ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

16/2012 9 de marzo de 2016

David Ramírez Morán

LA CIBERSEGURIDAD EN EL CONTEXTO DEL ARREGLO DE WASSENAAR

LA CIBERSEGURIDAD EN EL CONTEXTO DEL ARREGLO DE WASSENAAR

Resumen:

En la edición de 2013 se introdujeron en la lista de bienes y tecnologías de uso dual y municiones del Arreglo de Wassenaar el "Software de intrusión" y las tecnologías de vigilancia de comunicaciones IP. El objeto era dificultar el acceso a estas tecnologías por parte de países que no respetan los Derechos Humanos. Debido a la forma en que se definió el término "software de intrusión", una gran parte de las herramientas utilizadas con fines de ciberseguridad por investigadores y profesionales pueden considerarse incluidas en estas listas, lo que ha supuesto un problema para las empresas y profesionales de estos ámbitos que ha escalado hasta los gobiernos.

Abstract:

In the 2013 edition of the lists of the Wassenaar Agreement, "Intrusion Software" and IP communication surveillance technologies were included in the dual-use goods and technologies and munitions list. The purpose was to hinder the acquisition of these technologies by countries that do not respect the Human Rights. Due to how "intrusion software" was defined, a big set of the tools used for cybersecurity by researchers and professionals can be considered as included in the lists, what has given place to a problem for the enterprises and professionals of these fields that has escalated to the governments.

Palabras clave:

Ciberseguridad, Wassenaar, exportación, uso dual, intrusión, vigilancia.

Keywords:

Cibersecurity, Wassenaar, export, dual use, intrusion, surveillance.

INTRODUCCIÓN

El Arreglo de Wassenaar[1] fue firmado en diciembre de 1995 en la ciudad holandesa del mismo nombre y hoy forman parte de él 41 países. Se trata de uno organización en la que los países firmantes se comprometen a establecer mecanismos de control de la exportación de los bienes y tecnologías de uso dual y municiones recogidos en las listas que se revisan anualmente. Se trata de dos listas, la lista de bienes y tecnologías de uso dual y la lista de municiones.

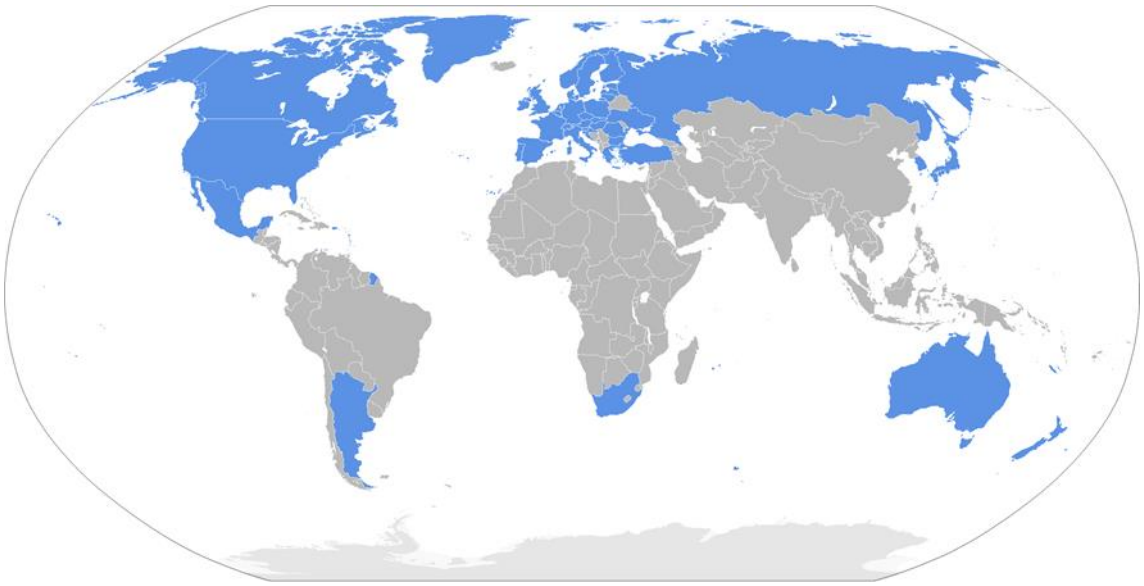

Figura 1: Países participantes en el arreglo de Wassenaar (Fuente: Wikimedia)

La primera está formada por 9 categorías: materiales especiales y equipamiento relacionado; procesado de materiales; electrónica; ordenadores; telecomunicaciones y seguridad de la información; sensores y láseres; navegación y aviónica; marítima; y aeroespacial y propulsión. Además, de entre los distintos apartados que forman estas categorías, se identifican aquellos que se consideran sensibles y los que se consideran muy sensibles, sobre los que hay tomar medidas de control adicionales.

Por su parte, la lista de municiones está formada por 22 elementos en los que se recogen materiales y bienes de diversa naturaleza entre la que figuran materiales explosivos, químicos, biológicos, material de guerra, etc.

1 www.wassenaar.org

EL ORIGEN DEL PROBLEMA

En la revisión de las listas del Acuerdo realizada en 2013 se introdujo una nuevo conjunto de bienes sujetos a las restricciones de exportación denominado "Software de intrusión" y que aparece definido como:

> «"Software de intrusión"
>
> "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:
>
> a. La extracción de datos o información, de un ordenador o dispositivo con capacidad de interconexión en red, o la modificación del sistema o de datos de usuario; o
>
> b. La modificación del flujo de ejecución estándar de un programa o proceso con objeto de permitir la ejecución de instrucciones proporcionadas desde el exterior.»

A esta definición le siguen dos notas que delimitan con más detalle el alcance de la definición, que excluyen e incluyen respectivamente sistemas en esta definición:

> «1. "Software de intrusión" no incluye ninguno de los siguientes:
>
> a. Hipervisores, depuradores o herramientas de Ingeniería inversa de Software (SRE);
>
> b. "Software" de Gestión Digital de Derechos (DRM); o
>
> c. "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.»

Asimismo, la definición se complementa con dos notas técnicas adicionales que especifican el significado de los dos elementos entrecomillados de la definición:

> «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 del , Productos de Seguridad Personal (PSP), Sistemas de Detección de Intrusos (IDS por sus siglas en inglés), Sistemas de Prevención de Intrusión (IPS por sus siglas en inglés) o firewalls.
>
> 2. 'Contramedidas protectoras': técnicas diseñadas para asegurar la ejecución segura de código, como Prevención de Ejecución de Datos (DEP por sus siglas en inglés), Aleatorización de la Distribución del Espacio de Direcciones (ASLR por sus siglas en inglés) o cajones de arena (sandboxing).»

Como se puede observar, se trata de una definición compleja, que ha sido elaborada por personas con una alta capacitación técnica y profundo conocimiento del estado del arte tecnológico.

También se aprecia en esta definición una participación del sector industrial importante, con la exclusión de tecnologías imprescindibles para el desarrollo de sistemas, como son los depuradores, o para la virtualización creciente que se está aplicando en los sistemas, como son los hipervisores. De esta forma se eliminan las posibles barreras que podrían dar lugar a problemas para la exportación de las tecnologías que aglutinan actualmente una parte muy importante de la facturación del sector. Esta exclusión responde a los principios bajo los que se incluyeron estas tecnologías en la lista, que perseguían dificultar el acceso a tecnologías que pudieran vulnerar la libertad de expresión o la privacidad a aquellos países que no respetan los Derechos Humanos[2], pero sin afectar al normal funcionamiento de los mercados tecnológicos con fines comerciales.

El problema surge del hecho de que la mayor parte de las herramientas utilizadas por los expertos en ciberseguridad se encuentran incluidas en la definición de "Software de intrusión", por lo que la adquisición transfronteriza de estas tecnologías debería estar sujeta a los procedimientos establecidos de autorización de la operación. En el caso de España, el procedimiento viene recogido en la Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso, donde se recoge el compromiso español con el Arreglo de Wassenaar entre otros.

Por otro lado, la exclusión específica de los sistemas de Gestión Digital de Derechos es un aspecto que resulta singular, pues su mera aparición en este documento, pese a ser descartados, considera la posibilidad de que estos sistemas pudieran estar siendo utilizados para extraer información, modificar datos de usuario, modificar el flujo de ejecución del software o ejecutar instrucciones recibidas del exterior y, además, sin ser detectadas por las herramientas de monitorización o saltándose las medidas protectoras implantadas en los dispositivos. Esta salvedad está muy relacionada con sucesos que han ocurrido en el pasado como los *rootkit* que se instalaban de forma encubierta en los ordenadores de los usuarios al reproducir un CD de música hace ya bastantes años[3], o la instalación persistente de software que introducía vulnerabilidades en los sistemas de los usuarios por parte de un gran fabricante de ordenadores[4] hace unos pocos meses. Resulta irónico pues al menos en el segundo caso (y en el primero de haber estado ya en vigor la actualización) podría aducirse que se estaba incurriendo en una vulneración del Arreglo al comerciar globalmente con bienes que incorporaban estas tecnologías.

Además del "software de intrusión", en la edición de 2013 del Arreglo se incorporó en la Categoría 5, de telecomunicaciones, un nuevo apartado 5.A.1.j por el que se incluían los equipos y sistemas de vigilancia de comunicaciones en redes IP. Esta adición, sin embargo, no ha dado lugar a problemas comparables debido a que se delimitan con precisión los equipos que son objeto de control.

2Collin Anderson. Considerations on Wassenaar Agreement control list additions for surveillance technologies. https://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf

3 *"Are You Infected by Sony-BMG's Rootkit?"* https://www.eff.org/deeplinks/2005/11/are-you-infected-sony-bmgs-rootkit

4 "*SuperFish Vulnerability*" https://support.lenovo.com/es/es/product_security/superfish

REACCIÓN INTERNACIONAL

El problema alcanzó su cénit cuando en 2015 la empresa HP declinó su asistencia al congreso Pwn2Own sobre ciberseguridad que iba a celebrarse en Japón, al considerar que traspasar una frontera con un *exploit* (demostración de la posibilidad de explotar una vulnerabilidad) que iba a presentar en el congreso suponía una transgresión del Arreglo de acuerdo a la implementación que Japón había aplicado[5]. Acudir al congreso suponía para la empresa un riesgo regulatorio que no estaba dispuesta a asumir. El problema fue a más hasta que finalmente fue cancelado el congreso y salieron a la luz los problemas asociados a la nueva redacción de la lista de bienes y tecnologías afectados.

De acuerdo a esta interpretación, todo intercambio de un *exploit* a través de una frontera debería estar sujeto a la obtención de una licencia, lo que incluía el intercambio de información entre los Centros de Respuesta ante Incidentes de Seguridad (CERT/CSIRT), lo que haría inviable la compartición de información sobre vulnerabilidades para poner fin a las amenazas identificadas. El mundo de la ciberseguridad se ha basado tradicionalmente en el intercambio de información entre actores para que los proveedores y fabricantes puedan poner solución a los problemas detectados

5 Mimoso, Michael, *Citing Wassenaar, HP pulls out of mobile Pwn2Own*. https://threatpost.com/citing-wassenaar-hp-pulls-out-of-mobile-pwn2own/114542/

antes de que grupos criminales tengan posibilidad de explotar estas vulnerabilidades con fines delictivos como el robo o alteración de la información u otros delitos cibernéticos.

Bajo esta coyuntura, las empresas cuyo modelo de negocio se basa en la venta de *zero day*, vulnerabilidades del software que no se han hecho públicas y constituyen, por tanto, una vía para poder acceder a sistemas de terceros, ven alterado su modelo de negocio hasta el punto de que plantean cambiar su ubicación a países que no formen parte del Arreglo. La empresa francesa VUPEN, por ejemplo, comunicó en su página web que las restricciones resultaban de aplicación a sus productos por lo que tendría que excluir automáticamente a todos los países sometidos a restricciones de la Unión Europea y aquellos que estén sometidos a embargos de los EE.UU. o las Naciones Unidas.[6]

Bajo el concepto comercial, se pueden aducir razones morales o éticas en contra de que haya empresas que negocien con este tipo de tecnologías para actividades como el espionaje, el robo de información económica, industrial o comercial, o incluso para que algunos países cuenten con los medios para violar los Derechos Humanos a la privacidad y seguridad de sus ciudadanos. También sin violar los Derechos Humanos, estos países pueden utilizar tecnologías de este tipo para acceder a información de industrias de otros países o información gubernamental con fines estratégicos.

Sin embargo, desde el punto de vista de la investigación y la aplicación profesional de la ciberseguridad, las prácticas establecidas chocan con lo recogido en el Arreglo. Por un lado, la investigación de los hackers se ve potenciada por la organización de congresos en los hacen públicas las vulnerabilidades que han detectado. Normalmente se sigue un proceso que se denomina de «*responsible disclosure»* o publicación responsable, por el que comunican la vulnerabilidad al proveedor o fabricante de forma que pueda poner solución al problema antes de hacer pública su existencia en uno de estos congresos. Cuando el descubridor de la vulnerabilidad y el proveedor no son del mismo país, la propia comunicación a través de la frontera podría considerarse como la exportación de un *exploit,* contraviniéndose así los principios del Arreglo en el caso de no solicitar una licencia de exportación. Asimismo, las herramientas que utilizan los investigadores y profesionales para hacer pruebas de intrusión de los sistemas de sus clientes figuran en la mayor parte de los casos dentro de la definición de "Software de intrusión", por lo que si cruzan una frontera con estas aplicaciones instaladas, por ejemplo, en un portátil, estarían incurriendo en tráfico ilegal de material de doble uso.

Incluso la industria comercial de productos de ciberseguridad elaboró una carta abierta a través de la Alianza del Software[7] en la que apelaba al Congreso de los EE.UU. a firmar la carta Langevin-McCaul contra la implementación de los cambios en el Arreglo pues afectaría negativamente a la seguridad nacional regulando el acceso a tecnologías de ciberseguridad fundamentales.

---

6 Granick, Jennifer, *Changes to export control arrangement apply to computer exploits and more.* The Center for Internet and Society, *15/01/2014* http://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more

7 http://www.bsa.org/~/media/Files/Policy/IssueBriefs/12072015Wassenaar.pdf

Desde mediados del año pasado, en la Unión Europea ya se vienen produciendo reacciones a la redacción actual del Arreglo, y se plantea la necesidad de su modificación.[8] En primer lugar se ha instado a los países a que a la hora de implantar la regulación lo hagan de forma tal que se minimicen los efectos indeseados de la aplicación de la definición en el Arreglo.

A mediados del mes de febrero se ha puesto en marcha en EE.UU. una iniciativa similar en la que se está considerando la posibilidad incluso de eliminar completamente el "Software de intrusión" del Arreglo. El motivo se basa en los problemas que han surgido a la hora de redactar las normas con las que implementar el Arreglo[9] por parte de los 41 países.

CONCLUSIONES

En el campo de la ciberseguridad es necesario alcanzar un punto de equilibrio entre la preservación de la privacidad y la seguridad de los ciudadanos. A esta difícil ecuación se están incorporando variables adicionales que contribuyen a desestabilizar este equilibrio con la introducción de intereses comerciales, así como el deseo de algunas naciones de explotar las capacidades tecnológicas con fines estratégicos e incluso políticos, desarrollando actividades que pueden llegar a violar los Derechos Humanos.

Las reacciones de los diversos actores involucrados en este problema hacen prever una modificación de los términos del Arreglo de Wassenaar para adecuarlo a los intereses y necesidades de todos los afectados. La cuestión es que los procedimientos que rigen el Arreglo hacen que la modificación de las listas no se pueda llevar a cabo hasta finales de 2016, por lo que queda todavía un largo periodo de vigencia de una norma que, a todas luces, no se ciñe únicamente a los principios con los que inicialmente fue implantada sino que ha dado lugar a efectos indeseados que afectan incluso a los propios gobiernos.

Nuevamente se produce en el campo de la ciberseguridad una situación caracterizada por la dificultad de establecer una regulación de aplicación directa cuando se ponen en juego los intereses internacionales de actores cuyas líneas de actuación presentan diferencias importantes.

David Ramírez Morán
Analista del IEEE

8 *Public online consultation on the export control policy review.*
http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190
9 https://langevin.house.gov/sites/langevin.house.gov/files/documents/01-28-16_NSC_Response.pdf