxínicas.

Asimismo, cabe destacar que el propósito de estos regímenes ha sido potenciado por la Resolución 1.540 (2004) del Consejo de Seguridad de Naciones Unidas. Esta norma, que tiene como objetivo principal prevenir «la proliferación en todos sus aspectos de todas las armas de destrucción masiva» y que está principalmente enfocada en impedir que agentes no estatales puedan adquirirlas, es obligatoria y vinculante para todos los Estados miembros de la organización. Específicamente, la Resolución obliga a los Estados a «establecer, desarrollar, evaluar y mantener controles nacionales apropiados y eficaces de la exportación y el transbordo» de bienes sensibles a través de la implementación de legislación y reglamentos, para lo cual reconoce la «utilidad de las listas de control», que han sido elaboradas por los regímenes multilaterales de control. La Resolución 1.540 es vista como un esfuerzo claro por definir, formalizar y resolver la no universalidad de los distintos instrumentos para combatir la proliferación, pues pone su foco en la amenaza que significa para la seguridad internacional que este tipo de armas lleguen a las manos de actores no estatales (Crail, 2006: 355; Heupel, 2007: 1; Kraig, 2009: 24; Stinnett y otros, 2011: 310).

Por lo tanto, el establecimiento de sistemas de control y las reglas acordadas voluntariamente en los regímenes son una herramienta para cumplir con una obligación internacional. En primer lugar, el Comité Zangger (1971) —el más antiguo de los regímenes— tiene como propósito armonizar la política de exportación de los países miembros del Tratado de No Proliferación, con un enfoque en el artículo 3.2 de dicho acuerdo, el cual compromete a los Estados parte a no exportar material nuclear y equipos que sirvan para la producción de armas. Para esto, el Comité posee una lista de productos relacionados con la energía nuclear que requieren de salvaguardias y licencias para ser vendidos. Su sitio web es http://zanggercommittee.org/.

También relacionado con la energía nuclear, el Grupo de Suministradores Nucleares (1975) surge en parte como respuesta a la explosión nuclear ocurrida en India en 1974, que mostró la necesidad de medidas adicionales para combatir la proliferación (Hibbs, 2011: 5). El Grupo estableció una lista de control de bienes diseñados específicamente para aplicaciones nucleares y materiales, como centrífugas, y otra compuesta por bienes de uso dual que pueden ser usados en la producción energía nuclear. Su sitio web es http://nuclearsuppliersgroup.org/.

En tercer lugar, el Grupo Australia (1985) es una alianza de países que tienen como objetivo luchar contra la proliferación de armas químicas y biológicas a través del

control de exportaciones de las sustancias y agentes sensibles, distribuido en cinco diferentes listas. Su sitio web es http://australiagroup.net/.

Respecto de los medios de distribución de armas de destrucción masiva, se constituyó el Régimen de Control de Tecnología de Misiles (1987) con el objetivo de contener la proliferación de misiles balísticos. Incluye una serie de acuerdos voluntarios para coordinar las autorizaciones de los países miembros sobre la exportación de misiles, componentes para vehículos no tripulados y otras tecnologías relacionadas. Al igual que el resto de los regímenes multilaterales de control de exportaciones, se basa en pautas comunes y una lista, de la cual cada Estado es responsable de implementar de acuerdo con la legislación nacional. Su sitio web es http://mtcr.info/.

Finalmente, el Arreglo de Wassenaar (1996) tiene su foco en el control de exportaciones de armas convencionales, bienes y tecnologías de doble uso. Actualmente está compuesto por 42 Estados miembros, y su objetivo principal es promover la transparencia y la responsabilidad en la transferencia de estos productos estratégicos, para que no se generen «acumulaciones desestabilizadoras» o que lleguen a actores no estatales (Hirschhorn, 2010: 456). La membresía es universal para todos los Estados que cumplan con los siguientes criterios: i) ser productor o exportador de armas o bienes de doblen uso y tecnología relacionada; ii) implementar políticas nacionales que no permitan la venta de armas o bienes de doble uso a países o entidades que sean un riesgo para la seguridad internacional; iii) tener un compromiso efectivo con las normas internacionales de no proliferación; y iv) tener un completo funcionamiento de estructuras de control de exportaciones. Al adherir al acuerdo, los países aceptan intercambiar información sobre las transferencias realizadas, como reportes de las denegaciones de licencias efectuadas.

Para cumplir con sus objetivos, el Arreglo de Wassenaar posee dos listas de control: una lista de municiones de 22 categorías, las cuales cubren bienes como armas pequeñas y ligeras, tanques y vehículos blindados, materiales explosivos, embarcaciones marinas, vehículos aéreos, entre otros (Ramírez Morán, 2016: 2); por otro lado, está la lista de materiales y tecnologías de uso dual, la cual se divide en nueve categorías:[3]

- Categoría 1: Materiales especiales y equipamiento relacionado.
- Categoría 2: Materiales de procesamiento.
- Categoría 3: Electrónicos.
- Categoría 4: Computadoras.
- Categoría 5 (parte 1): Telecomunicaciones.

3. Secretaría del Arreglo de Wassenaar, «List of dual-use goods and technologies and munitions list», 2017, disponible en https://www.wassenaar.org/control-lists/.

- Categoría 5 (parte 2): Seguridad de la información.
- Categoría 6: Sensores y láseres.
- Categoría 7: Navegación y aviónica.
- Categoría 8: Marina.
- Categoría 9: Aeroespacial y propulsión.

Adicionalmente, cada una de estas categorías se subdivide en cinco tipos:

- Sistemas, equipos y componentes.
- Equipos de prueba, inspección y producción.
- Materiales.
- Software.
- Tecnología.

En definitiva, los regímenes de control de exportaciones complementan y potencian un sistema mundial que intenta prevenir que se proliferen las armas. Específicamente, el Arreglo de Wassenaar es clave a la hora de controlar los componentes y materiales que podrían ser parte, por ejemplo, de un programa nuclear.

Arreglo de Wassenaar y la ciberseguridad

Las listas de control del Arreglo de Wassenaar antes mencionadas (bienes de uso dual y municiones) no son estáticas y pueden ser modificadas por consenso de sus miembros, con el fin de que el régimen se encuentre actualizado con las nuevas tecnologías y dinámicas de la proliferación. Sin embargo, aunque la revisión periódica de las listas fue acordada desde el inicio, la toma de decisiones se hace cada vez más difícil a medida que crece el número de Estados parte (Pyetranker, 2015: 161). De esta forma, en la reunión plenaria del año 2013, los representantes de los gobiernos de Francia y Reino Unido propusieron incorporar herramientas relacionadas con la ciberseguridad a una de las listas, lo cual fue ratificado por los miembros (Dullien, Iozzo y Tam, 2015: 3).

La razón esgrimida para esta incorporación fue restringir su acceso a regímenes autoritarios y represivos que pudieran utilizar este tipo de tecnologías para cometer abusos a los derechos humanos. La Primavera Árabe de 2011 —fenómeno que llevó a la desintegración de gobiernos y contribuyó a la movilización sociopolítica de otros— demostró el impacto de la tecnología en los derechos humanos desde dos perspectivas: por un lado, ciudadanos del Norte de África y Medio Oriente utilizaron este tipo de herramientas —principalmente redes sociales— como método de visualización de la violación de sus derechos fundamentales y para organizar y movilizar

a las masas.[4] Tal como sugiere Mohammad-Munir Adi (2013: 11), la mayor conectividad a internet y el surgimiento de plataformas como Facebook, Twitter y Youtube contribuyeron al uso y masificación de las herramientas digitales como medio de organización política.

Por su parte, la vinculación directa entre este fenómeno político en los países árabes y la enmienda del Arreglo de Wassenaar se relaciona con la revelación de que gobiernos como Egipto, Baréin o Siria habían utilizado estas herramientas para monitorear y posteriormente perseguir activistas de derechos humanos, disidentes y oponentes políticos (Bohnenberger, 2017: 83; Bronowicka y Wagner, 2015: 154-155). Debido a esto, se intentó restringir las exportaciones de empresas como Hacking Team y Gamma Group, que vendieron herramientas de vigilancia a estos Estados (Herr, 2016: 176).

En particular, el Gobierno de Reino Unido estaba preocupado por la transferencia de la tecnología de intrusión Finfisher, un tipo de software de vigilancia «espía» desarrollado por Gamma Group, de capitales británicos y alemanes. En tanto, Francia centró su preocupación en el comercio de sistemas de vigilancia IP, después de que se encontró evidencia de que la empresa Amesys suministró herramientas de monitoreo al régimen de Muammar Gaddafi en Libia (Bohnenberger, 2017: 84). De hecho, el Gobierno francés fue el primero de los socios de Wassenaar en implementar las nuevas restricciones. Además de lo anterior, de acuerdo con Wagner (2012: 5-11), existe evidencia de que compañías con base en Alemania, Dinamarca, Finlandia, Irlanda, Italia y Suecia desarrollaron tecnologías de vigilancia utilizadas en países con regímenes represivos.

En este contexto, se tomó la decisión de incorporar cierto tipo de tecnologías de información que según la declaración oficial del Arreglo de Wassenaar, «bajo ciertas condiciones, pueden ser perjudiciales para la seguridad y estabilidad regional e internacional».[5] Tal como sugieren Dullien, Iozzo y Tam (2015: 3), la enmienda se considera inédita, ya que el acuerdo «nunca fue concebido como un instrumento de mitigación para temas de derechos humanos». Específicamente, las cibertecnologías que se incluyeron en la lista de control de bienes de uso dual fueron «software de intrusión» en la categoría 4 y «tecnologías de vigilancia de comunicación IP» en la categoría 5.

En primer lugar, «software de intrusión» se refiere a las herramientas diseñadas para evadir defensas, ganar acceso y extraer información. Es importante destacar

4. Ekaterina Stepanova, «The role of information communication technologies in the Arab Spring: Implications beyond the region», PONARS Eurasia, disponible en http://bit.ly/2kWa1iH.

5. Secretaría del Arreglo de Wassenaar, «Public statement 2013 plenary meeting of the Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies», 2013, disponible en http://bit.ly/2HHkCqt.

que la lista no controla los bienes en sí, sino que la infraestructura de soporte usada para generar, desplegarse o comunicarse con este software de intrusión. La definición desarrollada en la lista de control el año 2013 es la siguiente:[6]

> «Software» especialmente diseñado o modificado para evitar la detección por «herramientas» de monitorización, o para vencer las «contramedidas protectoras» de un ordenador o un dispositivo con capacidad de interconexión en red, y que realice algo de los siguientes: 1) la extracción de datos o información de un ordenador o dispositivo con capacidad de interconexión en red, o la modificación del sistema de datos de usuario; o 2) la modificación del flujo de ejecución estándar de un programa o proceso con objeto de permitir la ejecución de instrucciones proporcionadas desde el exterior. […] Notas: 1) «software de intrusión» no incluye ninguno de los siguientes elementos: 1.1) hipervisores, depuradores o herramientas de ingeniería inversa de software (SER); 1.2) software de gestión digital de derechos (DRM); o 1.3) software diseñado para ser instalado por los fabricantes, administradores o usuarios con propósito de seguimiento de activos o recuperación. 2) Dispositivos con capacidad de interconexión en red incluye dispositivos móviles y contadores inteligentes. […] Notas técnicas: 1) «Herramientas de monitorización»: dispositivos software o hardware que monitorizan el comportamiento del sistema o los procesos ejecutándose en un dispositivo. Esto incluye productos antivirus (AV), productos de seguridad de punto final, productos de seguridad personal (PSP), sistemas de detección de intrusos (IDS), sistemas de prevención de intrusión (IPS) o *firewalls*. 2) «Contramedidas protectoras»: Técnicas diseñadas para asegurar la ejecución segura de código, como prevención de ejecución de datos (DEP), aleatorización de la distribución del espacio de direcciones (ASLR) o cajones de arena (*sandboxing*).[7]

Las anteriores definiciones, excepciones y detalles técnicos son la base y lo que delimita los bienes a controlar, los cuales en el caso del software de intrusión son los siguientes tres ítems:

> 4.A.5) Sistemas, equipos y componentes para ellos especialmente diseñados o modificados para la generación, el funcionamiento o la emisión de, o para la comunicación con, programas informáticos de intrusión. […] 4.D.4) Software especialmente diseñados o modificados para la generación, el funcionamiento o la emisión de, o para la comunicación con, software de intrusión. […] 4.E.1.c) Tecnología para el desarrollo de software de intrusión.[8]

6. Se utiliza la traducción oficial de la Unión Europea, ya que las listas solo se encuentran disponibles en inglés.

7. Secretaría del Arreglo de Wassenaar, «List of dual-use goods and technologies and munitions list», 2013, p. 209, disponible en http://bit.ly/2l15ADk.

8. Secretaría del Arreglo de Wassenaar, «List of dual-use goods», 2013, pp. 73-74.

Por su parte, las «tecnologías de vigilancia de comunicación IP» son entendidas como herramientas para la recolección y análisis de grandes volúmenes de redes (Herr, 2016: 176). En la versión de 2013, esta tecnología se incluye como:

> 5.A.1.j) Sistemas o equipos de vigilancia de las comunicaciones en red a través del protocolo de internet (IP) y componentes diseñados especialmente para ellos, que posean todas las características siguientes: 1) que realicen todas las siguientes funciones en red a través del protocolo de internet (IP) de clase portadora (por ejemplo, el eje troncal IP de grado nacional); análisis en la capa de aplicación (por ejemplo, capa 7 del modelo de interconexión de sistemas abiertos, ISO/IEC 7498-1); extracción de contenido de la aplicación y metadatos seleccionados (por ejemplo, voz, vídeo, mensajes, ficheros adjuntos), e indexación de los datos extraídos. 2) Diseñados especialmente para realizar cualquiera de las funciones siguientes: ejecución de búsquedas sobre la base de selectores rígidos, y cartografía de la red relacional de una persona o de un grupo de personas. […] Nota: el subartículo 5A001.j no somete a control los equipos y sistemas diseñados especialmente para cualquiera de las funciones siguientes: a) fines de comercialización, b) calidad del servicio, o c) calidad de la experiencia.[9]

Con la inclusión de estos artículos en la lista de bienes de uso dual, el Arreglo entra en acción respecto a la ciberseguridad. Con una amenaza cibernética inminente en el horizonte y ninguna agencia u organismo internacional con el mandato para lidiar con el tema, es finalmente un acuerdo sobre armas, el que se involucra en su control y gestión de transferencias (Pyetranker, 2015: 162).

Reacción internacional

La incorporación de estas tecnologías en la lista de control del Arreglo de Wassenaar ha generado un extenso debate a nivel político, académico y comercial. Las principales críticas que se han esgrimido tienen que ver con la generalidad de los conceptos utilizados, lo cual arrastra dos tipos de problemas: trabas a la implementación de las medidas en los Estados miembros y consecuencias negativas para la dinámica, desarrollo e intercambio de información en el sector de la ciberseguridad.

No obstante, es pertinente destacar que el flanco de críticas ha sido principalmente sobre el ítem «software de intrusión», definición que ha sido considerada muy amplia y ambigua. Por el contrario, la descripción de tecnologías de vigilancia de comunicación IP se caracteriza por su «especificidad técnica», la cual deja poco espacio para la interpretación, pues está definida de forma más precisa mediante métricas cuantitativas de rendimiento.[10] Adicionalmente, la mayor controversia en relación a

9. Secretaría del Arreglo de Wassenaar, «List of dual-use goods», 2013, p. 81.

10. Access, Center for Democracy and Technology, Collin Anderson, Electronic Frontier Foundation,

software tiene que ver con la manera en que ha sido incorporado a la lista través de una estructura de «dos niveles» separando la definición de los ítems que efectivamente los Estados deben controlar (Bohnenberger, 2017: 85).

A pesar de que desde el inicio ha existido polémica en torno a la enmienda, el tema alcanzó atención internacional en 2015, cuando la multinacional Hewlett-Packard y su iniciativa Zero Day —que buscaba reportar vulnerabilidades «día cero» a los responsables de las marcas afectadas— canceló su asistencia y patrocinio al congreso sobre ciberseguridad Pwn2Own con sede en Japón. Esto se debió a que la empresa no quería correr el riesgo de cruzar una frontera con un *exploit* (demostración de la posibilidad de explotar una vulnerabilidad) y menos ingresar a Japón, país que había implementado las disposiciones del Arreglo de Wassenaar (Flynn y Fletcher, 2016: 6; Ramírez Morán, 2016: 5). De acuerdo con la declaración de Jewel Timpe —encargada del área de investigación de amenazas de la compañía—, la razón por la cual se tomó la decisión de retirarse del congreso fue «la dificultad de manejar, definir y obtener las licencias requeridas en el tiempo que exige el concurso» y la «ausencia de un camino claro para hacerlo de manera fácil y rápida» (McGuire, 2016: 9). En definitiva, fue el resultado tanto de la ambigüedad atribuida a las disposiciones del Arreglo de Wassenaar, como a la libertad que poseen los Estados miembros a la hora de implementar el acuerdo. En contraste a lo ocurrido en Japón, ese mismo año HP patrocinó una competencia Pwn2Own en la conferencia CanSecWest en Vancouver, ya que la implementación de las normas en Canadá es «mucho más clara y simple de cumplir».[11]

En este contexto, las mencionadas debilidades en las definiciones han acarreado indiscutiblemente problemas en la implementación nacional de las listas de control. Al ser los ítems por controlar muy interpretables y amplios en su definición, los países han aplicado de forma diferente sus disposiciones, e incluso hay casos en que Estados miembros no han incluido las cibertecnologías en su regulación nacional. En el caso de Estados Unidos, las disposiciones no han sido implementadas hasta la fecha, debido a la oposición que ha generado en la comunidad de ciberseguridad y en sectores del Gobierno. En una reciente carta enviada por miembros del Congreso al exasesor de Seguridad Nacional, Michael Flynn, se pide renegociar el acuerdo debido a que afecta «la postura de ciberseguridad de la nación y la competitividad económica».[12]

Human Rights Watch y New America's Open Technology Institute, «Comments to the US Department of Commerce on implementation of 2013 Wassenaar Arrangement plenary agreements», Center for Democracy and Technology, 20 de julio de 2015, RIN 0694-AG49, p. 9, disponible en http://bit.ly/2Jz3NTH.

11. Dan Goodin, «Pwn2Own loses HP as its sponsor amid new cyberweapon restrictions», *Ars Technica*, 3 de septiembre de 2015, disponible en http://bit.ly/2sPfCLd.

12. «BSA applauds bipartisan House letter urging Trump Admin to renegotiate the Wassenaar Arrangement», BSA The Software Alliance, 10 de febrero de 2017, disponible en http://bit.ly/2Mi5F1R.

Asimismo, los problemas de implementación pueden ser contraproducentes para los objetivos de protección de derechos humanos que tiene la iniciativa. En el caso de Italia, Cheri McGuire, vicepresidente de Symantec Corporation, argumenta que su implementación ha sido esencialmente de nombre, con pocos o casi ningún mecanismo de aplicación (McGuire, 2016: 10). Esto se debe a que en 2015 autoridades italianas le otorgaron una «licencia global» a la firma Hacking Team, lo que les permite exportar sus productos (controlados) a países de riesgo, lo cual es precisamente lo que trata de prevenir el Arreglo de Wassenaar. Esta compañía tiene como modelo de negocio vender capacidades de intrusión ofensiva y de vigilancia, los cuales, como se mencionó, han sido utilizados para la violación de derechos fundamentales de ciudadanos en diferentes países del mundo. Cabe destacar que la autorización global para exportar fue revocada en 2016, después de una gran presión local e internacional (Flynn y Fletcher, 2016: 6).

Por otro lado, además de las críticas relacionadas con la escasa aplicabilidad de las normas, se encuentran las que apuntan a los posibles daños colaterales y consecuencias negativas que significa restringir el comercio de este tipo de herramientas cibernéticas cuando uno de los elementos centrales para el desarrollo del sector se relaciona con compartir información. El problema radica en que la definición aplica a casi todo el universo de herramientas de ciberseguridad, lo que incluye bienes que son necesarios para la misma seguridad de los Estados y empresas, así como para la investigación en torno a vulnerabilidades (Anderson, 2015: 13; Bohnenberger, 2017: 86). Como sugiere Dullien, Iozzo y Tam (2015: 4), habría dos caminos a seguir por los países miembros del acuerdo para prevenir las atribuidas consecuencias negativas que se desprenden de su implementación. Una alternativa es a través de una serie de excepciones y exclusiones que dejan prácticamente nulo el alcance de las medidas. La otra vía es a través de estándares de licencias excesivamente generosos, que finalmente no tienen impacto significativo en las transferencias comerciales de infraestructura de vigilancia, como se observó en el caso italiano.

Respecto a las especificaciones técnicas de la definición de «software de intrusión», concretamente la que se refiere a «la modificación del flujo de ejecución estándar de un programa o proceso con objeto de permitir la ejecución de instrucciones proporcionadas desde el exterior», se argumenta que es una característica común de muchas técnicas de ingeniería de software. Lejos de ser una característica única de un *malware* u otro sistema ofensivo, las mismas técnicas son utilizadas en software de administración remota, antivirus, en el monitoreo de las empresas y diferentes sistemas operativos. Por ejemplo, de acuerdo con Bratus y otros (2014: 2), el problema de imprecisión es tal que el popular software Detours de Microsoft —programa informático e instrumento clave en la industria para parches de seguridad, monitoreo y depuración de software— podría entrar en los parámetros establecidos por Wassenaar. Igualmente, las industrias, particularmente las que tienen como modelo

de negocio la comercialización de vulnerabilidades que no se han hecho públicas (día cero), ven alterado su funcionamiento en los países que han implementado las enmiendas del Arreglo de Wassenaar.

Desde el punto de vista de Ramírez Morán (2016: 6), la negativa internacional hacia la enmienda también se relaciona con los posibles efectos en «la investigación y la aplicación profesional de la ciberseguridad». La comunicación de los denominados *responsable disclosure*, los cuales informan sobre las vulnerabilidades o fallas al proveedor o fabricante, podría verse afectada. Cuando la entidad o la persona que descubre el problema se encuentre en un país distinto al del fabricante y desee comunicar la vulnerabilidad, deberá solicitar una autorización, ya que se consideraría como una exportación de un *exploit*. De la misma forma, las pruebas de intrusión de los sistemas que realizan profesionales a las compañías entrarían en la definición de software de intrusión, por lo que «si cruzan las fronteras con estas aplicaciones instaladas […] estarían incurriendo en tráfico ilegal de material de doble uso» (Ramírez Morán, 2016: 6).

En cuanto a los cambios que se deberían realizar a la lista de control, algunos abogan por una completa eliminación de las disposiciones relacionadas con ciberseguridad, mientras que otros por reformar las definiciones y especificaciones técnicas. A nivel europeo, el Parlamento y la Comisión Europea han defendido la idea de crear un mecanismo independiente que controle tecnologías de vigilancia cibernética (Bohnenberger, 2017: 89, 92). Otras reformas propuestas tienen que ver con aumentar las excepciones dispuestas en los ítems bajo control o centrar las definiciones en las características técnicas que sean capaces de convertir los software en programas verdaderamente dañinos. Por ejemplo, Herr y Rosenzweig (2015: 5, 8, 10-11) proponen basar el control en el componente *payload* de los sistemas, pues afirman que aquéllos incapaces de generar daño físico o digital deberían estar exentos de control. Por su parte, otros proponen que se deberían delimitar los controles a los sistemas que tengan capacidad de exfiltración de datos de un equipo sin la autorización o conocimiento del dueño o administrador (Bohnenberger, 2017: 86-87; Dullien, Iozzo y Tam, 2015: 7-9).

La contundente oposición internacional al contenido de la enmienda, debido a la incorporación de cibertecnologías a las listas de control, ha tenido resultados. En el plenario de diciembre de 2017 se discutió el lenguaje y especificaciones del ítem «software de intrusión», lo que llevó a que se reformularan algunos de los bienes a controlar, específicamente 4.D.4 y 4.E.1.c. Estas nuevas reglas crean excepciones para los individuos que participan en la coordinación internacional sobre vulnerabilidades de seguridad, y se definen de forma más clara los mecanismos de actualización de software, que no se relacionen con intrusión a los sistemas.[13]

13. Tom Cross, «New changes to Wassenaar Arrangement export controls will benefit cybersecurity», *Forbes*, Community Voice, 16 de enero de 2018, disponible en http://bit.ly/2xOX97j.

En detalle, los cambios incorporados fueron:

> 4.D.4 […] Nota: 4.D.4 no se aplica a software especialmente diseñado y limitado para proporcionar actualizaciones o mejoras que cumplan con lo siguiente: a) La actualización o mejora opera solo con la autorización del propietario o administrador del sistema que la recibe; y b) Después de la actualización o mejora, el software actualizado o mejorado no es ninguno de los siguientes: 1) software especificado por 4.D.4; 2) software de intrusión.
>
> 4.E.1.c […] Nota 1: 4.E.1.a. y 4.E.1.c. no aplica para divulgación de vulnerabilidad o respuesta a incidente cibernético. […] Nota 2: Nota 1 no disminuye el derecho de las autoridades nacionales para determinar el cumplimiento de 4.E.1.a. y 4.E.1.c […] Nota técnica: «Divulgación de vulnerabilidad» significa el proceso de identificación, notificación o comunicación de vulnerabilidad, o el análisis de una vulnerabilidad con individuos u organizaciones responsables de realizar o coordinar la remediación con el fin de resolver la vulnerabilidad. […] «Respuesta a incidentes cibernéticos» significa el proceso de intercambio de información necesaria sobre incidentes de seguridad cibernética con personas u organizaciones responsables de realizar o coordinar la remediación para abordar el incidente de ciberseguridad.[14]

La nueva lista de control del Arreglo de Wassenaar mejora el control de cibertecnologías eliminando algunos de los obstáculos que las regulaciones interponían a la industria en su colaboración con la lucha contras las amenazas de seguridad de la información. Fue principalmente gracias a la presión impuesta por las compañías afectadas y a la delegación de Estados Unidos presente en el plenario, quienes fueron asesorados técnicamente por expertos en la materia.[15] A pesar de no ser perfectos, estos cambios pueden ser considerados una pequeña victoria para sus opositores.

¿Es posible (y deseable) controlar este tipo de tecnologías?

Además de entender la oposición que ha generado el control a la exportación de cibertecnologías, es fundamental plantearse la interrogante sobre la factibilidad de regularlas. En otras palabras, es pertinente analizar la viabilidad y, sobre todo, la conveniencia de aplicar este tipo de normas a tecnologías de la información; bienes que finalmente son y se desenvuelven de forma diferente que los controlados tradicionalmente por los regímenes de control de exportaciones. Es así como, más allá de los problemas ya mencionados respecto de la implementación y las consecuencias negativas atribuidas a la hora de incorporar las normas establecidas por el Arreglo de Wassenaar, se puede afirmar que hay cuatro argumentos que permiten vislumbrar la dificultad a la hora del control.

14. Secretaría del Arreglo de Wassenaar, «List of dual-use goods», 2017, pp. 78-79.
15. Tom Cross, «New changes to Wassenaar».

En primer lugar, los bienes controlados tradicionalmente por el Arreglo de Wassenaar son de naturaleza distinta a los incluidos en el año 2013. Las cibertecnologías se caracterizan por ser bienes intangibles, es decir, productos inmateriales que no pueden ser apreciados por los sentidos (Rodríguez, 2014: 21). A esto se suma el cómo estas tecnologías interactúan con el sistema económico globalizado, lo cual se escapa de los procesos tradicionales de exportación (Pyetranker, 2015: 173-178).[16] El desafío está en controlar bienes intangibles que se transfieren de un lugar a otro también de manera intangible. Los regímenes están conceptualizados en un sistema económico y político tradicional basado en fronteras, a diferencia de la dinámica de la tecnología de información, en la cual la única condición para su transferencia es una conexión a internet. En esta línea, académicos como Herr (2016: 176) sugieren que el enfoque del control de exportaciones presenta una serie de limitaciones a la hora de desenvolverse con herramientas de ciberseguridad debido a la estructura del mercado, lo cual hace que el impacto en el control de la actividad maliciosa, que es lo que pretende prevenir Wassenaar, sea mínimo.

La naturaleza intangible de las cibertecnologías, tanto en el bien a controlar como en la forma en que se exporta, puede generar que ciertas compañías que producen ítems que serían controlados por el acuerdo simplemente se muevan a otra jurisdicción para evadir las restricciones a sus transferencias. De hecho, de acuerdo con el informe de McGuire (2016: 10), el Grupo Gamma, propietario de Finfisher, ha abierto nuevas filiales y cerrado otras, en parte debido a los controles impuestos por los países miembros de Wassenaar. Incluso, según el reporte, el estatus legal del producto Finfisher pareciera estar en manos de una entidad completamente separada a la de Gamma.

En segundo lugar, el enfoque tradicional del Arreglo de Wassenaar es la prevención de la proliferación de armas convencionales y de destrucción masiva, al cual los países adhieren de forma voluntaria creando directrices y normativas comunes para asegurar que sus exportaciones no contribuyan a este propósito. En este caso, el objetivo de la incorporación de las nuevas herramientas tiene relación con la protección de los derechos humanos, al controlar tecnología relacionada con la ciberseguridad, concepto del cual no existe consenso internacional (Álvarez y Vera, 2017: 43). En definitiva, se está desarrollando un marco operacional para prevenir que este tipo de tecnología cause algún daño, sin tener ninguna definición de trabajo de ciberarma (Herr y Rosenzweig, 2015: 301-302). Esta realidad genera muchos problemas y limitaciones en un régimen multilateral que funciona a partir del consenso de sus miembros.

En tercer lugar, la definición amplia de software de intrusión ha impuesto aún más obstáculos. Se comete el error de «equiparar las técnicas incorporadas en el software con solo uno de sus usos potenciales», los que genera una serie de consecuencias

16. «Review of dual-use export controls», Parlamento Europeo, Think Thank, 12 de enero de 2018, disponible en http://bit.ly/2HDCylO.

negativas (Bratus y otros, 2014: 3). Asimismo, la falta de tecnicismo y precisión demuestra la necesidad de que el mundo político y el técnico conversen y cooperen para armar normativa internacional que sea específica, aplicable y realmente efectiva (Herr y Rosenzweig, 2015: 319). Este caso demuestra fielmente la dificultad de definir y crear normativa por parte de actores internacionales con diferentes intereses y enfoques sobre ciberseguridad (Ramírez Morán, 2016: 7).

Finalmente, existe un argumento histórico en la literatura que tiene que ver con la dificultad de controlar este tipo de tecnologías. La enmienda del 2013 a la lista de control de Wassenaar no es el primer intento de controlar el flujo de cibertecnologías, pues a finales de la década del noventa, Estados Unidos patrocinó a través del Arreglo de Wassenaar la restricción de exportación de tecnología de cifrado, lo que desencadenó que en 1998 se incorporara a la lista de uso dual el ítem «software de cifrado» con claves numéricas de más de 64 bits de longitud. Sin embargo, poco tiempo después que el plenario de países miembros ratificara la enmienda, el consenso comenzó a romperse y la incorporación a la legislación nacional de los países fue casi nula. Por ejemplo, Francia decidió eliminar los controles al software de hasta 128 bits. Alemania y Finlandia, por su parte, a la hora de la implementación de las restricciones decidieron eliminar cualquier control de tecnología de cifrado. Asimismo, debido a la expansión del uso de internet, los controles de exportación a programas informáticos de cifrado perdieron todo su efecto. En pocas palabras, las consecuencias negativas que traía el control de este tipo de tecnologías que tienen un uso legítimo, y la dificultad de controlar su transferencia internacional en la práctica, forman parte del argumento que respalda que la actual «ciberenmienda» también será un fracaso (Pyetranker, 2015: 165-166).

Conclusiones

En definitiva, la base del debate y las críticas hacia la incorporación de cibertecnologías se relaciona con sus posibles consecuencias negativas para la ingeniería de herramientas de seguridad y para la investigación de vulnerabilidades, industrias que se caracterizan por una dinámica cooperación transfronteriza. El problema radica en que el Arreglo de Wassenaar actualmente intenta normar sobre un tema en el que no tiene experiencia previa, al incorporar bienes de distinta naturaleza en una misma lista de control, y respecto del cual no existe normativa comúnmente establecida, como es la ciberseguridad, ya sea por falta de voluntad política o consenso.

En este sentido, es un desafío importante abordar los temas de derechos humanos y lograr un equilibrio sin afectar negativamente el desarrollo del sector. Sin embargo, lo que se considera realmente significativo de este debate es entender que la ciberseguridad es un desafío en sí misma. Para que este tipo de controles sean efectivos, además de corregir las definiciones pertinentes, deben ser complementados con ini-

ciativas de política interior y exterior que incorporen la seguridad de la información como elemento clave.

Es también pertinente considerar la importancia que tiene esta discusión para nuestro país, ya que se solicitó el ingreso al Arreglo de Wassenaar en enero de 2015. La futura adherencia al acuerdo multilateral depende de que se formule en Chile la legislación adecuada para crear un sistema integral de control de exportaciones.[17] El requerimiento se enmarca dentro de los objetivos que tenemos como Estado de cumplir con los estándares internacionales en la materia, la necesidad de que los bienes que se exportan desde el territorio nacional tengan un uso y usuario final seguro, y con la implementación de las obligaciones que nos impone la Resolución 1.540. Por lo tanto, los problemas que ha generado la inclusión de cibertecnologías en la lista de Wassenaar no son vistos como un obstáculo para que Chile perfeccione y fortalezca su sistema de comercio estratégico.

En conclusión, tanto los beneficios que ha traído el Arreglo de Wassenaar en torno a la seguridad internacional y la proliferación de armas de destrucción masiva, como sus implicancias para la ciberseguridad mencionadas a lo largo de este artículo, deben ser entendidas en contexto. A pesar de ser un acuerdo no vinculante, este tipo de regímenes complementan los esfuerzos de los tratados o de la llamada *hard law,* con lo que crean normas que presionan a los Estados a establecer estándares mínimos en la materia. El problema principal está en la naturaleza de los bienes que se quiere regular, los cuales no tienen como límite una frontera física, por lo que se considera necesario debatir y replantear su control.

Referencias

Adi, Mohammad-Munir (2013). *The usage of social media in the Arab Spring*. Berlín: LIT Verlag Münster.

Álvarez, Daniel y Francisco Vera (2017). «Ciberseguridad y derechos humanos en América Latina». En Agustina del Campo (compiladora), *Hacia una internet libre de censura 2: Perspectivas en América Latina*. 1.ª ed. Buenos Aires: Universidad de Palermo.

Anderson, Collin (2015). *Considerations on Wassenaar Arrangement control list additions for surveillance technologies.* Nueva York: Access. Disponible en http://bit.ly/2kUQIpM.

Beck, Michael, Cassady Craft, Seema Gahlaut y Scott Jones (2002). *Strengthening multilateral export controls: A non proliferation priority*. Athens: Center for International Trade and Security, Universidad de Georgia. Disponible en http://bit.ly/2xVkMen.

17. «National progress report: Chile», Nuclear Security Summit, 31 de marzo de 2016, disponible en http://bit.ly/2y1KDl9.

Bratus, Sergey, DJ Capelis, Michael Locasto y Anna Shubina (2014). «Why Wassenaar's definitions of intrusion software and controlled items put security research and defense at risk, and how to fix it». Comentario público. Disponible en http://bit.ly/2JGmS6u.

Bohnenberger, Fabian (2017). «The proliferation of cyber surveillance technologies: Challenges and prospects for strengthened export controls». *Strategic Trade Review,* 4: 81-102. Disponible en http://bit.ly/2M7gH9X.

Bonarriva, Joanna, Michell Koscielski y Edward Wilson (2009). «Export controls: An overview of their use, economic effects, and treatment in the global trading system». Documento de trabajo ID-23. Disponible en http://bit.ly/2Mbn1xi.

Bronowicka, Joanna y Ben Wagner (2015). «Between international relations and arms controls: Understanding export controls for surveillance technologies». *Przegląd Politologiczny*, 3: 153-165. DOI: 10.14746/pp.2015.20.3.11.

Crail, Peter (2006). «Implementing UN Security Council Resolution 1.540». *The Non-proliferation Review*, 13 (2): 355-399. DOI: 10.1080/10736700601012193.

Dullien, Tomas, Vicenzo Iozzo y Mara Tam (2015). «Surveillance, software, security, and export controls: Reflections and recommendations for the Wassenaar Arrangement licensing and enforcement officers meeting». Informe. Disponible en http://bit.ly/2sPk4tt.

Flynn, Cristin y Brian Fletcher (2016). «Export controls and cybersecurity tools: Renegotiating Wassenaar». RSA Conference, 20 a 22 de julio de 2016. Singapur. Disponible en http://bit.ly/2sRtzIC.

Fuhrmann, Matthew (2008). «Exporting mass destruction? The determinants of dual-use trade». *Journal of Peace Research*, 45 (5): 633-652. DOI: 10.1177/0022343308094324.

Herr, Trey (2016). «Malware counter-proliferation and the Wassenaar Arrangement». Octava Conferencia Internacional sobre Ciber Conflicto. DOI: 10.2139/ssrn.2711070.

Herr, Trey y Paul Rosenzweig (2015). «Cyber weapons and export control: Incorporating dual use with the prep model». *Journal of National Security Law & Policy,* 8 (2): 1-19. DOI: 10.2139/ssrn.2501789.

Heupel, Monica (2007). «Implementing UN Security Council Resolution 1.540: A division of labor strategy». *Carnegie Papers,* 87: 1-21. Disponible en http://ceip.org/2HwamBD.

Hibbs, Mark (2011). *The future of the nuclear suppliers group*. Washington DC: Carnegie Endowment for International Peace.

Hirschhorn, Eric (2010). *The export control and embargo handbook*. Nueva York: Oxford University Press.

Kraig, Michael (2009). *United Nations Security Council Resolution 1.540 at the crossroads: The challenge of implementation.* Muscatine: The Stanley Foundation. Disponible en http://bit.ly/2LAoI3c.

McGuire, Cheri (2016) «Prepared testimony and statement for the record of Cheri F. McGuire». Presentación ante el Comité de la Cámara de Estados Unidos sobre Seguridad Nacional, Subcomité sobre Ciberseguridad, Protección de Infraestructura y Tecnologías de Seguridad, 12 de enero de 2016. Disponible en http://bit.ly/2xRwN4J.

Pyetranker, Innokenty (2015). «An umbrella in a hurricane: Cyber technology and the December 2013 Amendment to the Wassenaar Arrangement». *Northwestern Journal of Technology and Intellectual Property*, 13 (2): 154-179. Disponible en http://bit.ly/2kZ7mVy.

Ramírez Morán, David (2016). «La ciberseguridad en el contexto del arreglo de Wassenaar». *Boletín IEEE*, 1: 270-276. Disponible en http://bit.ly/2kWyxjF.

Rodríguez, Aldo (2014). *Bienes intangibles, licencias y regalías*. Ciudad de México: LAWGIC.

Sidel, Victor y Barry Levy (2007). «Proliferation of nuclear weapons: Opportunities for control and abolition». *American Journal of Public Health,* 97 (9): 1.589-1.594. DOI: 10.2105/AJPH.2006.100602.

Stinnett, Douglas, Bryan Early, Cale Horne y Johannes Karreth (2011). «Complying by denying: Explaining why States develop nonproliferation export controls». *International Studies Perspectives*, 12 (3): 308-326. DOI: 10.1111/j.1528-3585.2011.00436.x.

Wagner, Ben (2012). *After the Arab Spring: New paths for human rights and the internet in European foreign policy*. Bruselas: Unión Europea. Disponible en http://bit.ly/2kZ9Tz2.

Sobre la autora

Camila Hernández Sánchez es cientista política. Licenciada en Ciencia Política por la Pontificia Universidad Católica de Chile. Magíster en Conflicto, Seguridad y Desarrollo por el King's College, Reino Unido. Su correo electrónico es chernandezs@uc.cl.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.cl).