ARI 49/2024 (versión en español)
22 de abril de 2024

Transferencias tecnológicas ilícitas a países preocupantes: retos para la comunidad internacional

Gonzalo de Salazar | Asesor para Asuntos Estratégicos y coordinador de la Política de Sanciones, Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.

Tema

La eficiencia de los regímenes multilaterales de control de exportaciones militares y de doble uso implantados en el siglo XX se ha visto mermada por las redes de tráfico ilícito y las lagunas en los controles de las exportaciones.

Resumen

La información reciente sobre el uso de tecnología occidental en armas empleadas por Rusia ha planteado la cuestión de la eficacia de las sanciones y de los mecanismos de control de las exportaciones implantados entre 1975 y 1995, puesto que el panorama mundial actual es muy distinto al de las últimas décadas del siglo XX. En este documento se analiza la necesidad de atender a la naturaleza de las transacciones que conlleven riesgos, detectar las carencias, proponer la modernización de los controles a las exportaciones mediante políticas de concienciación, actualizar el marco normativo y dotar de los recursos adecuados a los organismos ejecutores nacionales.

Análisis

Deficiencias en los controles a las exportaciones: situación actual

Los indicios que apuntan a exportaciones de fabricantes occidentales a Rusia después de la invasión de Ucrania en 2022 ponen de manifiesto hasta qué punto dependen sus armas de estos componentes.[1] Un análisis pormenorizado de la tecnología empleada por los sistemas militares rusos muestra que el sector de la defensa utiliza numerosos elementos de fabricación extranjera.[2] También se han encontrado tecnologías occidentales en los vehículos aéreos no tripulados del ejército iraní. Es importante señalar que, en muchos casos, las empresas que fabrican esos artículos no incurren en

[1] El Instituto RUSI ha llegado a identificar 450 componentes de fabricación extranjera al examinar 27 sistemas militares rusos diferentes, entre ellos los misiles Kalibr e Iskander. El programa de modernización militar de Rusia ha dependido del uso a gran escala de componentes microelectrónicos fabricados en Occidente. También se han descubierto pruebas del uso de componentes falsificados en los sistemas de armamento rusos y, por lo tanto, de la posibilidad de que las entidades identificadas no hayan fabricado los componentes en los que aparecen sus propios logotipos. James Byrne *et al*. (2022), "Silicon lifeline: western electronics at the heart of Russia's war machine", RUSI, agosto.

[2] Conclusiones basadas en datos de más de 170 componentes individuales encontrados en equipos rusos con las marcas o logotipos de empresas extranjeras, entre ellos microchips empleados para hacer funcionar teléfonos móviles y ordenadores portátiles suministrados por países intermediarios, si bien la investigación no corrobora que estas transferencias hayan conculcado ninguna reglamentación internacional o nacional. Véase International Partnership for Human Rights (IPHR) & The Independent Anti-Corruption Commission (NAKO) (2023), "Enabling war crimes? Western-made components in Russia's war against Ukraine" y "The chips are down: Putin scrambles for high-tech parts as his arsenal goes up in smoke", Politico, 5/IX/2022.

responsabilidad penal alguna, sobre todo cuando los componentes transferidos no figuran como restringidos en ninguna reglamentación de control de las exportaciones.

Ciertas restricciones relativas a la exportación a Irán de tecnologías relacionadas con los sectores nuclear y militar derivadas de la Resolución 2231 del Consejo de Seguridad de las Naciones Unidas (la cual refrendó el Plan de Acción Integral Conjunto en 2015) no se consideraron "sanciones" en su momento, sino "restricciones temporales" para garantizar que el acuerdo llegase a buen puerto. Cabe mencionar también que esta Resolución 2231 impuso limitaciones comerciales a la tecnología nuclear, las transferencias de armas convencionales, los misiles y los vehículos aéreos no tripulados.[3] Asimismo, esas restricciones impiden que los países miembros de la Organización de las Naciones Unidas (ONU) participen en el suministro, la venta o la transferencia a o desde Irán de cualquier artículo, material, equipo, bien o tecnología que aparezca como restringido en el Régimen de Control de la Tecnología de Misiles. Ahora bien, los límites impuestos por el Consejo de Seguridad de la ONU para el comercio con Irán de misiles avanzados y vehículos aéreos no tripulados expiraron el 18 de octubre de 2023.[4] En estos momentos, el arsenal ruso incluye vehículos aéreos no tripulados iraníes. Además, determinados agentes no estatales (como Hamás, las milicias huzí y Hizbulah) tienen capacidad para ensamblar o producir algunas de estas armas, lo que podría indicar que cuentan con asistencia y suministros procedentes del extranjero, muy probablemente de Irán.

Las políticas sancionadoras se cuentan entre los instrumentos de carácter no militar más utilizados con fines de represalia, presión y disuasión. Se suelen equiparar las "sanciones" con las "medidas restrictivas", pero en la práctica puede haber medidas restrictivas sin un carácter sancionador. Dicho de otro modo, todas las sanciones son medidas restrictivas, pero no todas las medidas restrictivas son sanciones. Este último caso es el de la mayoría de los procedimientos aplicados por los regímenes multilaterales de control de las exportaciones (el Grupo de Suministradores Nucleares, el Grupo de Australia, el Régimen de Control de la Tecnología de Misiles y el Arreglo de Wassenaar), ya que no fueron creados como órganos sancionadores, sino como mecanismos encargados de conciliar los intereses comerciales legítimos con la

[3] La Resolución 2231 del Consejo de Seguridad de la ONU, aprobada el 20 de julio de 2015, tuvo como objetivo respaldar la aplicación del Plan de Acción Integral Conjunto (PAIC) e impuso limitaciones que estuvieron en vigor durante 90 días. Estas restricciones se aplicaban a todos los países miembros de la ONU y solamente se podrían revocar previa aprobación del Consejo de Seguridad. Estas restricciones limitadas en el tiempo para las transferencias de armas convencionales, que incluían la venta o adquisición de misiles y vehículos aéreos no tripulados con armamento, expiraron en 2020. Las relativas a misiles y vehículos aéreos no tripulados incluidos en los párrafos 3 y 4 del Anexo B de la resolución quedaron sin efecto el 18 de octubre de 2023. Se entiende que las definiciones del párrafo 3 se aplican a sistemas de Categoría I conforme a lo descrito en el Régimen de Control de la Tecnología de Misiles (cohetes y vehículos aéreos no tripulados con un rango mínimo de 300 km y una capacidad mínima de carga útil de 500 kg). El párrafo 4 incluye los sistemas de Categoría I y Categoría II (misiles y vehículos aéreos no tripulados con una carga útil inferior a 500 kg). Hasta el 18 de octubre, Irán tenía prohibido comerciar con cohetes guiados o no guiados y vehículos aéreos no tripulados con una autonomía igual o superior a 300 km. Además, las limitaciones para las actividades nucleares de Irán expirarán en octubre de 2025.

[4] El día antes, Rusia anunció que dejaría de respetar los límites impuestos por la Resolución 2231 e instó a los países europeos a dejar de lado las restricciones a Irán relativas a misiles y vehículos aéreos no tripulados, lo que ayudó al país asiático a impulsar sus exportaciones de armas, vehículos aéreos no tripulados y misiles. Rusia ha desplegado y utilizado misiles y vehículos aéreos no tripulados iraníes en Ucrania, así como misiles comprados a Corea del Norte.

seguridad internacional. No obstante, los anexos de estos regímenes sobre artículos y conocimientos técnicos también se han empleado como herramientas para la aplicación de sanciones.

Al hablar de los mecanismos de control de las exportaciones, debemos preguntarnos si los regímenes multilaterales en vigor pueden dar respuesta a las necesidades y los retos actuales. La respuesta es, hasta cierto punto, sí. Entre 1971 y 1996 se crearon varios regímenes multilaterales de exportaciones militares y de doble uso con el objetivo principal de encontrar un equilibrio entre los intereses comerciales y las inquietudes legítimas en materia de seguridad. Los regímenes de control de las exportaciones creados durante este periodo fueron el Comité Zangger en 1971, el Grupo de Suministradores Nucleares (GSN) en 1975, el Grupo de Australia (GA) en 1985, el Régimen de Control de la Tecnología de Misiles (RCTN) en 1987 y el Arreglo de Wassenaar (AW) en 1996. Con el paso de los años, estos regímenes han sido objeto de actualizaciones y han dado cabida a nuevos miembros. No obstante, el panorama mundial actual es muy distinto al de las últimas décadas del siglo XX, ya que cada vez se aprecian más deficiencias en los controles a las exportaciones y la eficiencia de estos regímenes se ha visto seriamente mermada. Hay motivos políticos y económicos de peso detrás de esta tendencia, pero el presente análisis se centrará en los aspectos técnicos.

Transacciones de riesgo a países que suscitan preocupación

Este documento comienza con una referencia a la acumulación creciente de pruebas sobre las exportaciones de fabricantes occidentales a Rusia después de invadir Ucrania en 2022. Los investigadores han descubierto empresas o intermediarios que podrían haber participado en actividades de elusión de las sanciones. También hay indicios que apuntan al uso de componentes falsificados en los sistemas de armas rusos e iraníes y a la posibilidad de que algunas de esas entidades identificadas no hayan fabricado los componentes en cuestión. Por lo tanto, este aspecto de las transferencias tecnológicas desestabilizadoras guarda relación con las redes de tráfico ilícito y las entidades de terceros países capaces de falsificar componentes mediante ingeniería inversa.

La mayoría de los productos encontrados en la cadena de suministro ilícita son de doble uso, si bien aparecen numerosos artículos de doble uso no restringidos como microchips diseñados para teléfonos móviles y ordenadores portátiles. Entre los artículos del primer grupo se encuentran:

- Máquinas robotizadas y máquinas de control numérico por ordenador.
- Piezas de recambio, refrigerantes, lubricantes y programas informáticos para máquinas de control numérico por ordenador.
- Módulos de memoria para unidades de computación y navegación por satélite para misiles.
- Circuitos, microprocesadores, interruptores y osciladores.
- Ordenadores y otros componentes electrónicos.
- Semiconductores, sistemas de navegación por satélite, ordenadores de guiado y altímetros.
- Giroscopios y chips aptos para GLONASS.
- Aparatos de radio.

Un segundo problema es el alcance y el *modus operandi* de las redes de tráfico ilícito. Aparte de la entrada de nuevos productores de tecnologías avanzadas militares y de doble uso, se han ido desarrollando mercados clandestinos paralelos a través del tráfico ilícito. Muchos de los artículos mencionados llegan a su destino a través de países que no forman parte de la "coalición sancionadora" o no aplican reglamentaciones adecuadas para el control de las exportaciones. Una gran parte de las redes ilícitas con actividad en estos países son supervisadas por los servicios de seguridad de los países de destino y suelen pasar desapercibidas para las autoridades locales.

Las armas y las tecnologías militares y de doble uso circulan fuera del alcance de los mecanismos multilaterales de control de las exportaciones. La implicación de las redes de tráfico ilícito en los conflictos armados y en cadenas clandestinas de suministro para países sometidos a embargos internacionales de armas plantea un gran reto a los gobiernos de los países proveedores. Hasta cierto punto, existe un vínculo entre las actividades delictivas organizadas y estas transferencias ilícitas. Estas redes, que a menudo presentan conexiones con el crimen organizado, han impulsado el desarrollo de mercados paralelos para estas tecnologías que surten a programas clandestinos de armas o de ingeniería inversa. Hay nuevos clientes que ven en estas redes una herramienta útil y grupos delictivos dedicados al contrabando que encuentran oportunidades de lucrarse, por lo que estas redes también buscan un beneficio económico en su relación con agentes estatales y no estatales. De hecho, existen numerosos intermediarios en la cadena de suministro.

Una vez establecidas las redes de tráfico ilícito, su perfil bajo, su gran movilidad y su carácter clandestino las sitúan *de facto* fuera del alcance de los mecanismos sancionadores y de control de las exportaciones, por lo que resultan atractivas para los países que suscitan preocupación, los grupos terroristas y los distintos grupos armados. Cuanto más pequeñas sean estas redes de transporte, más difícil será que las fuerzas del orden las detecten. Sin embargo, esas transferencias también se dan en países donde no resultan aplicables las sanciones o las reglamentaciones para el control de las exportaciones, por lo que se convierten en una "zona gris" y no contravienen la legislación vigente ni sus procedimientos de aplicación. Las transferencias de tecnologías intangibles dificultan aún más la aplicación de las reglamentaciones de aduanas y control de las exportaciones. Cada vez urge más contar con un marco jurídico actualizado e impartir formación especializada a los investigadores encargados del cumplimiento de la ley, así como insistir en la prevención y disuasión de transferencias ilícitas de tecnologías intangibles en el ámbito del control de las exportaciones.
Según las fuentes disponibles de libre acceso, las cadenas ilícitas de suministro suelen presentar las siguientes características:

- En muchos casos, los componentes llegan a su destino a través de una red transnacional de filiales y distribuidores operada por los propios países preocupantes para adquirir bienes a través de sociedades interpuestas. En ocasiones se trata de empresas pantalla que desarrollan su actividad durante un solo día para impedir que las incluyan en las listas de sanciones. Los centros de transbordo y las redes clandestinas se dedican a crear rutas que garanticen el acceso a la microelectrónica occidental.

- Recurren a certificados de usuario final fraudulentos, documentos que se emplean en las transferencias internacionales de venta y suministro de armas y tecnologías de doble uso. Sirven para identificar a los destinatarios finales de los materiales y certificar que no pretenden llevar a cabo envíos posteriores a terceros. El certificado se utiliza para especificar los detalles del destino final de las mercancías y su uso (empresa o entidad, dirección, país de destino y finalidad prevista –civil o militar–). Los certificados de usuario final se pueden falsificar con fines fraudulentos.

- En ocasiones, los usuarios finales son reales, pero se dedican a proyectos de ingeniería inversa para clientes desconocidos. La empresa declarada como usuario final puede desmontar los equipos, copiar los componentes del sistema y diseñar una réplica o un derivado que, a continuación, se vende a otro cliente desconocido para el exportador del producto original.

- Los datos aduaneros que figuran en los documentos de envío proporcionan una descripción de los productos muy general o incluyen información poco precisa. A veces ni siquiera incluyen el nombre de los bienes.

- Los destinatarios recurren a distintos métodos de pago: efectivo, transferencias bancarias e incluso trueque de mercancías (petróleo o materias primas), oro y criptomonedas. Efectúan transferencias en moneda local (rublos, yuanes, etc.) a cuentas bancarias de sus propios países (no sometidas a restricciones de exportación) o a cuentas extranjeras que aceptan esas divisas. A continuación, se transfieren los fondos y se convierten a otra divisa internacional (dólares estadounidenses, euros, etc.) para pagar al proveedor.

Transferencias de productos de doble uso sensibles, pero no restringidos

Muchas de las tecnologías en cuestión son bienes industriales producidos en masa que no están sujetos a los controles sobre el doble uso y se encuentran disponibles sin restricciones en el mercado. La transferencia de esos productos a países que suscitan preocupación es un tema sensible, pero no se trata de transferencias ilegales.

Además, las empresas proveedoras pueden tener su sede en un país obligado a respetar las sanciones y las reglamentaciones de control de las exportaciones, pero tener su producción ubicada en terceros países cuyas filiales locales tengan acceso a la tecnología original sin estar sujetas a las reglamentaciones sobre exportación del país de la sociedad matriz.[5] También pueden exportar artículos sensibles, pero no regulados, a terceros países que no impongan sanciones a los países preocupantes en cuestión, por lo que entrarían en una “zona gris” transnacional.

[5] Muchos países participan en los regímenes multilaterales de control de las exportaciones con directrices y reglamentaciones compartidas para el comercio internacional de armas y tecnologías de doble uso. Las filiales deslocalizadas de las empresas correspondientes en terceros países pueden tener acceso a tecnología sensible para producir determinados bienes y exportarlos legalmente si no se ven sometidas a las mismas reglamentaciones.

La mayoría de las medidas restrictivas internacionales las imponen los países occidentales a través de regímenes sancionadores y embargos sobre la base de la legislación nacional o multilateral. Menos de 40 países afines se muestran dispuestos a aplicar esas medidas en todo el mundo, pero el resto de la comunidad internacional se mueve en una "zona gris" en la que sólo se aplican de modo oficial las medidas restrictivas aprobadas por el Consejo de Seguridad de la ONU. Para que los proveedores transfieran a estos países algún artículo restringido hará falta contar con un certificado de usuario final. No obstante, estos mercados –cerca de 150 países– dan pie a las transferencias ulteriores a terceros países, bien por el escaso control sobre los artículos restringidos –lo que contraviene las condiciones del contrato con el proveedor–, bien por el libre intercambio de las tecnologías no restringidas. Son cuatro los motivos principales para llevar a cabo esta actividad:

1. Muchos países consideran ilegítimas las medidas restrictivas impuestas por todo ente que no sea el Consejo de Seguridad de la ONU.
2. Aunque opinen que son válidas, podrían no contar con los medios jurídicos o técnicos para hacer efectivos los controles.
3. Las herramientas jurídicas existentes tienen limitaciones a la hora de intervenir o prevenir las exportaciones de tecnologías de doble uso sensibles, pero no restringidas.
4. Algunos Estados dependen de los "países que suscitan preocupación" porque las armas, la tecnología, los proveedores energéticos y el flujo garantizado de esos suministros sigue siendo fundamental para su seguridad nacional. Para estos países, perder el acceso a equipos, componentes o suministros energéticos constituye una amenaza para su seguridad, lo que podría servirles de acicate para facilitar la evasión de las sanciones. En muchos casos, prevalecen las políticas orientadas al mundo empresarial y se crea una cadena de suministro alternativa.

No existe un consenso internacional en torno a los conceptos "transferencia desestabilizadora" o "cadena de suministro desestabilizadora". Las desavenencias en torno a la definición de una "transferencia desestabilizadora" son un reflejo de la propia naturaleza del sistema internacional, la dinámica de la competitividad estratégica y las percepciones diferentes (o contrapuestas) sobre la seguridad regional o internacional. Por ejemplo, Rusia, Irán y Corea del Norte consideran que las cadenas de suministro que refuerzan su propia seguridad y la sostenibilidad de sus operaciones militares –incluso a costa de la seguridad internacional y la integridad territorial de otros Estados– son un "factor estabilizador". No obstante, esta cuestión es fundamental para las controversias geopolíticas y no se puede abordar con éxito a través de los regímenes multilaterales de control de las exportaciones, si bien puede ser objeto de debate en las actividades de difusión.

La existencia de una "zona gris" compuesta por Estados que cumplen formalmente con las resoluciones del Consejo de Seguridad de la ONU, pero que no respetan otras medidas restrictivas (las impuestas por el G7, la Unión Europea –UE– y países afines) ni otras directrices para el control de las exportaciones, da pie a la actividad de redes de tráfico con ánimo de lucro –no necesariamente ilegales– que sacan partido de las lagunas de los regímenes sancionadores internacionales. Los países que sí respetan formalmente las medidas restrictivas y las directrices sobre el control de exportaciones,

pero sin contar con las herramientas jurídicas ni los conocimientos técnicos necesarios, pertenecen también a esta "zona gris".

El comercio mundial es el escenario en el que tienen lugar las transacciones preocupantes, las cuales afectan a países que no están comprometidos con el control de las exportaciones por tener opiniones distintas y divergentes o que no cuentan con la legislación ni las herramientas adecuadas para hacer frente a las cadenas de suministro ilícitas presentes en su territorio. La expansión de las restricciones a terceros países de la "zona gris" implicaría imponer restricciones a un mercado que representa la mitad del PIB mundial, con la consiguiente perturbación del comercio internacional.

Ambas cuestiones –las transferencias de riesgo en redes transnacionales de tráfico ilícito y las transferencias de tecnología en la "zona gris"– exigen una mayor atención por parte de los regímenes multilaterales de control de las exportaciones en el panorama internacional actual. Las estrategias de difusión deberían abordar estas cuestiones con el fin de buscar una fuente de legitimidad para las sanciones y los controles a la exportación, aumentar la creación de capacidades y ofrecer cadenas de suministro alternativas para las tecnologías esenciales.

Otros obstáculos para la eficacia de los controles a las exportaciones: tecnologías de doble uso, derivados y transferencias tecnológicas intangibles

A la hora de superar los obstáculos que se plantean para la eficacia de las medidas restrictivas en el ámbito tecnológico, deberán tenerse en cuenta algunos factores adicionales:

- El crecimiento de la demanda de tecnologías de doble uso. Es importante destacar que muchos de estos componentes tienen una finalidad civil y no están incluidos en las listas de sanciones o de control de las exportaciones al ser de uso común en la industria y estar presentes incluso en pequeños electrodomésticos.

- Lidiar con las tecnologías de doble uso no restringidas resulta problemático porque afecta al marco jurídico de las actividades empresariales. Los organismos nacionales de control de las exportaciones no cuentan con los medios jurídicos necesarios para actuar contra esta actividad comercial, ya que queda fuera del ámbito de aplicación actual de las reglamentaciones de control de las exportaciones. Hasta ahora, los controles a las exportaciones se han basado en el uso de "cláusulas genéricas" que permiten a las autoridades nacionales controlar cualquier producto no restringido cuando su exportación se considere contraria a los principios de no proliferación (teniendo en cuenta factores como la identidad del importador, el país de destino y un nuevo uso potencial del producto). Sin embargo, recurrir con frecuencia a esas cláusulas para los artículos no restringidos suscita controversia.

- Esas tecnologías de doble uso no restringidas pueden servir para modernizar sistemas militares existentes con aplicaciones novedosas o bien para fabricar nuevas. Un importador busca en el mercado tecnologías disponibles capaces de desempeñar una función que el usuario final haya determinado previamente como una necesidad. Muchas armas empleadas por agentes estatales y no estatales en contiendas asimétricas son el resultado de "ingeniería inversa" o se derivan de

procesos de “diseño inverso”. El proceso de adquisición de tecnologías sensibles al que recurren los agentes estatales y no estatales sometidos a sanciones suele comenzar con artículos comerciales disponibles que se compran en el mercado normal o en el mercado negro. A continuación, se desmontan estos artículos para crear réplicas o bien se rediseñan o modernizan recurriendo a otras tecnologías disponibles para producir derivados que se adapten a sus necesidades y recursos. Es posible que estos productos presenten un nivel tecnológico inferior y peores prestaciones que las del sistema original, pero acaban desempeñando una función similar.

- El uso de transferencias de tecnologías intangibles. Algunos de los riesgos descritos surgen también de las transferencias tecnológicas intangibles a raíz de las transferencias digitales y de las transferencias de datos técnicos en formato no físico. Las autoridades encargadas del control de las exportaciones en los países proveedores se enfrentan a escollos jurídicos y procedimentales para lidiar con las transferencias intangibles sensibles.[6]

Inversiones directas

Las inversiones directas en sectores estratégicos pueden dar pie a transferencias de tecnologías integradas en la cadena de suministro de los principales contratistas de artículos de defensa y de doble uso. Puede ocurrir por una inversión extranjera para la adquisición de una empresa nacional o bien por una inversión nacional en el extranjero en una actividad industrial deslocalizada en terceros países que no estén sujetos a las mismas normas de control de las exportaciones que debe respetar la sociedad matriz. Estas inversiones abren la puerta a riesgos de propagación tecnológica, con la consiguiente necesidad de contar con un inventario de esas empresas y de crear el marco jurídico adecuado para examinar las propuestas de adquisición presentadas por entidades extranjeras o la reubicación de actividades industriales en el extranjero. En cualquier caso, no resulta fácil controlar las tecnologías emergentes en estos procesos, ya que su desarrollo viene dado principalmente por el sector privado y evoluciona más rápido que el encaje legislativo de las inversiones estratégicas y, por lo tanto, en ocasiones escapa al control gubernamental. Estas limitaciones para el control se complican aún más por el hecho de que una gran parte de estas tecnologías consista en información digital que se puede transferir por medios intangibles. Se hace necesaria la coordinación internacional entre países afines.

Después de la Comunicación Conjunta de la Comisión Europea sobre una Estrategia Europea de Seguridad Económica (2023),[7] el Libro blanco sobre inversiones salientes (2024) de la Comisión incluye propuestas no vinculantes para impedir la filtración de

[6] La tecnología basada en la nube ha ido suscitando más interés y generando más inversiones gracias a su eficiencia en materia de gestión de servidores informáticos, redes y almacenamiento de datos. Sin embargo, el acceso no autorizado a estas nubes puede dar lugar a la transferencia ilegal de tecnologías a través de canales intangibles. Puede ocurrir por el robo o el desciframiento de contraseñas, o bien por la cooperación voluntaria de personal interno. Cabe señalar que en el ciberespacio no existen fronteras físicas y los controles aduaneros no se aplican en este ámbito.

[7] Comunicación Conjunta JOIN (2023) 20 final relativa a una “Estrategia Europea de Seguridad Económica”, 20/VI/2023.

tecnologías estratégicas.[8] En la misma línea, y de conformidad con la Orden ejecutiva sobre inversiones en determinadas tecnologías y productos de seguridad nacional en países preocupantes (2023) de Estados Unidos (EEUU), los inversores deben actuar con más cautela al invertir en países extranjeros específicos. El gobierno estadounidense regula ahora las inversiones nacionales en China, con especial hincapié en la salvaguardia de tecnologías importantes que resulten esenciales para la seguridad nacional. Como parte de esta misma iniciativa, el Departamento del Tesoro de EEUU y otras agencias aplicarán reglamentaciones que restringen las inversiones en determinados sectores clave de la economía china.[9]

Conclusiones

Los esfuerzos destinados hasta la fecha a mejorar los controles a las exportaciones se han centrado en tareas de gran importancia como efectuar un seguimiento de las tendencias tecnológicas, implicar a la industria y al mundo académico, acercarse a países no miembros y combatir el tráfico ilícito. Las dificultades descritas figuran desde hace muchos años en la agenda de los gobiernos que aplican las reglamentaciones de control de las exportaciones y las sanciones internacionales. He aquí algunos elementos de una estrategia común para mejorar su eficacia: concienciar a la industria y al mundo académico para convertirlos en la "primera línea de defensa", subsanar las carencias en cuanto a las herramientas jurídicas nacionales, aumentar los recursos de los organismos nacionales pertinentes e impulsar la cooperación internacional.

Concienciar a la industria y al mundo académico

Las relaciones entre los organismos públicos de control de las exportaciones, la industria y el mundo académico deberían evolucionar hacia un planteamiento de cooperación. La concienciación y la promoción de la autorregulación entre los proveedores de tecnologías sensibles y conocimientos técnicos los habilitará para formar parte de la "primera línea de defensa" de la seguridad nacional. Las empresas y los centros de investigación deben reforzar su política de conocimiento de los clientes (KYC) y la vigilancia de los usuarios finales para asegurarse de que sus productos no acaben empleándose de forma contraria a sus compromisos éticos y jurídicos, subsanando así las lagunas presentes en la legislación nacional. Los artículos de doble uso no restringidos que entren en la categoría de "tecnologías sensibles" suelen controlarse gracias a cláusulas genéricas que, pese a haberse diseñado para casos excepcionales, se emplean con frecuencia para abarcar una "zona gris" de las transacciones internacionales, con el riesgo que conlleva de generar incertidumbre jurídica entre las empresas proveedoras. Urge llevar a cabo una actualización del marco jurídico e incluir un enfoque que abarque las tecnologías de doble uso y los nuevos conceptos transaccionales, así como formación especializada para los investigadores que velan por el cumplimiento de la ley. También es necesario actualizar la legislación para abordar las tecnologías no restringidas con fuertes implicaciones militares y de seguridad, lo que incluye revisar las condiciones de deslocalización de la producción y

[8] Comunicación COM (2024) 24 final relativa al "Libro blanco sobre inversiones salientes", 24/I/2024.

[9] En estos sectores se incluyen los semiconductores y la microelectrónica, las tecnologías de información cuántica y las tecnologías que guarden relación con la inteligencia artificial. Véase Casa Blanca (2023), "Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern", Washington DC, 9/VIII/2023.

las cadenas de suministro. Asimismo, los legisladores y las fuerzas de seguridad deberán plantearse los parámetros de cumplimiento en un espacio intangible donde no cabe aplicar los controles aduaneros y coercitivos tradicionales. Las transferencias de tecnologías intangibles exigen aplicar un nuevo enfoque para afrontar los retos que plantean para el control de las exportaciones, como se aprecia en las transacciones de información sensible en las que el concepto de frontera nacional se difumina o, directamente, desaparece.

Aumentar los recursos de los organismos nacionales pertinentes

En muchos casos, los órganos administrativos encargados del control de las exportaciones en los países proveedores no cuentan con recursos acordes con la complejidad de los regímenes sancionadores ni con el número cada vez mayor de transacciones sensibles. El volumen de trabajo de estas transacciones no hace más que aumentar, así como el número de tecnologías sensibles en potencia, hasta salirse del ámbito de actuación jurídico original de estos organismos en su condición de órganos administrativos, debido a la demanda creciente de artículos de doble uso. Sin embargo, los recursos humanos y financieros de estos organismos no crecen al mismo ritmo. Estos retos exigen contar con nuevas herramientas y recursos adicionales para los organismos de control de las exportaciones y las fuerzas del orden, como por ejemplo marcos jurídicos nacionales para técnicas especiales de investigación en la red con el fin de llevar a cabo un seguimiento de las transferencias electrónicas de información sensible, siempre bajo supervisión judicial y de conformidad con la legislación nacional.

Cooperación internacional

Por último, la propagación geográfica de las transacciones transnacionales y la creciente complejidad de las redes de tráfico ilícito en la “zona gris” exigen revisar y evaluar las políticas de membresía, difusión y compromiso en los regímenes multilaterales de control de las exportaciones, así como incrementar la cooperación internacional entre gobiernos afines. Esa idea abre la puerta a otra cuestión fundamental en este ámbito: la participación de los no miembros en las políticas de control de las exportaciones.