Analisis de la actualidad internacional:

¿Hacia un Cyber-Wassenaar?

AUTOR: Ángel Vallejo, responsable de relaciones institucionales de THIBER, the cybersecurity think tank.

El Acuerdo de Wassenaar (WA ó Wassenaar Agreement) es hoy día el texto internacional no normativo de referencia en lo tocante a control en la exportación de municiones, por un lado, y de bienes y tecnologías de uso dual por otro.

Aprobado en 1995 en la ciudad holandesa que le da nombre, el Acuerdo comenzó a ser plenamente operativo en septiembre de 1996, con la idea de complementar los regímenes ya existentes en materia de no proliferación de armas de destrucción masiva. Su foco fundamental era y es la detección y prevención de amenazas a la paz y a la estabilidad, tanto de carácter regional como internacional. Frente a las regulaciones enfocadas a las armas en sentido estricto, el Acuerdo hace hincapié desde su génesis en las tecnologías y bienes de doble uso, es decir, en aquellas que, siendo inicialmente ideadas con miras a un uso civil o comercial, tenían la capacidad de ser también utilizadas en el desarrollo o implementación de sistemas militares.

Con un claro antecedente en los trabajos del Comité de Coordinación para el Control Multilateral de las Exportaciones Estratégicas (COCOM) creado en 1950, en plena guerra fría y disuelto en 1994, el Acuerdo supone el compromiso de los miembros firmantes (cuarenta y dos países en la actualidad, desde los treinta y tres inicialmente adheridos) de establecer un control en las exportaciones de los elementos incluidos en las

"En diciembre de 2016, Estados Unidos llevó al pleno Wassenaar la necesidad de aprobar una revisión del lenguaje en que se definía y trataba el software intrusivo en el texto de 2013, indicando que, de no hacerse, los efectos negativos en la industria, la academia y la investigación podrían ser irreversibles"

listas oficiales (las listas Wassenaar), de manera que puedan prohibirlas hacia determinados países o, en su caso, requerir una licencia para tal exportación. El Acuerdo no tiene carácter de tratado internacional, si bien los estados miembros se comprometen a implementar en sus normativas internas la legislación que permita la efectividad del deseado control en las referidas exportaciones. Por lo que hoy nos ocupa, es fácil entender que entre el año en que el Acuerdo comienza su andadura (1996) y el actual 2018 el panorama de la tecnología ha sufrido una transformación de tal calibre, tanto en el sector armamentístico como en el civil, que los objetivos y medios que los primeros firmantes se representaban como deseables y adecuados respectivamente se hayan visto drásticamente condicionados por el ritmo de la innovación.

La mera consideración del software como algo que debiera ser objeto de control bien podía representarse en aquel entonces como algo impensable fuera de las *cryptowars* de los años noventa, de carácter mucho más específico y sectorial. De hecho, la única referencia que el Acuerdo hizo sobre la materia fue en 1998 cuando estableció ciertas restricciones a la exportación de determinados productos para encriptación.

En España la primera incorporación relevante de parte de los conceptos del Acuerdo se produjo a mediados de los años dos mil, a través de la Ley 53/2007, haciéndose en esta norma una referencia expresa a dicho texto y a la necesidad de implementar normativa doméstica al respecto. En Europa, la más relevante adecuación con referencia también expresa al Acuerdo se estableció por medio del Reglamento 428/2009, que entre otras cosas incluía una lista de *productos* de doble uso acorde con los términos Wassenaar con miras a establecer un régimen comunitario de control de las exportaciones, transferencia, corretaje y tránsito de los mismos.

Desde los efectos de las *cryptowars* en el Acuerdo en 1998 hasta 2013 asistimos a quince años en los que el desarrollo de las tecnologías de la información y la comunicación (TIC) sufre una eclosión que cambia de raíz todas las estructuras sociales a nivel local, nacional e internacional, introduciendo y haciendo accesibles al gran público múltiples herramientas que hasta el momento solo estaban disponibles para los estados y las grandes corporaciones.

En 2013 se produce por fin la inclusión amplia y expresa en el Acuerdo de elementos del ámbito ciber, entre otras cosas (así se justificó) debido a la constatación de que los gobiernos de ciertos países estaban usando tecnologías de software con finalidades puramente represivas para con sus ciudadanos, y también con la finalidad de monitorizar y acceder de manera indetectable a las comunicaciones privadas de los mismos a gran escala. La primavera árabe y el uso de software intrusivo por los gobiernos afectados se han citado recurrentemente como justificación de una necesaria adaptación de algunos de los principios y objetos del Acuerdo.

En ese año el Reino Unido y Francia introducen potentes propuestas de negociación para la restricción (y, por tanto, inclusión en las listas Wassenaar) del llamado software intrusivo. Los casos revelados de la compañía italiana Hacking Team y sus vínculos con gobiernos como el de Siria, Etiopía, Bahrein y Egipto, y paralelamente la inglesa Gamma Group International, también relacionada con la venta a gobiernos considerados *de opresión* que espiaban no solo computadoras sino también los dispositivos móviles particulares hicieron mucho por la presión de adecuar el texto del Acuerdo a la realidad tecnológica y al ubicuo uso como instrumento pretendidamente oculto de poder de cara a los ciudadanos.

El efecto de lo anterior fue que lo que se consideraba software intrusivo y sus herramientas aparejadas fueron incluidos en las listas, bajo los conceptos "software de información" y "tecnologías de software de información" respectivamente. Del nuevo texto Wassenaar se derivaron posteriores implementaciones en las legislaciones de la mayoría de los países firmantes, con mayor o menor acierto. En Europa el Reglamento 599/2014 traspuso con celeridad buena parte de los nuevos conceptos del Acuerdo, a través de una modificación y adaptación del anterior Reglamento 528/2009.

Pero no en todos los entornos la transición resultó ni tan rápida ni tan fluida. En Estados Unidos, la industria de las TIC, la academia y también el Departamento de Defensa pusieron sobre la mesa serias preocupaciones, todas ellas relacionadas con lo que consideraban una terminología demasiado amplia o extensa en la modificación del Acuerdo en 2013. Se generó un cierto consenso entre los citados actores en lo relativo a que, tal y como se había redactado por los miembros de Wassenaar, la implementación doméstica en Estados Unidos podía producir un perjuicio irreparable.

Las nefastas perspectivas que en Norteamérica se pusieron sobre el tapete apuntaban, esencialmente a dos cuestiones. La primera de ellas, la situación de práctica ilegalidad en la que podía quedar un im-

portante número de compañías del sector de las TIC (especialmente las desarrolladoras de software destinado a la ciberseguridad) si la implementación doméstica se hacía en los términos tan amplios que obraban en el Acuerdo de 2013. La segunda, el perjuicio que tal implementación produciría para la soberanía del país. LA relevancia de estos problemas no puede subestimarse, dado que, de hecho, las actividades de investigación y comercialización para seguridad de elementos como los *zero days,* por mucho que se llevaran a cabo de manera transparente y en el seno de relaciones comerciales ya establecidas, podían considerarse potencialmente infractoras de los principios citados si se desarrollaban a nivel internacional desde compañías norteamericanas. Los acérrimos resistentes a la implementación afirmaban que salir del país con un *exploit,* aun con destino a eventos académicos y en el seno de un "responsable disclosure", podía suponer una actividad sujeta a control de exportación, de modo que en los numerosos congresos de ciberseguridad que se celebraban a lo largo del globo la cuestión generaba agrias polémicas.

Se argüía por la industria norteamericana que la literalidad del Acuerdo en su versión renovada requiriría la expedición de licencias de control de exportación a prácticamente cualquier compañía o profesional individual que trabajase en el ámbito de tecnologías y software de control necesarios para proteger los sistemas en tiempo real contra el ataque de un botnet.

En diciembre de 2016, Estados Unidos llevó al pleno Wassenaar la necesidad de aprobar una revisión del lenguaje en que se definía y trataba el software intrusivo en el texto de 2013, indicando que, de no hacerse, los efectos negativos en la industria, la academia y la investigación podrían ser irreversibles. El equipo norteamericano no tuvo el éxito deseado y el año 2017 fue un tiempo de frenética actividad doméstica e internacional en los despachos de las grandes compañías, las delegaciones diplomáticas y las agencias del gobierno USA.

Se hizo evidente que había que acotar la literalidad del texto de 2013, pero de hecho el año 2017 se consideró a nivel interno como un período de *limbo* regulatorio, quedando su gobierno como uno de los más retrasados respecto a la adaptación ocurrida cuatro años antes, una adaptación que la mayoría de países miembros ya había traspuesto a nivel doméstico con

"El planteamiento internacional de un acuerdo específico, y no uno de carácter general, que regule la exportación de tecnologías de doble uso en el ámbito de las TIC (y especialmente en el área de la ciberseguridad) parece inaplazable"

mayor o menor contundencia. La carta remitida por los congresistas Langevin, McCaul y Thompson en febrero de 2017 al Teniente General Michael Flynn, asesor del presidente en materia de seguridad nacional contenía de manera condensada las urgencias que el gobierno estadounidense debía atender de cara al Acuerdo.

Hubo que esperar hasta el pleno siguiente, en diciembre de 2017 para que las propuestas de Estados Unidos tuvieran el tan buscado eco, si bien parcial, en el marco Wassenaar, atendiendo al menos a los más importantes problemas planteados por la industria de la ciberseguridad norteamericana (obviamente compartidos por otras muchas europeas y de otras áreas).

Podemos identificar tres cambios esencialmente relevantes respecto de 2013, siendo el primero el establecimiento de una excepción a la restricción de software o tecnologías de intrusión, siempre que estén destinados a la detección de vulnerabilidades o a las respuestas a ciberincidentes. Se trata aquí, obviamente, de permitir una legítima ciber defensa ante un ataque ilícito.

En segundo lugar, se acota la definición de las restricciones aplicadas sobre el genérico software de intrusión, sustituyendo las referencias al "software especialmente diseñado para operar o comunicarse con software de intrusión" por la expresión "software especialmente diseñado para la ejecución y el control del software de intrusión". Lo primero supone la posibilidad de gestionar una situación en la que se sufre el uso de software intrusivo y lo segundo supone, obviamente, la creación y ejecución de software con finalidad intrusiva.

Por último, se introduce una aclaración consistente en especificar que las nuevas excepciones de 2017 a las reglas generales de 2013 no significarán una disminución de las facultades de las autoridades nacionales de verificar el oportuno cumplimiento de los estándares adoptados.

Más allá de las concretas modificaciones que el estado de la técnica exige respecto de las normas que se ven obviamente superadas por el desarrollo tecnológico, es esencial detectar que cuando la situación de hecho que pretende ser regulada por una norma de obligado cumplimiento (como un tratado internacional) o de mero compromiso (como el tan citado acuerdo Wassenaar) cambia en el modo en que han cambiado las TIC, la adaptación de normas ya existentes puede resultar más compleja que la promulgación de normas creadas *ad hoc* para esa concreta materia. Parece indiscutible, a estas alturas, que un texto de 1996, por mucho que se vaya adaptando cada cuatro o seis años, no puede razonablemente pretender estar acompasado con una realidad tecnológica que se reinventa cada pocos meses.

Sobre esta premisa, el planteamiento internacional de un acuerdo específico que regule la exportación de tecnologías de doble uso en el ámbito de las TIC (y especialmente en el área de la ciberseguridad) parece inaplazable. La decisión de si esto se va a afrontar desde el enfoque de una suerte de *Ciber-Wassenaar* o desde un acuerdo desvinculado totalmente del texto aprobado en 1996, que saque esta materia del Acuerdo original y la lleve a un nuevo marco, es algo que en interés de la seguridad internacional debe adoptarse sin demora.