China, 5G y la Seguridad de la Alianza más allá de las cumbres 2021/22 de la OTAN

Este resumen presenta los puntos clave discutidos en la mesa redonda organizada por GMF y mantenida debajo la regla de Chatham House, que reunió a expertos de Europa y Estados Unidos para explorar cómo se estaban abordando cuestiones generales sobre China, 5G, resiliencia e infraestructura crítica en el contexto de la OTAN. La mesa redonda tuvo lugar en 2021 pero las conclusiones y el análisis se actualizaron tras la invasión de Ucrania y la cumbre de la OTAN 2022 en Madrid.

- La invasión de Rusia a Ucrania subraya el rol indispensable de la OTAN para la seguridad de los aliados europeos, mientras que el anuncio de China de una asociación "sin límites" con Rusia ha demostrado el espectro de amenazas más amplio que la OTAN debe tener en cuenta ahora. Esto refuerza el imperativo de asegurar que la OTAN esté bien adaptada a todas las dimensiones del nuevo entorno de seguridad que enfrenta.
- A partir del principal trío de cumbres realizado durante la visita del presidente Joe Biden a Europa durante el verano de 2021 y la cumbre de Madrid de 2022, ha quedado claro que China ocupará un rol central en la relación transatlántica durante los próximos años. China ahora cruza la agenda de la OTAN de varias maneras, y ocupa una parte del debate mucho más atrincherada que nunca. Si bien la OTAN no está en conflicto militar con China, China sigue siendo un competidor geopolítico clave para la totalidad de Occidente. Más aún, Estados Unidos considera a China como una amenaza directa a la seguridad nacional y hay varias contingencias plausibles que podrían llevar a ambas partes a una confrontación militar. Aunque pueda haber distintas opiniones en Europa sobre este asunto, los aliados europeos en la OTAN han asumido tradicionalmente parte de la agenda de seguridad y defensa de Estados Unidos a cambio de garantías de seguridad. Sin embargo, China también presenta un conjunto de riesgos de seguridad estrictamente europeos. Una cuestión en particular se relaciona con la resiliencia e infraestructura crítica, dada la considerable dependencia de la infraestructura digital de Europa con la tecnología china. El debate actual es acerca de si la OTAN es la plataforma óptima para abordar esos asuntos, si, en cambio, la UE debería asumir un rol más activo, o si hay una adecuada división de responsabilidades entre ellas.
- La OTAN ha identificado a las telecomunicaciones como una nueva área de enfoque. Para cumplir su misión clave de defensa colectiva, la OTAN necesita una infraestructura más fuerte para soportar las interferencias híbridas. Sin embargo, en la mayoría de los países europeos, la infraestructura es de propiedad privada. Esto la hace susceptible a interferencias externas e impulsa decisiones económicas que pueden descuidar los aspectos de la seguridad nacional, si no están claramente regulados por la ley. Rusia es un actor estatal que recurre a varios tipos de tácticas híbridas en el territorio de la OTAN. Sin embargo, China también comenzó a usar varias tácticas sofisticadas, políticas y no militares, contra la OTAN en general y contra países individuales, para extender su influencia política y económica.
- Para que la resiliencia sea el catalizador de una cooperación OTAN-UE más estrecha, se debe hallar un equilibrio en el que queden explícitamente definidos los roles de ambas organizaciones. Actualmente, la OTAN está adoptando un marco más robusto, incluso en la dimensión no militar. La OTAN se ocupa principalmente de coordinación y consultas políticas, la administración de crisis y la defensa colectiva, así como de la interoperabilidad. Por otra parte, la UE tiene una gama de instrumentos regulatorios a su disposición, desde la Caja de herramientas 5G hasta el Plan de Acción de la Democracia Europea, que aborda algunos de los problemas de resiliencia más amplios. Por lo tanto, se deberían determinar las responsabilidades compartidas y coincidentes de la UE y la OTAN,

y establecer vínculos más estrechos entre la tradicional planificación de capacidades militares, y se deberían establecer requisitos de resiliencia, ya que esto será uno de los pilares clave para el futuro de la cooperación entre la OTAN y la UE.

- Es todavía incierto si la protección de la infraestructura civil de Europa debería caer bajo el alcance de la OTAN. En otras palabras, ¿un ciberataque a infraestructura civil de Europa activaría el Artículo Cinco? Si no fuera así, ¿eso sería competencia de la UE? Además, los límites entre la infraestructura civil y la infraestructura militar son borrosos, especialmente cuando se trata de las telecomunicaciones.

- Las telecomunicaciones están asumiendo cada vez más importancia para el funcionamiento de nuestras sociedades y economías, así como proveyendo las bases y el futuro de la innovación. Estas dos dimensiones están vinculadas subsiguientemente en la carrera por la supremacía tecnológica. La tecnología ha sido, y será, la llave para la disuasión y la defensa. El dominio tecnológico garantiza no solo la supremacía en el campo de batalla, sino también la supremacía más allá del mismo. Tal dominancia es contingente con una base industrial robusta y en continuo progreso que integre la innovación, investigación y desarrollo de los sectores civil y militar. Se necesitan iniciativas de innovación conjuntas a través del Atlántico para mantener y intensificar las capacidades críticas dentro y fuera del campo de batalla. Esto requiere vínculos mejores y más eficientes entre las industrias civiles y militares. La OTAN necesita encontrar maneras inteligentes de integrar las dimensiones económicas que apuntalan los elementos de sus políticas de seguridad, particularmente a medida que la estrategia industrial vuelve a ocupar el primer plano del pensamiento en Europa y los Estados Unidos. Se deben construir nuevos canales políticos para facilitar dicha integración y fortalecer la resiliencia de la alianza, así como mantener su ventaja competitiva.

- Por ahora, parecería que la OTAN se está esforzando con este rol. Es por eso que se necesita precisión para identificar y categorizar los problemas que quedan bajo su alcance. Un primer paso para los políticos es establecer parámetros claros en áreas en las cuales hacer negocios con China no significaría comprometer la seguridad nacional. La OTAN es también una plataforma natural para mantener intercambios de seguridad con varias instituciones, entidades no estatales y socios de la OTAN que tenga experiencia en tratar con China, como Japón y Corea del Sur. Por lo tanto, la OTAN debería continuar priorizando la infraestructura digital (5G/avanzada, cable submarino, etc.) y China, manteniendo ambos en los primeros lugares de su agenda.

- Dado que las amenazas cibernéticas han sido un área de preocupación de la OTAN desde hace tiempo, las redes 5G se han convertido naturalmente en un foco para los debates de la OTAN – aunque sus aspectos de defensa se han ido incorporando lentamente en la agenda. Además, la manera en que la información se procesa y almacena es un área de seguridad clave que no debe convertirse en un punto ciego. Proteger a nuestro sector público y a nuestras industrias, junto con asegurar que las empresas, ciudadanos e instituciones gubernamentales tengan la posibilidad de enviar su tráfico de manera integral a una red que no sea china, está en el centro de este asunto. En 5G, por ejemplo, la infraestructura desempeñará un rol significativo. Bajo la legislación china, el gobierno chino puede solicitar y obtener acceso a la información de cualquier empresa privada de China, poniendo en riesgo toda la información de una nube 5G china. Para tomar el ejemplo de Bélgica, toda su infraestructura de telecomunicaciones se apoyaba previamente en equipos chinos, incluso en las comunicaciones móviles usadas por las administraciones de la UE y la OTAN. De manera similar, los equipos chinos forman parte de las redes de Alemania; lo que significa que el tráfico móvil de todas las tropas de la OTAN basadas en Alemania pasan, en algún punto, a través de redes basadas en tecnología china. La nueva ley de Seguridad de TI de Alemania se refiere correctamente a las necesidades de seguridad de la OTAN cuando se trata de la evaluación de la integridad de los proveedores. También muestra que las ambiciones y la implementación pueden diferenciarse considerablemente: desde que la ley entró en vigencia el año pasado, la participación de Huawei en la red 5G de Deutsche Telekom (DT) ha crecido muy por arriba del 60 %. En 2020, la nube de DT, construida y operada por Huawei, tiene al Centro de Investigaciones Nucleares (CERN, por sus siglas en inglés) de Suiza, como un cliente de referencia clave desde su lanzamiento. En

otras palabras, el principal centro de investigación nuclear almacena su información en una nube china. Por lo tanto, es un requisito mínimo que las redes que cumplen funciones para las redes gubernamentales, la industria de la defensa y la seguridad interna, no dependan en equipos chinos. Más allá de ello, las redes que cumplen funciones críticas para la sociedad, como el sector de servicios públicos y el sector farmacéutico, el cuidado de la salud, la banca o el transporte y las comunicaciones, deberían adoptar medidas similares para evitar estar comprometidos.

- Los aliados de la OTAN en Europa oriental han sido hasta ahora recelosos a incrementar la atención de la OTAN sobre China, preocupados por una distracción indebida de la amenaza que significa Rusia. Las últimas semanas han demostrado que la OTAN debe hacer ambas cosas: tratar con las amenazas de Rusia y de China – en realidad, ambas están entrelazadas. La guerra contra Ucrania ha demostrado drásticamente el peligro inmediato de agresión de parte del régimen ruso. Por otra parte, los vínculos más estrechos que nunca de China con Rusia, su apoyo explícito a la postura de Rusia con respecto a la OTAN, la total implementación de sus canales de propaganda a favor de las posiciones de Moscú, y la posibilidad latente de que Beijing pueda intervenir con apoyo económico – o incluso transferencias de armas – subrayan que la cooperación chino-rusa "sin límites" significa básicamente cooperación contra Occidente. La OTAN debe tener en cuenta que las capacidades conjuntas chino-rusas pueden ser dirigidas hacia objetivos rusos en Europa, objetivos chinos en Asia y objetivos conjuntos en cualquier otro lugar.
- Esto originará un drástico incremento de los riesgos de seguridad generados por los equipos de telecomunicaciones chinos en las redes de los aliados de Europa central y occidental. A medida que la OTAN incrementa sus capacidades de defensa militar en su frontera oriental ante la amenaza de Rusia, las redes de telecomunicaciones de Polonia, Rumania y otros países todavía dependen en gran medida de equipos chinos. En realidad, ninguno de estos países garantiza la eliminación de proveedores no dignos de confianza en los próximos años. Las reglas más estrictas limitan la introducción de más equipos chinos, pero aceptan el riesgo de equipos existentes no fiables hasta mediados de la década y más allá; un enfoque difícilmente aceptable. La posibilidad de que China, en caso de un conflicto, pudiera dar a Rusia acceso a, por ej.: las redes de telecomunicaciones polacas a través de Huawei o ZTE es real y de consecuencias dramáticas.
- El coste de reemplazar la infraestructura china de las empresas de telecomunicaciones en Europa no sería prohibitivo: a medida que las operadoras pasan de 4G a 5G, todos sus equipos más antiguos serán reemplazados de todas maneras. Por lo tanto, una prohibición total de nuevos equipos de Huawei en Europa podría tardar "naturalmente" unos seis años antes de que se llegue a eliminar la base instalada no fiable. La cuestión es asegurar una transición más rápida a tecnología fiable en términos de seguridad nacional, en la que las consideraciones comerciales a corto plazo referidas a los plazos de sustitución de equipos no sean las que marquen el ritmo. Otro mito recurrente es que los proveedores chinos están más avanzados tecnológicamente que los proveedores europeos. A los Estados Unidos y Corea del Sur se los considera líderes en el lanzamiento de las redes 5G; su infraestructura ha sido implementada sin recurrir a ningún equipo chino, ya que mayoritariamente dependen de tecnología europea. En cuanto a los precios, los proveedores europeos también pueden competir con sus competidores chinos; pero no pueden competir con el estado chino. Los subsidios de China a las empresas de origen nacional que operan en mercados globales, así como la preferencia por empresas chinas en su mercado doméstico, sigue distorsionando el campo de juego. El problema es más agudo para las operadoras más pequeñas de toda Europa, América latina y Asia, que tienen calificaciones crediticias más débiles y se ven obligadas a recurrir a préstamos chinos a menos que se les ofrezcan mecanismos alternativos de financiamiento. Un enfoque que se está sugiriendo como una alternativa es Open-RAN. Sin embargo, en la práctica, la presencia e influencia china en sus estructuras de desarrollo debe plantear preguntas y requiere una evaluación integral de riesgos.
- La Caja de Herramientas para 5G de la UE es un buen punto de partida para avanzar. Sin embargo, su naturaleza no obligatoria permite que los miembros de la UE tengan diferentes interpretaciones e implementaciones, y esto crea vulnerabilidades. Un paso

concreto hacia adelante sería asegurar una implementación más estricta de la caja de herramientas en toda la UE. De todas maneras, la Caja de Herramientas para 5G de la UE solo puede ser un punto de partida. Las redes que conectan activos críticos mediante fibra óptica, transporte y cables submarinos requieren el mismo escrutinio y la estricta implementación de salvaguardas que el acceso por radio y la red del núcleo central. El desarrollo conjunto de cajas de herramientas para estos perímetros de redes podría ser una opción.

- Si bien se adoptó un lenguaje sutil en las cumbres de OTAN 2021/2, los aliados han concordado en que el comportamiento de China interfiere con nuestros principios democráticos y seguridad nacional. Por lo tanto, el reto sistémico que plantea China se ha convertido en un artículo clave de la agenda de la OTAN y es amplificado por la intensificación de la colaboración ruso-china. La política de la alianza hacia China se ha solidificada en el Concepto Estratégico, que se ha adoptado en la cumbre de Madrid. El aspecto desafiante para la OTAN será abordar las numerosas y diversas amenazas de seguridad actuales a la vez; disuasión híbrida, tecnologías disruptivas y emergentes, e infraestructura crítica vulnerable. Debido al panorama de seguridad rápidamente cambiante y al rápido desarrollo de la tecnología, lograr superarse en todos los frentes será crucial para el éxito continuo de la OTAN.