Màster en Relacions Internacionals Seguretat i Desenvolupament (MURISD)

Ciberseguridad y redes 5G en las relaciones internacionales: el caso de Huawei

Autora: Mireia Martín Porras

Tutora: Nora Sainz Gsell

Treballs de màster i postgrau. Màster en Relacions Internacionals, Seguretat i Desenvolupament (MURISD). Curs 2021/2022

Universitat Autònoma de Barcelona

Treballs de màster i postgrau. Màster en Relacions Internacionals, Seguretat i desenvolupament (MURISD). Curs 2021/2022

http://murisd.uab.cat

Coordinador de la col·lecció: Dr. Rafael Grasa Hernández, Rafael.Grasa@uab.cat.

Aquesta col·lecció recull una selecció de treballs duts a terme pels estudiants del Màster Universitari en Relacions Internacionals, Seguretat i Desenvolpament. Els treballs es publiquen en algunes de les tres llengües del màster, català, castellà i anglès

Esta colección recoge una selección de trabajos realizados por estudiantes del Máster Universitario en Relaciones Internacionales, Seguridad y Desarrollo. Los trabajos se publican en algunas de las tres lenguas del máster, catalán, castellano y inglés

This collection includes a selection of research by students of Master's Degree in International Relations, Security and Development. These researches are published in any of the three languages of the master's degree, catalan, spanish and english

RESUMEN: La creciente importancia de los actores transnacionales a escala mundial ha convertido a las empresas en actores clave en las relaciones internacionales. Asimismo, el desarrollo tecnológico ha introducido nuevos retos y amenazas en la ejecución de la acción exterior. El presente trabajo investiga estas dos nuevas realidades, centradas en el caso de Huawei, una empresa china acusada por Estados Unidos de ciberespionaje a través de las redes 5G. Este estudiose propone descubrir los objetivos subyacentes de la acusación mediante el análisis económico de Huawei y las estadounidenses Intel y Qualcomm. Además, reúne información sobre el contexto de este conflicto y las medidas adoptadas por Australia, Nueva Zelanda, el Reino Unido, Canadá y la Unión Europea.

PALABRAS CLAVE: Geopolítica, Ciberseguridad, Actor transnacional, 5G, Huawei, Estados Unidos

ABSTRACT: As non-state actors are becoming increasingly important worldwide, business companies seem to have established themselves as key actors in international relations. Moreover, emerging technological developments have posed new challenges and threats to the enforcement of external action. This paper investigates these two new realities, focusing on the case of Huawei, a Chinese company accused by the United States of cyber espionage using 5G networks. This study aims to uncover the underlying objectives of the accusation through an economic analysis of Huawei and the US companies Intel and Qualcomm. Furthermore, it gathers information on the context of this conflict and the measures taken by Australia, New Zealand, the United Kingdom, Canada, and the European Union.

KEYWORDS: Geopolitics, Cybersecurity, Non-state actor, 5G, Huawei, United State

Universitat Autònoma de Barcelona

MÁSTER UNIVERSITARIO EN RELACIONES INTERNACIONALES, SEGURIDAD Y DESARROLLO

CIBERSEGURIDAD Y REDES 5G EN LAS RELACIONES INTERNACIONALES: EL CASO DE HUAWEI

AUTORA:

Mireia Martín Porras

TUTORA:

Nora Sainz Gsell

Convocatoria: Julio 2022

4 de julio de 2022

Declaro, con mi firma al pie, que el presente trabajo es original y que no contiene plagios o usos indebidos de otras fuentes y acepto las consecuencias que podría tener contravenir el presente compromiso.

Firma

RESUMEN

La creciente importancia de los actores transnacionales a escala mundial ha convertido a las empresas en actores clave en las relaciones internacionales. Asimismo, el desarrollo tecnológico ha introducido nuevos retos y amenazas en la ejecución de la acción exterior. El presente trabajo investiga estas dos nuevas realidades, centradas en el caso de Huawei, una empresa china acusada por Estados Unidos de ciberespionaje a través de las redes 5G. Este estudio se propone descubrir los objetivos subyacentes de la acusación mediante el análisis económico de Huawei y las estadounidenses Intel y Qualcomm. Además, reúne información sobre el contexto de este conflicto y las medidas adoptadas por Australia, Nueva Zelanda, el Reino Unido, Canadá y la Unión Europea.

Palabras clave: geopolítica, ciberseguridad, actor transnacional, 5G, Huawei, Estados Unidos

ABSTRACT

As non-state actors are becoming increasingly important worldwide, business companies seem to have established themselves as key actors in international relations. Moreover, emerging technological developments have posed new challenges and threats to the enforcement of external action. This paper investigates these two new realities, focusing on the case of Huawei, a Chinese company accused by the United States of cyber espionage using 5G networks. This study aims to uncover the underlying objectives of the accusation through an economic analysis of Huawei and the US companies Intel and Qualcomm. Furthermore, it gathers information on the context of this conflict and the measures taken by Australia, New Zealand, the United Kingdom, Canada, and the European Union.

Key words: geopolitics, cybersecurity, non-state actor, 5G, Huawei, United States

TABLA DE CONTENIDO

1. INTRODUCCIÓN **1**
   1.1. OBJETO DE ESTUDIO Y OBJETIVOS 1
   1.2. PREGUNTAS Y METODOLOGÍA 2
   1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN E HIPÓTESIS 2
2. ESTADO DE LA CUESTIÓN **3**
   2.1. DEFINICIONES 3
   2.2. CONTEXTO 6
   2.3. DELIMITACIÓN DEL CONFLICTO 9
3. POSICIONAMIENTO DE LOS ACTORES **11**
   3.1. AUSTRALIA 11
   3.2. NUEVA ZELANDA 12
   3.3. REINO UNIDO 12
   3.4. CANADÁ 13
   3.5. UNIÓN EUROPEA 14
4. ANÁLISIS ECONÓMICO **17**
   4.1. HUAWEI 18
   4.2. INTEL 19
   4.3. QUALCOMM 21
5. CONCLUSIONES **23**
6. BIBLIOGRAFÍA **24**
7. ANEXOS **29**
   7.1. ANEXO I 29

1. INTRODUCCIÓN

La era digital ha supuesto enormes facilidades en la vida cotidiana y avances en diferentes áreas de conocimiento. En 2019, el 56,7% de la población mundial utilizaba internet y en 2020 ya se contaba con 89 189 073 servidores de internet seguros (Banco Mundial, 2022). Sin embargo, la digitalización también ha supuesto la creación de nuevos peligros. Como explican Arcinegas y Corzo (2021), la aceleración del cambio tecnológico ha revolucionado la forma en que se desenvuelven las guerras, al crearse ataques, protecciones y estrategias en espacios tales como el cibernético.

El presente trabajo aborda la ciberseguridad en las relaciones internacionales. De manera más precisa, el tema de estudio es la gestión de las amenazas en el ciberespacio a partir del desarrollo de las redes 5G. La incipiente amenaza de la ciberguerra y la invasión de la privacidad de los usuarios han llevado a la comunidad internacional a adaptarse a la era digital a través de nuevas cláusulas, políticas, sanciones, reglamentos y decisiones para garantizar la seguridad en este ámbito.

1.1. OBJETO DE ESTUDIO Y OBJETIVOS

La revolución tecnológica ha suscitado varios debates, entre ellos, el relacionado con la acusación de Estados Unidos (en adelante, EE. UU.[1]) a Huawei Technologies Co., Ltd. (en adelante, Huawei) de ciberespionaje. La acusación se basa en el presunto mal uso de las redes 5G a través del acceso a secretos estatales, datos de los usuarios y otra información confidencial. Este TFM estudia la reacción de Australia, Nueva Zelanda, el Reino Unido, Canadá y la Unión Europea (en adelante, UE) y las consecuencias de las medidas adoptadas al respecto. A partir de la creciente importancia de los actores transnacionales en la actualidad, el estudio observa los efectos del veto estadounidense a Huawei en las empresas de telecomunicaciones de la República Popular China (en adelante, China) y EE. UU. El objeto de estudio de este trabajo es el impacto de las decisiones de cinco actores internacionales en la economía china y estadounidense ante la acusación a Huawei de ciberespionaje.

Dado que la crisis de Huawei tiene sus inicios en 2018, el trabajo estudia esta situación entre 2017 y 2020, para hacer un análisis comparativo entre la situación económica de las empresas antes y después del nacimiento del debate sobre las tecnologías de quinta generación (5G). El tema seleccionado es muy acotado, al estar centrado en la empresa china Huawei, y reciente, por lo que reúne información todavía no muy tratada en la literatura sobre relaciones internacionales.

Este estudio persigue tres objetivos. En primer lugar, reunir y aportar información contextual y teórica sobre el 5G, el ciberespionaje, la ciberseguridad y Huawei. En segundo lugar, investigar el posicionamiento de diferentes actores internacionales ante la acusación estadounidense de ciberespionaje a Huawei y evaluar las medidas consecuentes. En tercer lugar, comparar los efectos de las decisiones de los diferentes actores en las empresas de telecomunicaciones chinas y estadounidenses. Para obtener un análisis

[1] El presente trabajo sigue la recomendación de Fundéu y el Diccionario panhispánico de dudas referente a la abreviatura de los Estados Unidos, por las que aceptan las formas «EE. UU.» y «EUA», disponible en: https://www.fundeu.es/recomendacion/ee-uu-eua-usa-us/

riguroso de los efectos económicos en estas empresas, el trabajo compara la situación económica en 2017, antes de la crisis de Huawei, y en 2020, después de que surgiera el debate sobre las redes 5G.

1.2. PREGUNTAS Y METODOLOGÍA

Las preguntas planteadas en el presente trabajo guían el estudio a través de los objetivos detallados anteriormente. Las preguntas son las siguientes:

- ¿Cómo perciben las redes 5G, el ciberespionaje y la ciberseguridad los diferentes actores implicados en el caso de estudio?
- ¿Por qué Huawei tiene un papel tan destacado en temas de ciberseguridad y 5G?
- ¿Qué actores han tomado medidas contra Huawei a partir de la acusación estadounidense de ciberespionaje? ¿Qué medidas han tomado?
- ¿Qué consecuencias han tenido las medidas adoptadas contra Huawei?
- ¿Cómo se han visto afectadas las empresas de telecomunicaciones estadounidenses?

El trabajo es aplicado, más concretamente, es un análisis del objeto mencionado, ya que define el estado de la cuestión, investiga las posiciones de los actores implicados y evalúa el impacto de las consecuencias, entre otros aspectos. La información tratada en este trabajo proviene de fuentes primarias y secundarias. Por un lado, entre las fuentes primarias, destacan diferentes informes anuales, normativas, leyes y decisiones. Por otro lado, en cuanto a las fuentes secundarias, se trata principalmente de artículos académicos sobre relaciones internacionales. La pauta de análisis con la que se aborda el tema es la siguiente:

1. Estado de la cuestión: Aproximación contextual y temática desde 2017 hasta 2020.
2. Posicionamientos y decisiones: Análisis de las medidas adoptadas contra Huawei por los diferentes actores clave.
3. Consecuencias: Evaluación del impacto económico de las decisiones y análisis comparativo temporal de las empresas de telecomunicaciones chinas y estadounidenses.

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN E HIPÓTESIS

Este trabajo resulta muy pertinente porque estudia un tema reciente del cual todavía no existe abundante literatura académica. Además, se centra particularmente en el caso de la empresa china Huawei, con la finalidad de recoger información de la manera más precisa y acotada posible. El análisis comparativo del estado de la cuestión antes y después de los sucesos clave también aporta datos significativos y relevantes para el estudio, destinado al sector privado e instituciones del sector público, como empresas multinacionales y ministerios.

Varios estudios recientes plantean que Huawei no es el único actor transnacional que emplea las redes 5G para obtener datos confidenciales. Sin embargo, este planteamiento es un interrogante todavía pendiente de resolver. Algunos expertos en

relaciones internacionales aseguran que «el ciberespionaje no es una acción que se contemple de forma aislada en China; sino que es una práctica común en países imperialistas lo que produce que, en general, los usuarios de internet estemos subordinados al Big Data (Salazar, 2020, p. 50)»[2]. Por este motivo, la hipótesis que presenta el TFM es que la acusación estadounidense de ciberespionaje a Huawei persigue objetivos que van más allá de la protección de la seguridad en las redes y que están centrados en la rivalidad actual con China por la hegemonía mundial. Parece ser que EE. UU. acusó estratégicamente a Huawei con el fin de frenar los avances de esta empresa en el desarrollo del 5G y atraer a sus clientes hacia empresas de telecomunicaciones estadounidenses, como Intel Corporation (en adelante, Intel) y Qualcomm Incorporated (en adelante, Qualcomm), para incrementar el poder económico del país.

2. ESTADO DE LA CUESTIÓN

Este apartado reúne información contextual e histórica del tema de estudio, puesto que aporta datos y definiciones clave para entender el conflicto tratado en el trabajo. Por una parte, la apreciación y definición de la terminología depende del actor que la utiliza, por lo que este apartado recoge y explica siete términos clave cuya definición varía en función del emisor. Por otra parte, resulta esencial investigar y comprender el contexto del caso Huawei para poder evaluar de manera correcta el impacto de las medidas consecuentes.

2.1. DEFINICIONES

Algunos de los términos más destacados al tratar temas vinculados a la ciberseguridad en las relaciones internacionales son el ciberespionaje, el ciberdelito, la geopolítica, los actores transnacionales, las redes 5G y, en el caso particular de este trabajo, la empresa Huawei. A continuación, se analizan las similitudes y diferencias semánticas de los conceptos mencionados para los actores internacionales más relevantes para este caso. Además, se detalla el significado de dichos términos para este estudio.

En lo referente al **ciberespionaje**, China lo percibe como el acceso ilegal a información del conjunto de la nación, formada por ciudadanos, gobierno e incluso empresas, como se explica en el *Reglamento de medidas de seguridad contra el espionaje*[3] del Ministerio de Seguridad de China. En lo que concierne a EE. UU., como se observa en el discurso del 19 de julio de 2021 de Antony Blinken, vicesecretario de Estado, ese país tiene una visión centrada en el aspecto gubernamental e incluso militar del ciberespionaje, concebido principalmente como intrusiones en sistemas de información del estado. En cuanto a la UE, la nueva Brújula Estratégica relaciona este término con la protección de los ciudadanos, es decir, la información de los usuarios. La definición de este concepto no es universal, puesto que existen diferencias en cuanto a la

[2] Este trabajo sigue la recomendación de Fundéu y el Diccionario panhispánico de dudas referente al uso de las comillas latinas (« ») en la reproducción de citas textuales cortas (menos de 40 palabras), disponible en: https://www.fundeu.es/recomendacion/comillas-uso-de-este-signo-ortografico/

[3] Las traducciones del chino al español y del inglés al español incluidas en el cuerpo y la bibliografía de este trabajo han sido realizadas por la autora.

afectación de esta práctica. Este estudio entiende por ciberespionaje el acceso a información privada y la toma de control de cuentas de todos los usuarios de internet, tanto a nivel particular como gubernamental y empresarial.

En segundo lugar, la **ciberseguridad** es interpretada por China, según la *Ley de Seguridad de las Redes*, como la protección de la seguridad en internet, la soberanía del ciberespacio, la seguridad nacional y los derechos e intereses legítimos de los ciudadanos. Según el Buró Federal de Investigaciones (FBI, por sus siglas en inglés) de EE. UU., este concepto se ve reflejado en el robo de información y dinero, que puede afectar a la economía y los servicios de los que dependen la vida de los ciudadanos. Otros actores, como la UE en su estrategia digital, consideran que la ciberseguridad se ve comprometida por el espionaje y el robo de datos de los usuarios. En este caso, las diferencias en la apreciación del concepto recaen en las amenazas que comprometen la ciberseguridad. En este trabajo se entiende por ciberseguridad el control de amenazas en el espacio cibernético, ya sea en el campo de la privacidad de los usuarios, como el económico, financiero y militar, entre otros.

En cuanto al **ciberdelito**, ciertas fuentes de diversas organizaciones internacionales, como la página web sobre cibercrimen de la Oficina de las Naciones Unidas (en adelante, ONU) contra la Droga y el Delito, la página oficial de la Organización del Tratado Atlántico Norte (OTAN) sobre ciberdefensa, el lugar web de la Secretaría de la Organización para la Seguridad y la Cooperación en Europa (OSCE) sobre ciberseguridad y el periódico vietnamita *Nhan Dan* sobre la Asociación de Naciones de Asia Sudoriental (ASEAN) emplean definiciones muy amplias de este término centradas en el fortalecimiento, la respuesta conjunta y el desarrollo de estas organizaciones ante dicha amenaza. Sin embargo, la UE, una organización internacional *sui generis*, responsabiliza en la página web de la Comisión Europea a hackers individuales, grupos de hackers o incluso estados de este delito, una acción que, para esta organización, no solo se dirige a ordenadores personales, sino a redes enteras de comunicación. En lo referente a los estados, China relaciona la ciberdelincuencia con organizaciones, proveedores de servicios de red, empresas, instituciones y actores individuales en la *Decisión del Comité Permanente de la Asamblea Popular Nacional relativa al fortalecimiento de la protección de la información en Internet*. EE. UU., a través de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA, por sus siglas en inglés), señala a delincuentes y estados-nación. En este caso, existen diferencias semánticas en cuanto a los responsables del uso ilegal del espacio cibernético. El ciberdelito es concebido aquí como el uso ilegal de las redes por parte de cualquier individuo u organización, por lo que engloba el acceso a información confidencial, la distribución de datos personales y la manipulación de sistemas informáticos, entre otros. En el caso particular de EE. UU., el término se inscribe en el concepto «crimen transnacional organizado», lo cual enlaza con el siguiente término a tratar.

El concepto **«actor transnacional»** ha sido foco de enormes debates en el estudio de las relaciones internacionales. Grandes expertos en la materia, como Keohane, Nye, Morgenthau, Merle, y Mansbach han tratado de definirlo según las diferentes corrientes de pensamiento de la disciplina. En lo referente a este término, el Consejo Nacional de Inteligencia de EE. UU. lo define como entidades soberanas que ejercen un importante

poder e influencia económica, política y social a nivel nacional y, en algunos casos, internacional. Principalmente, destaca empresas multinacionales, organizaciones no gubernamentales (ONG) e, incluso, individuos particulares con gran poder. En el caso de las organizaciones internacionales, el Tribunal de Cuentas Europeo y el comunicado de prensa de la ONU del 21 de junio de 2004, están de acuerdo con los ejemplos aportados por EE. UU., a los que añaden *think tanks* como actores transnacionales. Además, estas organizaciones destacan su creciente importancia en los últimos años. China, en la entrada del buscador chino Baidu sobre actores transnacionales, también destaca el momento de auge que caracteriza a este tipo de entidades, apreciadas como actores no vinculados al estado pero que afectan a su acción exterior. En línea con lo dispuesto, este trabajo identifica un actor transnacional como cualquier tipo de ente no estatal con capacidad de influir en el ámbito internacional.

Por lo que concierne a la **geopolítica**, se trata de un concepto particularmente destacable en cuanto a la variedad semántica en función del emisor. Algunas organizaciones internacionales, como la ONU en un estudio del Centro de Investigación de Políticas de la Universidad de las Naciones Unidas (UNU-CPR, por sus siglas en inglés), tienen un concepto muy amplio de este término, que se limita principalmente a las relaciones entre estados. Para otras, como la UE en la página web de la Comisión Europea, la geopolítica se vincula con el nivel de poder y proyección alcanzado a escala internacional. En cuanto a los actores estatales, EE. UU., según el discurso del 3 de marzo de 2021 de Antony Blinken, lo considera primordialmente una rivalidad entre estados, mientras que China, en las *Medidas de control de seguridad de las redes* del Ministerio de Seguridad, utiliza este término como el análisis y predicción estratégica del comportamiento de los estados. Este trabajo entiende por geopolítica el uso estratégico de la situación geográfica y las esferas de influencia en las relaciones entre estados.

Con respecto a las **redes 5G**, el análisis semántico no se centra tanto en la comparación entre actores, sino en la definición de un concepto que se aleja del ámbito de las relaciones internacionales. La página web de la CISA sobre redes 5G y el artículo del 14 de julio de 2021 del Consejo de Estado de China sobre este mismo asunto lo perciben como una transformación integral de las redes de telecomunicaciones que impulsa el desarrollo industrial, económico y social. Este término se aprecia aquí como un avance tecnológico que supone una mayor velocidad en línea y permite el desarrollo de nuevas utilidades. Este estudio, así como también EE. UU. y China, sigue la definición de Carmona (2020, p. 4), quien explica que:

> El 1G permitió el uso de teléfonos móviles, el 2G los mensajes de texto, el 3G llevó internet al móvil, y el 4G permite el *streaming* de audio y video. El 5G, por su parte, no solo aumentará la velocidad de descarga, sino que servirá también para que más dispositivos estén conectados a la vez, abriendo la puerta a un gran

> número de industrias como las *smart cities*, los coches sin conductor o el Internet de las cosas (IoT, por sus siglas en inglés)[4].

Por último, se analiza la naturaleza de la empresa **Huawei** y su importancia en el desarrollo del 5G. Huawei (s.f.), fundada en China en 1987, asegura ser «un proveedor líder mundial de infraestructuras de tecnologías de la información y la comunicación (TIC) y de dispositivos inteligentes». Según el Departamento de Justicia de los EE. UU., se trata del mayor fabricante de equipos de telecomunicaciones del mundo. Huawei recalca de manera pública su estatus de empresa privada, dados los rumores de asociación con el gobierno chino. Estas acusaciones se basan en que el fundador y actual presidente de la empresa, Ren Zhengfei, es un exoficial del Ejército Popular de Liberación (EPL), las fuerzas armadas de China. La empresa afirma que:

> Ninguna agencia gubernamental u organización externa posee acciones de Huawei [...]. Contamos con aproximadamente 197 000 empleados y operamos en más de 170 países y regiones, prestando servicio a más de 3 000 millones de personas en todo el mundo. Huawei es una empresa privada, propiedad exclusiva de su personal.
>
> (Huawei, s.f.)

Varios expertos coinciden en la relevancia de este actor en términos de liderazgo del desarrollo de las redes 5G. Carmona (2020) explica que en la actualidad existen varias empresas con patentes en la industria del 5G, entre ellas, las chinas Huawei y ZTE, las europeas Nokia y Ericsson, las estadounidenses Qualcomm e Intel o las surcoreanas Samsung y LG. Sin embargo, considera que es Huawei quien está en condiciones de ofrecer la instalación más completa y económicamente asequible.

2.2. CONTEXTO

En la última década, el caso Huawei ha sido uno de los protagonistas en la relación entre EE. UU. y China. Salazar (2020, p. 6) afirma que «la confrontación entre Estados Unidos y China por el veto a Huawei en el uso de la tecnología 5G representa, según el análisis de poder Weberiano, la lucha de dos modelos imperialistas en disputa por un lugar hegemónico en el espacio geopolítico».

[4] Este trabajo sigue las normas de citación APA, según las cuales las citas largas (de 40 palabras o más) se escriben aparte del texto, sin comillas, con sangría, sin cursiva, con mismo tipo y tamaño de fuente y con interlineado doble, disponibles en: https://normas-apa.org/citas/citas-con-mas-de-40-palabras/comment-page-2/

Las acusaciones de ciberdelincuencia a Huawei se remontan a 2001, cuando la India informó de la colaboración de esta empresa con los talibanes, Irak y Pakistán a través del suministro de equipos de vigilancia y telecomunicaciones. Sin embargo, no se llegó a profundizar en este asunto. Ese mismo año, China ingresó en la Organización Mundial del Comercio (OMC), lo que supuso una remodelación de las normativas chinas que daban prioridad a las empresas nacionales sobre las extranjeras.

Durante los siguientes años, la empresa china fue acusada de numerosos delitos. En 2003, la compañía estadounidense Cisco Systems demandó a Huawei por infracción de sus patentes. En 2008, el presidente de EE. UU. interrumpió la compra por parte de Huawei de una empresa estadounidense de fabricación de equipos de redes informáticas, alegando que suponía riesgos en la seguridad del país. Poco después, se acusó a Huawei de comerciar con Irán, de modo que se infringían las sanciones comerciales impuestas por EE. UU., por lo que el FBI investigó al director ejecutivo de la empresa. En 2009, Motorola también demandó a Huawei por espionaje corporativo. En 2011, el presidente de EE. UU. bloqueó el desarrollo de infraestructuras de redes de Huawei en ese país por, de nuevo, preocupaciones de seguridad. En 2012, el Departamento de Inteligencia de EE. UU. abrió una investigación a Huawei y ZTE sobre sus presuntos vínculos con el gobierno chino. Washington parecía estar convencido del presunto ciberespionaje al gobierno estadounidense por parte gobierno chino a través de empresas de telecomunicaciones, como Huawei y ZTE. Ya en marzo de 2014, Wikileaks reveló la llamada «Operación *Shotgiant*», donde se mostraba cómo la Agencia de Seguridad Nacional de EE. UU. (NSA, por sus siglas en inglés) espiaba a Huawei desde 2009.

Sin embargo, el período más importante en el caso Huawei y la crisis de esta empresa como tal empezaron en 2018[5]. En enero, EE. UU. prohibió el lanzamiento y la venta del teléfono *Huawei Mate 10*, puesto que se creía que el dispositivo obtendría datos de los usuarios para, más tarde, remitirlos al gobierno chino. El 3 de mayo, el Departamento de Defensa de EE. UU. prohibió el uso de teléfonos de Huawei y ZTE en las bases militares estadounidenses. Más adelante, Washington prohibió la compra de equipos de redes chinos porque consideraba que comprometían la seguridad nacional a través de las redes 5G. Unos meses después, el 1 de diciembre, la directora financiera de Huawei, Meng Wanzhou, fue detenida en Canadá acusada de infringir las sanciones impuestas por EE. UU. a Irán. Las tensiones entre las dos grandes potencias continuaron creciendo, hasta que, el 28 de enero de 2019, el Departamento de Justicia de EE. UU. emprendió la vía legal y acusó a Huawei de 23 cargos, entre los cuales destaca el fraude y el robo de tecnología e información privada. A modo de respuesta, el 9 de marzo, China demandó a EE. UU. por la prohibición de sus productos en el mercado estadounidense, alegando que esa acción iba en contra de las leyes comerciales.

Como explica Salazar (2020), el punto de mayor inflexión tuvo lugar el 16 de mayo de 2019, cuando la administración de Trump emitió una orden ejecutiva justo después de que Huawei se diera a conocer como empresa pionera en el desarrollo del 5G. La orden ejecutiva tenía por objetivo evitar que las empresas de telecomunicaciones del país comprasen equipos de fabricación extranjera. A pesar de que en la orden ejecutiva

[5] Consultar Anexo I.

no se mencionaba específicamente a Huawei, el Departamento de Comercio incluyó después a esta empresa en la *Entity List*, una lista de restricciones comerciales. Las personas, empresas y gobiernos incluidas en esta lista se encuentran sujetas a los requisitos de licencia de los EE. UU. para la exportación o transferencia de determinados artículos, pero las empresas estadounidenses no tienen prohibida la compra de sus artículos. A partir de ese momento, EE. UU. consideró oficialmente a Huawei como una amenaza para la seguridad nacional, por lo que las empresas estadounidenses necesitaban una licencia especial para comerciar con la empresa china. EE. UU. decidió dejar de proveer software y hardware a Huawei y, tres días más tarde, el 19 de mayo, Google suspendió las relaciones con esta empresa, de modo que los nuevos dispositivos de Huawei no incluían el sistema operativo Android, ni sus aplicaciones, como YouTube y Gmail.

Las ventas de Huawei se desplomaron ante lo acontecido hasta ese momento. Las empresas estadounidenses encontraban múltiples dificultades a la hora de adquirir artículos de Huawei y los usuarios temían que sus dispositivos fueran inservibles a causa de las restricciones comerciales. Sin embargo, China no se dio por vencida. El 1 de junio, Beijing respondió a las acciones emprendidas por EE. UU. subiendo los aranceles a las importaciones estadounidenses. Además, Huawei decidió incrementar su autonomía estratégica al desarrollar su propio sistema operativo, Harmony OS, alternativo al estadounidense Android y presentado el 9 de agosto de 2019. Desde el inicio de este conflicto, la empresa ha recurrido a todas las opciones a su alcance, como utilizar licencias antiguas. Los teléfonos que Huawei ha sacado al mercado desde entonces se han lanzado con Android 10, pero sin las aplicaciones y servicios de Google. En su lugar, utilizan los Huawei Mobile Services.

La empresa china siempre ha negado las acusaciones de ciberespionaje debido a la falta de pruebas que demuestren su culpabilidad. Por ese motivo, múltiples estados y actores transnacionales encuentran dificultades para posicionarse ante la polémica del 5G. Varias autoras, como Carmona (2020, p. 3), argumentan lo siguiente:

> El crecimiento chino ha traído consigo una nueva realidad: una situación de enfrentamiento estructural entre Estados Unidos, que intentará hacer lo que esté en su mano por frenar el auge chino, y China, que, siguiendo una estrategia muy calculada, se está colocando como superpotencia en el orden mundial […]. Estados Unidos, acorde a sus intereses de ralentizar el auge chino, ha vetado y pedido a sus socios europeos que veten a Huawei, campeón chino en la materia y primera opción para la implantación de estas redes en la mayoría de Estados miembros por varios motivos.

Los estados del norte global se han visto obligados a posicionarse ante el debate del 5G y el enfrentamiento entre las dos grandes potencias. Para ello, resulta esencial tener en cuenta tanto la ciberseguridad, como las relaciones con EE. UU. y China y su posible afectación ante el posicionamiento y las medidas adoptadas al respecto.

2.3. DELIMITACIÓN DEL CONFLICTO

A continuación, se trata la delimitación del conflicto entre Huawei y EE. UU., donde se explica el motivo de la discordia, se detallan los actores implicados y se recogen los intereses de partida de estos actores. Primero, se analizan cinco estados clave en este conflicto y, después, se profundiza en el caso de la UE.

Desde 2018, mientras Huawei trabajaba en defenderse de las acusaciones y ataques recibidos, EE. UU. utilizaba su enorme influencia a nivel doméstico y mundial para instar la comunidad internacional a tomar medidas restrictivas contra el gigante tecnológico. A nivel doméstico, Google y Android cortaron sus relaciones con la empresa china desde prácticamente el inicio del conflicto, pero la influencia de Washington no se detuvo en sus fronteras. Japón[6], Australia y Nueva Zelanda se sumaron a la prohibición de los productos de esta empresa, siguiendo la iniciativa estadounidense, en 2018. La presión de EE. UU. fue internacionalizada, especialmente en el Reino Unido y la UE, socios comerciales importantes en el mercado de Huawei. El gobierno americano instó a los países a no contratar servicios de tecnología 5G, ya que podría derivar en un espionaje sistémico que vulnerase la seguridad estatal, lo que obligaría a Washington a limitar la cooperación con los estados europeos. Las advertencias hicieron eco principalmente en el Reino Unido, quien firmó un acuerdo comercial con Estados Unidos tras el Brexit, y terminó bloqueando de su economía al gigante de las telecomunicaciones (Salazar, 2020). En mayo de 2022, Canadá también se unió a este bloque al prohibir a Huawei trabajar en el 5G canadiense por preocupaciones de seguridad.

EE. UU. cuenta con 5 aliados estatales cuyos intereses de partida están muy vinculados al mantenimiento de las buenas relaciones con este país. La alianza Cinco Ojos (FIORC, por sus siglas en inglés), también conocida como *Five Eyes*, es uno de los factores clave en la restricción del 5G de Huawei. FIORC es una alianza centrada en la inteligencia, formada por EE. UU., Australia, Canadá, Nueva Zelanda y el Reino Unido. Entre los principales objetivos destaca el intercambio información de sobre temas de interés y preocupación mutuos y la búsqueda de áreas en las que se permita la cooperación en materia de evaluación y la puesta en común de resultados. Tras identificar esta alianza, no resulta de extrañar que todos los Estados miembros hayan adoptado medidas restrictivas contra Huawei.

Por lo que respecta a la UE, un actor sin autonomía tecnológica, se ha visto presionada por ambas potencias para vetar o incluir a Huawei en las redes 5G (Carmona,

[6] Japón prohibió la adquisición gubernamental de productos de telecomunicaciones de las empresas chinas Huawei y ZTE debido la preocupación por las filtraciones de información y los ciberataques. A pesar de que la normativa no menciona a las dos empresas en concreto, les afecta directamente, ya que el gobierno japonés pretende evitar la filtración de información sensible. Esta acción sigue a la decisión de EE. UU. de prohibir la compra de equipos de Huawei. Sin embargo, este trabajo se centra solamente en el posicionamiento de los estados miembros de FIORC y la UE, dada su vinculación con el objeto de estudio.

2020). La organización ha mostrado una gran preocupación por la seguridad europea en el ciberespacio, pero nunca ha llegado a prohibir explícitamente los servicios de Huawei. Al inicio del conflicto, los Estados miembros de la UE se mostraron a favor del gigante chino. A principios de 2019, Alemania, Italia y Francia compartieron su apoyo al afirmar, de una manera u otra, que las acusaciones de ciberespionaje carecían de evidencias. La UE opinaba que ningún fabricante debía ser excluido del 5G sin pruebas.

> Las capitales europeas se han visto envueltas en la competencia entre dos grandes potencias, llegando a ser presionadas tanto por Washington como por Pekín. Con Estados Unidos llegando a amenazar a la UE y a sus miembros con represalias en cooperación en materia de inteligencia o defensa si no bloqueaban a Huawei; y con China haciendo lo propio con medidas económicas si la vetaban como pedía Washington […]. Esta decisión es muy difícil para los Estados miembros. Seguir a Estados Unidos es caro y disruptivo desde el punto de vista técnico. Además de que supone ir en contra de China, importantísimo socio comercial para las capitales europeas. Incluir a Huawei en la implantación es lo lógico desde el punto de vista económico y va en línea con China, pero va en contra de Estados Unidos, de quien dependemos para nuestra seguridad y defensa.
>
> (Carmona, 2020, p. 19-23)

La UE decidió actuar con prudencia al permitir que cada Estado miembro tomase sus propias decisiones ante este conflicto. Por ese motivo, en este escenario encontramos 17 puntos de vista diferentes. Aún así, la presión estadounidense terminó haciendo su efecto en la UE, como explica el Parlamento Europeo (2019): «EE. UU. ha presionado a sus aliados para que sigan su ejemplo y ha amenazado con que el uso de equipos chinos podría reducir el intercambio de información con EE. UU. y afectar a la cooperación dentro de la OTAN». Por ese motivo, en enero de 2020, la Comisión Europea presentó la *EU Toolbox para la seguridad 5G*, una serie de medidas para garantizar la seguridad en las redes reduciendo los riesgos de manera eficaz y que permiten garantizar, por tanto, el despliegue de redes 5G seguras en Europa (Jiménez, A. C. et al., 2020). A mediados de diciembre del mismo año, la UE publicó el borrador de la Ley de Servicios Digitales y de la Ley de Mercados Digitales siguiendo la estrategia «Una Europa Adaptada a la Era Digital» (Rodríguez, A. G., 2021). A nivel doméstico, Alemania presentó en 2021 la nueva *Ley de Seguridad Informática 2.0*, aprobada por el Bundestag, que restringe el papel de los proveedores no fiables de tecnología 5G y exige a los operadores de

telecomunicaciones que notifiquen al gobierno si firman contratos de componentes 5G. Ese mismo año, el tribunal supremo de Francia aprobó la ley introducida por el gobierno sobre la seguridad de las redes 5G, apodada «Ley anti-Huawei». Según el Consejo Constitucional francés, el objetivo de la ley es velar por la defensa y la seguridad nacionales y proteger las redes de telecomunicaciones de riesgos como el espionaje, la piratería y el sabotaje.

A pesar de que Huawei ha negado desde el inicio las acusaciones de ciberespionaje y obviando la falta de evidencias en este caso, todos los actores mencionados han optado por seguir las indicaciones de EE. UU. de vetar a esta empresa. La UE y los Estados miembros de FIORC tienen una fuerte relación con Washington que, como resulta evidente, no están dispuestos a romper.

3. POSICIONAMIENTO DE LOS ACTORES

En este apartado se investigan las medidas concretas adoptadas contra Huawei a partir del conflicto con EE. UU. sobre el 5G. Los actores seleccionados para este análisis son Australia, Nueva Zelanda, el Reino Unido, Canadá y la Unión Europea, puesto que se consideran los más destacables para este estudio por su relación con EE. UU., su poder a escala mundial y su alta implicación en el conflicto.

3.1. AUSTRALIA

Australia fue el primer Estado miembro de FIORC en unirse a las prohibiciones estadounidenses al vetar el 5G de Huawei en agosto de 2018. De hecho, se posicionó en este conflicto de manera muy radical. No solo prohibió a Huawei y ZTE, sino que cualquier empresa procedente de China quedó fuera de la posibilidad de formar parte de la cadena de suministro de 5G de Australia, ya que la orden no hacía mención específica a ninguna empresa en concreto. Cuando se anunció la prohibición, el entonces Ministro de Interior en funciones, Scott Morrison, anunció en un comunicado de prensa que:

> El Gobierno considera que la presencia de proveedores que puedan estar sujetos a órdenes extrajudiciales de otro gobierno que entren en conflicto con la legislación australiana, puede suponer que el operador no proteja adecuadamente la red 5G de accesos no autorizados o interferencias.
>
> (Scott Morrison, 2018)

El comunicado destaca que el gobierno considera que ambas empresas chinas podrían suponer una amenaza para la seguridad nacional. Sin embargo, el problema es que eliminar radicalmente todos los productos y equipos chinos de una futura red 5G australiana podría suponer grandes dificultades para la infraestructura de telecomunicaciones de este país.

3.2. NUEVA ZELANDA

Para gobierno neozelandés no resultó tan sencillo posicionarse ante este conflicto. En noviembre de 2018, la Oficina de Seguridad y Comunicaciones del Gobierno (GCSB, por sus siglas en inglés) publicó una declaración en la que se notificaba un riesgo significativo en la seguridad de la red de telecomunicaciones neozelandesa. Sin embargo, el gobierno no hizo alusión expresa a ningún estado o empresa culpable de dicho riesgo.

El caso de Nueva Zelanda destaca por la poca información existente en relación con el conflicto entre Huawei y EE. UU. por el 5G. El gobierno no ha emitido públicamente ningún comunicado en el que se acuse explícitamente a Huawei de ciberespionaje. Parece ser que Nueva Zelanda finalmente se habría decantado por prohibir el 5G de Huawei bajo la influencia de EE. UU. para asegurar el mantenimiento de las alianzas y buenas relaciones entre los dos estados. La decisión final de restringir el comercio al gigante chino de las telecomunicaciones se alinea, además, con Australia, país con el cual también tiene muchos intereses económicos y políticos, y, más tarde, con el resto de Estados miembros de FIORC. A pesar de la discreción neozelandesa en este conflicto, China se ha mostrado en desacuerdo con todos los estados que han prohibido el 5G de Huawei, por lo que parece que el gobierno neozelandés no habría obtenido los resultados esperados con su posicionamiento.

3.3. REINO UNIDO

A lo largo de 2020, el gobierno de Boris Johnson emitió una serie de comunicados sobre el uso de bienes y servicios de Huawei, categorizado como proveedor de alto riesgo. El Reino Unido se propone proteger su infraestructura de telecomunicaciones de los proveedores de alto riesgo y se ha comprometido a emitir duras sanciones a los proveedores que no cumplan con sus estándares de seguridad. Para ello, la *Ley de Telecomunicaciones (Seguridad)* de 2021 marca los pasos a seguir para eliminar los riesgos que plantea Huawei a través de las siguientes medidas:

- No instalar equipos de Huawei en las redes 5G, con efecto inmediato tras la emisión de la resolución;
- No instalar equipos de Huawei afectados por las sanciones en redes de fibra óptica integral, con efecto inmediato tras la emisión de la resolución. Esto incluye cualquier equipo cuya cadena de suministro o proceso de fabricación se haya alterado debido al impacto de las sanciones estadounidenses;
- Retirar todos los equipos de Huawei del núcleo de las redes de telecomunicaciones antes del 28 de enero de 2023;
- Reducir la proporción de equipos de Huawei al 35% de las redes de fibra óptica integral y de acceso 5G antes del 31 de julio de 2023, seis meses más tarde de lo previsto debido a las dificultades a las que se han enfrentado los proveedores durante la pandemia;
- Retirar los equipos de transmisión de datos de alta velocidad de Huawei (hardware que envía datos a través de una red sin procesarlos) de todas las redes para el 31 de diciembre de 2025;
- Retirar todos los equipos de Huawei de las redes 5G para finales de 2027.

A pesar de la preocupación que muestra el Reino Unido por su seguridad en relación con Huawei, en enero de 2022, Vince Cable, quien fue ministro de Empresa e Industria, explicó que la decisión contra el gigante tecnológico chino «no tuvo nada que ver con la seguridad nacional» y se tomó «porque los estadounidenses nos dijeron que debíamos hacerlo».

3.4. CANADÁ

Canadá ha sido el último Estado miembro de FIORC en emprender la vía legal contra Huawei. En mayo de 2022, el gobierno canadiense se posicionó claramente en este conflicto al compartir que:

> El Gobierno de Canadá tiene serias preocupaciones sobre proveedores como Huawei y ZTE, que podrían verse obligados a seguir órdenes extrajudiciales de otros gobiernos de manera que entrarían en conflicto con las leyes canadienses o irían en perjuicio de los intereses canadienses. Los aliados de Canadá más cercanos comparten la misma preocupación por estos dos proveedores. Dadas las posibles repercusiones económicas y de seguridad que podría causar una brecha en la cadena de suministro de telecomunicaciones, los aliados han tomado medidas a fin de poder prohibir el despliegue de productos y servicios de Huawei y ZTE en sus redes de telecomunicaciones 5G.
>
> (Gobierno de Canadá, 2022)

En esta declaración, titulada «Protección el sistema de telecomunicaciones de Canadá», se detallan una serie de medidas restrictivas contra Huawei y ZTE por supuestas preocupaciones en la seguridad del país. Las medidas más destacables son:

- Prohibir el uso de nuevos equipos de 5G y de servicios gestionados por Huawei y ZTE;
- Frenar la adquisición de nuevos equipos 4G o 5G a esas empresas para septiembre de 2022;
- Retirar o dar de baja los equipos 5G existentes de Huawei y ZTE antes del 28 de junio de 2024;
- Retirar o dar de baja cualquier equipo 4G ya existente proporcionado por estas empresas antes del 31 de diciembre de 2027.

3.5. UNIÓN EUROPEA

Al inicio del conflicto, la UE no se posicionó de manera unánime. Además de tener en cuenta las consideraciones técnicas, jurídicas y políticas relacionadas con la seguridad, resultaba fundamental que la organización preservase su autonomía estratégica en un contexto de presión geopolítica por parte de EE. UU. y China y de duras circunstancias económicas, como la gran dependencia actual de los operadores de telecomunicaciones de la UE de los equipos chinos (por ejemplo, en Alemania y Francia). En 2019, la Comisión Europea instó a los Estados miembros a compartir más datos para hacer frente a los riesgos de ciberseguridad relacionados con las redes 5G, pero todavía ignoraba los llamamientos de EE. UU. para prohibir a Huawei en su mercado. Sin embargo, tiempo después quedó claro que los beneficios económicos perdían protagonismo frente a los geopolíticos a escala global. Los Estados miembros, de manera particular, y la UE, de manera general, expusieron públicamente su preocupación general por la seguridad nacional en las redes 5G:

> La Comisión Europea, la Agencia Europea de Ciberseguridad (ENISA) o el Grupo de Cooperación NIS, han señalado un incremento significativo de los riesgos de seguridad en las redes 5G respecto a otras generaciones de redes móviles. Estos riesgos guardan especial relación con la disponibilidad, integridad, privacidad, confidencialidad y accesibilidad de las redes.
>
> (Jiménez, A. C. et al., 2020, p. 2)

La UE se mostró visiblemente preocupada por la ciberseguridad en su territorio, pero no estaba dispuesta a romper sus relaciones con el país asiático. Para ello, dotó de autonomía a los Estados miembros para decidir qué papel podía desempeñar Huawei en sus redes de telecomunicaciones 5G. A pesar de que los Estados miembros tenían diferentes relaciones con China, existía un consenso general en la preferencia por el mantenimiento de la alianza trasatlántica y el mantenimiento de China como socio comercial en la medida de los posible. Hasta la fecha, cada Estado ha tomado sus decisiones al respecto de manera independiente (Carmona, 2020). La UE resistió inicialmente a la presión de EE. UU. para una prohibición total, mientras Washington opinaba que los Estados miembros de la UE no tenían ninguna razón para utilizar la tecnología móvil 5G de Huawei porque la sueca Ericsson, la finlandesa Nokia y la surcoreana Samsung estaban a la par con el grupo chino en ese campo.

Mientras que la mayoría de los países de la UE siguieron las directrices de la UE sobre ciberseguridad 5G, los enfoques entre los Estados miembros difieren considerablemente. Aun así, las instituciones de la UE emprendieron una serie de iniciativas para lidiar con el peligro de las redes 5G, relacionado, una vez más, con China:

> En 2018, Huawei Technologies ocupó el primer lugar entre los siete principales proveedores de equipos de telecomunicaciones a nivel mundial, por delante de las estadounidenses Cisco y Ciena, la sueca Ericsson, la finlandesa Nokia, la surcoreana Samsung y la estatal china ZTE Corporation […]. Huawei cuenta con una importante presencia en el mercado de la UE por sus precios competitivos y su supuesta mejor calidad. Hasta hace poco había poca conciencia pública en la UE de cómo los estrechos lazos que las empresas públicas y privadas chinas mantienen con el Partido Comunista Chino, para prosperar en el ecosistema chino, pueden exponer a las democracias liberales a ciberataques, ciberespionaje, autoritarismo digital y guerra de la información en el contexto del 5G. Un informe de una consultora estadounidense de 2018 señala una serie de factores de riesgo asociados a Huawei, siendo las preocupaciones más graves las relacionadas con la ciberseguridad, el espionaje promovido por el Estado, la influencia militar y la interferencia política extranjera.
>
> (Parlamento Europeo, 2019)

Ante esta declaración, la UE decidió mejorar su legislación en términos de ciberseguridad y dotarse de herramientas de auto defensa en este campo. Dado que los Estados miembros de la UE son los únicos competentes en materia de seguridad nacional y el papel de la UE es meramente complementario, el 26 de marzo de 2019, la Comisión Europea emitió una recomendación no vinculante sobre la ciberseguridad de las redes 5G. Esto siguió a los llamamientos del Parlamento Europeo para un enfoque común de la ciberseguridad, en su resolución del 12 de marzo de 2019. La recomendación de la Comisión establecía una hoja de ruta hasta finales de 2019 para una evaluación coordinada del riesgo de la UE, basada en las evaluaciones de riesgo de los Estados miembros utilizando factores técnicos y un conjunto común de medidas de mitigación del riesgo. A falta de una legislación armonizada de la UE, los Estados miembros pueden optar por declarar obligatorio el sistema de certificación de ciberseguridad europeo, que debe desarrollarse en el marco del *Reglamento sobre la Ciberseguridad de la UE*.

Dada la falta de coherencia dentro de la UE ante este conflicto, la organización presenta tantos posicionamientos como Estados miembros. En este trabajo se han seleccionado los seis principales. Alemania, Francia e Italia se consideran relevantes al ser las grandes economías de la UE. También se estudia el caso de España, por ser el

estado en el que se realiza este trabajo. Irlanda resulta pertinente dado que aparece, más adelante, en el análisis económico de la compañía estadounidense Qualcomm. Por último, se destaca Suecia al ser uno de los estados más activos en cuanto a la toma de medidas restrictivas contra Huawei:

- **Alemania:** En este país, Huawei es el principal proveedor de componentes básicos para los operadores de telecomunicaciones, por lo que la prohibición explícita de esta empresa no es una opción. Alemania ha sido criticada durante mucho tiempo por su enfoque burocrático a la hora de evaluar qué proveedor de 5G se considera digno de confianza. Por ello, la versión final de la *Ley de Seguridad Informática 2.0* añadió la perspectiva política al brindarle al gobierno alemán la capacidad de vetar la contratación de proveedores no fiables. Aunque la ley no señala directamente a Huawei, el mensaje es claro, Alemania considera que las empresas que están bajo el control de Estados autoritarios se consideran poco fiables. El enfoque alemán sobre Huawei siguió en gran medida las directrices que la UE estableció en la *EU Toolbox para la seguridad 5G* y en su informe de evaluación de riesgos para la ciberseguridad de las redes 5G. Ambos documentos se diseñaron para mitigar los riesgos potenciales en el despliegue europeo de 5G. A pesar de que en ninguno de los dos documentos se menciona directamente a Huawei, se define la posible interferencia de terceros Estados como uno de los principales riesgos de seguridad en el despliegue del 5G.
- **Francia:** Aunque el gobierno francés prohibió directamente a Huawei, sus agencias de ciberseguridad han desarrollado amplios poderes para bloquear la adquisición de equipos de Huawei. El enfoque francés está centrado en la Agencia Nacional de Seguridad de los Sistemas de Información (en adelante, ANSSI). Aunque el presidente francés tiene amplios poderes para vetar la adquisición de equipos 5G de proveedores de alto riesgo, la ANSSI desempeña un papel clave en el enfoque de Francia. Esta agencia de ciberseguridad ha restringido el uso de equipos de Huawei y tiene previsto eliminar los equipos actualmente en uso para 2028.
- **Italia:** Ha modificado recientemente su legislación para permitir al gobierno bloquear los contratos con proveedores de telecomunicaciones ajenos a la UE. En este país, el gobierno puede vetar los acuerdos de suministro de 5G que se consideren una amenaza para su seguridad nacional. En octubre de 2020, el gobierno utilizó este poder para bloquear un acuerdo entre Huawei y la empresa de telecomunicaciones Fastweb sobre la adquisición de piezas básicas para 5G y pidió a Fastweb que diversificara sus proveedores. En países como Portugal y los Países Bajos, los gobiernos recomendaron a los proveedores de telecomunicaciones que no utilizaran equipos de Huawei en su despliegue de 5G.
- **España:** Ha adoptado un enfoque más suave. España fue prudente al no prohibir explícitamente a Huawei en el suministro de las redes 5G. En su lugar, adoptó un enfoque neutral, basado en procedimientos burocráticos y no en evaluaciones políticas. La decisión de permitir o no a la empresa china entrar en el mercado del 5G depende únicamente del nivel de riesgo supuesto por la empresa, evaluado por

los expertos españoles. La Ley de Ciberseguridad española destaca aún más las obligaciones de los proveedores y suministradores de 5G.

- **Irlanda:** La empresa de telecomunicaciones irlandesa Eir no tiene previsto retirar a Huawei de su red y afirma que cualquier cambio en la postura actual de la UE supondría grandes costes para los proveedores y los clientes. Eir utiliza una combinación de proveedores formada por Ericsson, en el núcleo de su red 5G, y Huawei, que proporciona el equipo de acceso de radio. La directora ejecutiva, Carolan Lennon, confía en la seguridad de Huawei y asegura que la empresa de telecomunicaciones mantendrá estos equipos en partes de su red siguiendo las recomendaciones de la UE sobre el veto a los proveedores. En una entrevista, Lennon (2020) dijo que: «Gestionamos y supervisamos nuestra red por nuestra cuenta con nuestro propio personal. Apoyamos esa propuesta de la UE, [la *EU Toolbox para la seguridad 5G*,] en la que no hay ninguna recomendación de prohibir a ningún proveedor de red en particular».
- **Suecia:** Los países escandinavos y de Europa del Este han adoptado la postura más dura contra Huawei. Suecia ha prohibido a los proveedores chinos el despliegue de la 5G y ha establecido que los operadores de telecomunicaciones deberán retirar los equipos chinos de sus infraestructuras en 2025. Dinamarca siguió un camino similar. Aunque el país nórdico no mencionó directamente a Huawei, dejó claro que no permitiría equipos procedentes de países no considerados aliados en materia de seguridad. Otros, como Eslovenia, Polonia, República Checa, Rumanía, Estonia, Letonia, Eslovaquia y Bulgaria se comprometieron a excluir a los proveedores que no son de confianza, entre los cuales se encuentra Huawei, de su despliegue de 5G. Polonia y Rumanía ya han emprendido acciones legales para excluir a Huawei de su mercado 5G.

4. ANÁLISIS ECONÓMICO

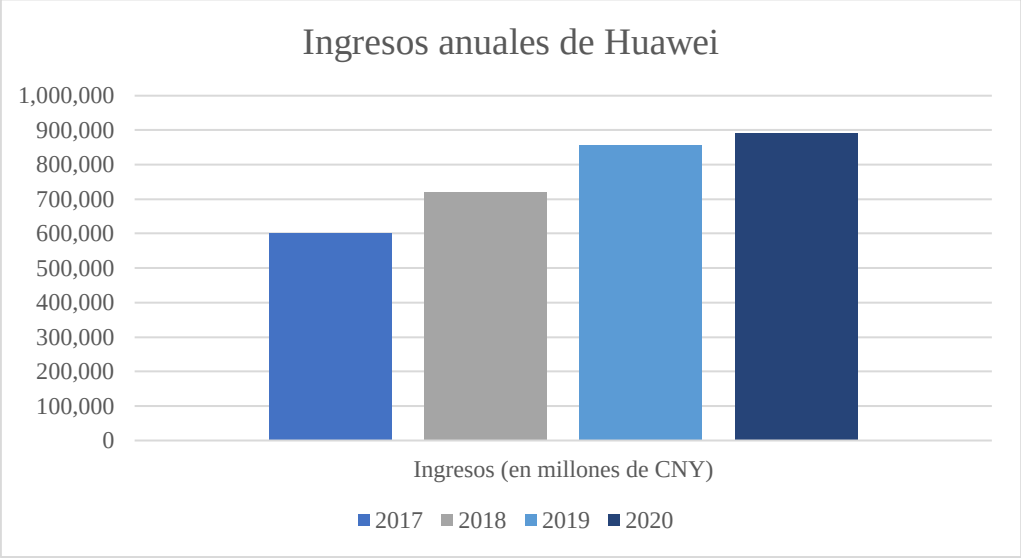
Para poder dar respuesta a la hipótesis se analizan los informes económicos de Huawei, Intel y Qualcomm desde 2017 hasta 2020. La comparación financiera y temporal de estas empresas en relación con el contexto aporta datos numéricos sobre las consecuencias de las medidas adoptadas por Australia, Nueva Zelanda, el Reino Unido, Canadá y la UE.

El análisis aborda tres empresas clave: Huawei, por ser la principal afectada en este conflicto, Intel y Qualcomm, relevantes al ser dos empresas estadounidenses. La metodología de este análisis de caso consiste en la extracción de datos de los informes anuales consultados en las páginas oficiales de las tres empresas. El espacio temporal seleccionado va desde 2017 hasta 2020 para poder comparar el estado de estas empresas antes de los momentos decisivos en el conflicto y evaluar su evolución hasta prácticamente la actualidad.

4.1. HUAWEI

Los datos financieros muestran que Huawei no ha dejado de crecer económicamente durante los últimos años. De hecho, Ortega (2020, p. 17) explica que «China prioriza la idea del mayor bien para el mayor número de personas, en lugar de un imperativo moral para proteger los derechos individuales, que predomina en Occidente. Los consumidores chinos parecen menos preocupados por la privacidad, incluidos los sistemas de reconocimiento facial y las funciones de vigilancia». En 2017, la empresa ingresó 603 621¥ millones, una cifra que ha ido en constante aumento en los años siguientes hasta alcanzar los 891 368¥ millones en 2020. Por lo que respecta al beneficio neto de la empresa, las cifras, en millones, son las siguientes: 47 455¥ (2017), 59 345¥ (2018), 62 656¥ (2019) y 64 649¥ (2020). Estos datos demuestran que Huawei ha incrementado su presencia en el campo de la informática y justifican que se le considere el «gigante tecnológico».

Tabla 1. Ingresos anuales de la empresa Huawei



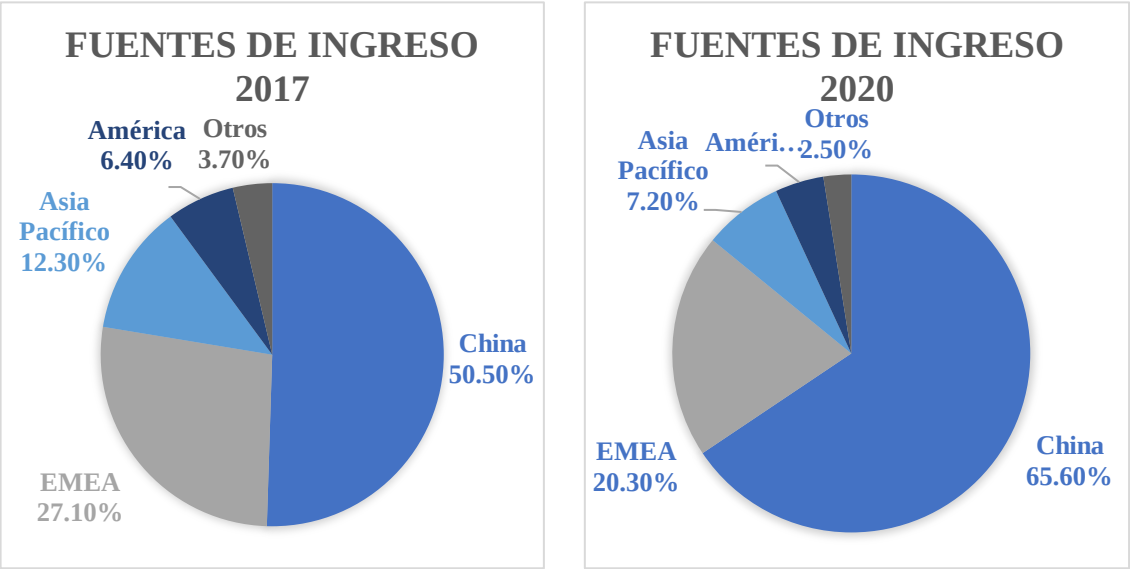
Fuente: Elaboración propia a partir de los informes anuales de Huawei

Huawei clasifica las fuentes de sus ingresos en cuatro grupos principales: China, Asia Pacífico, América y el bloque formado por Europa, Oriente Medio y África (EMEA, por sus siglas en inglés). Como se observa en los siguientes gráficos circulares, la presencia de la empresa china a escala internacional ha ido en leve descenso con el paso de los años, suponiendo un aumento en los ingresos nacionales. Los informes de los cuatro años seleccionados muestran la progresiva disminución de ingresos extranjeros en la empresa, pero Huawei no se limita a la aportación de datos, sino que también explica las causas.

En el caso de EMEA, la compañía china considera que el desarrollo de las redes 5G ha sido el principal impulsor en las relaciones comerciales. Sin embargo, explica que «dado que a nuestro negocio se le ha denegado el acceso a los Servicios Móviles de Google, nuestros ingresos totales de esta región disminuyeron un 12,2% con respecto al año anterior, suponiendo hasta 180 849¥ millones (Huawei Investment & Holding Co., Ltd., 2020, p. 17)». Se relaciona la misma causa para la disminución del 8,7% de ingresos

del Asia Pacífico en 2020 con respecto a 2019. En el caso de América, «los ingresos disminuyeron un 24,5%, 39 638¥ millones, debido a las fluctuaciones de inversión en los mercados de telecomunicaciones de algunos países y la falta de acceso los Servicios Móviles de Google (Huawei Investment & Holding Co., Ltd., 2020, p. 17)».

Tabla 2. Fuentes de ingreso de Huawei



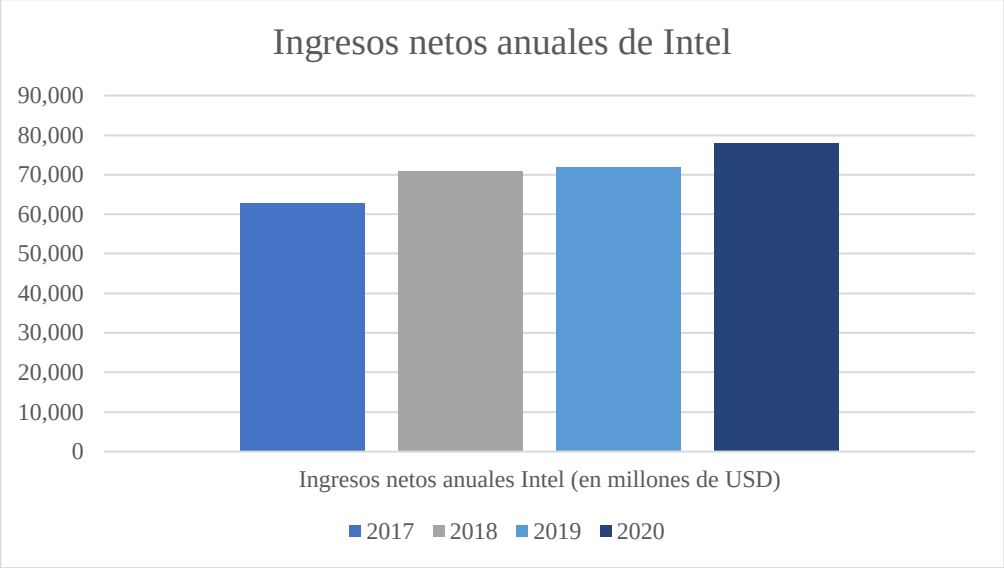
Fuente: Elaboración propia a partir de los informes anuales de Huawei

El análisis financiero de Huawei muestra la resiliencia que le caracteriza. A pesar de su decreciente papel a escala internacional, el aumento constante de ingresos refleja el gran desarrollo del gigante de las telecomunicaciones. Además, la propia empresa vincula la disminución de ingresos extranjeros al conflicto con EE. UU., al mencionar la prohibición de uso de los Servicios Móviles de Google. Los datos muestran que las restricciones de comercio y uso de Huawei, derivadas de la presión estadounidense, han tenido un fuerte impacto negativo en la empresa. Sin embargo, Huawei trabaja día a día por recuperarse de los daños causados por las acusaciones de ciberespionaje, que todavía carecen de pruebas.

4.2. INTEL

Intel es una de las mayores empresas estadounidenses de tecnología y procesadores informáticos, sobre todo, de ordenadores. El análisis financiero muestra que esta empresa también está en constante crecimiento, con un aumento de los ingresos netos desde 2017 ($62 761 millones) hasta 2020 ($77 867 millones). Es evidente que la era digital supone un innegable crecimiento de este tipo de empresas, pero la gran variedad de servicios y la enorme competencia en este campo supone que consolidarse como líder del sector sea un gran reto. Por lo que respecta al beneficio neto de la empresa, ha evolucionado de la siguiente manera (en millones): $9 601 (2017), $21 053 (2018), $21 048 (2019) y $20 899 (2020). Destaca el gran incremento de beneficios entre 2017 y 2018, pero no parece tener relación con el conflicto tratado en este trabajo, ya que las medidas restrictivas contra Huawei se iniciaron en 2018.

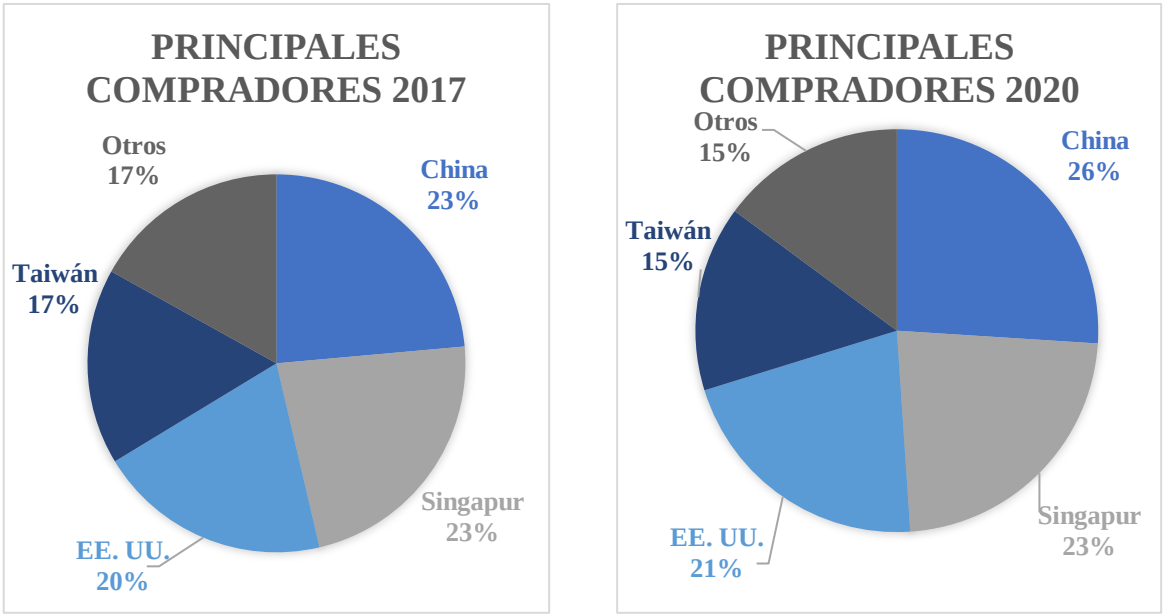
Tabla 3. Ingresos netos anuales de la empresa Intel



Fuente: Elaboración propia a partir de los informes anuales de Intel

El aspecto más impactante del análisis de esta empresa es el origen de sus ingresos por país. Resultaría lógico pensar que el principal comprador de productos de Intel es EE. UU., pero sorprende descubrir que no es así. El principal comprador de sus productos es China, seguida de Singapur. De hecho, la distribución de las principales fuentes de ingresos prácticamente no ha variado con el paso de los años. A medida que la empresa ha aumentado los ingresos anuales, ha mantenido a sus principales compradores.

Tabla 4. Principales compradores de productos de Intel



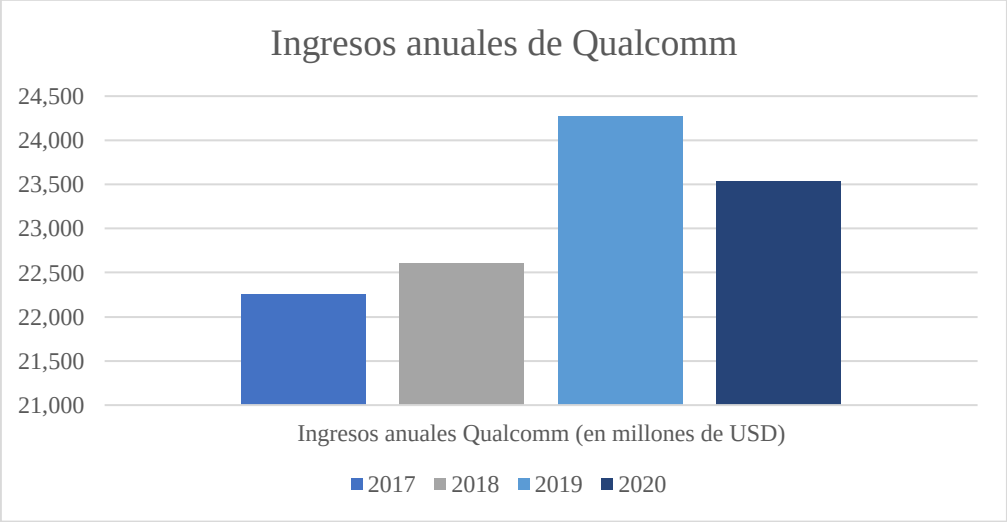
Fuente: Elaboración propia a partir de los informes anuales de Intel

Los datos muestran que Intel no se ha visto afectada por el conflicto entre EE. UU. y Huawei. El desarrollo de la empresa ha permitido incrementar sus ganancias, pero no parecen ser resultado de las medidas restrictivas contra Huawei. De ser así, se observarían cambios en las principales fuentes de ingreso de la compañía, incrementando el porcentaje de la sección «otros» o incluso incluyendo actores como Australia, Nueva Zelanda, el Reino Unido y la UE. Sin embargo, el análisis financiero muestra que Intel ha mantenido su mercado y no se ha visto afectada, ni negativa ni positivamente, por la polémica del 5G.

4.3. QUALCOMM

Esta empresa es también uno de los fabricantes de procesadores informáticos más importantes a nivel mundial, en este caso, de telefonía móvil. Qualcomm es la única de las tres compañías seleccionadas que muestra un comportamiento irregular en sus ingresos anuales. Como se observa en la *tabla 5*, la empresa se mantuvo en constante crecimiento hasta 2019, al alcanzar los $24 273 millones, pero en el ejercicio 2020, hubo un receso en los ingresos al contabilizar $23 531 millones. A causa de este descenso en los beneficios, el informe de 2020 no se limita a la recopilación de datos, sino que también aborda las causas de lo ocurrido.

Tabla 5



Fuente: Elaboración propia a partir de los informes anuales de Qualcomm

Para poder entender lo sucedido en esta empresa resulta esencial analizar el contexto que le rodea. Desde 2017, Qualcomm ha estado envuelta en múltiples batallas judiciales contra Apple y Huawei. Esta situación supuso que las dos empresas debiesen enormes cantidades de dinero a Qualcomm en los sucesivos años. A pesar de las numerosas demandas interpuestas bilateralmente, los conflictos se resolvieron fuera de los tribunales, a través de acuerdos de conciliación. Por un lado, Apple se comprometió a emplear los módems 5G de Qualcomm en los iPhone, lo que supuso eliminar a Intel del mercado de chips 5G para teléfonos móviles. Por otro lado, en julio de 2020, Huawei también llegó a un acuerdo de conciliación, además de a un nuevo acuerdo de licencia de

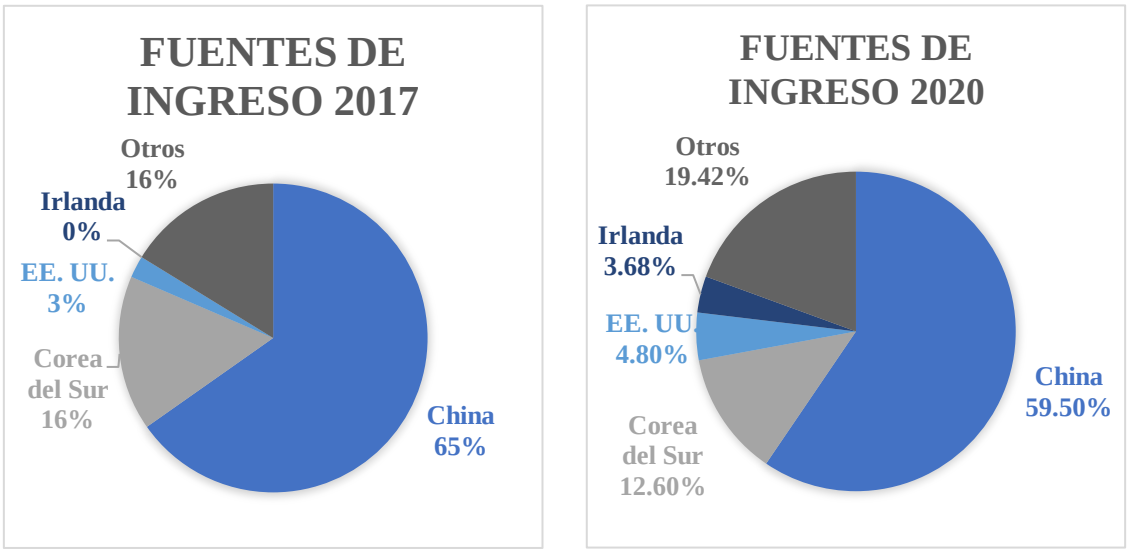
patentes global a largo plazo. Como consecuencia de esta situación, Qualcomm explica en su informe anual la afectación en sus ingresos (Qualcomm Incorporated, 2020):

- 2017: Los ingresos del ejercicio 2017 se vieron afectados negativamente por las acciones emprendidas por Apple y Huawei, dos empresas que no pagaron completamente los derechos adeudados en los últimos tres trimestres de ese año.
- 2018: Los ingresos del ejercicio 2018 se vieron afectados negativamente por el litigio con Apple, parcialmente compensado por los $600 millones pagados en virtud de un acuerdo provisional con Huawei.
- 2019: Los ingresos de explotación del ejercicio 2019 se vieron afectados por un cargo de $275 millones atribuido a una multa impuesta por la Comisión Europea. Sin embargo, se añadieron $4 700 millones en ingresos por licencias registrados en el tercer trimestre del ejercicio 2019 como consecuencia del acuerdo con Apple, lo cual explica el enorme ascenso en los ingresos de ese año.
- 2020: Los ingresos netos del ejercicio 2020 se vieron afectados por la pérdida de $405 millones por deterioro de inversiones no comercializables. Sin embargo, los ingresos de ese año incluyeron $1 800 millones resultantes del acuerdo con Huawei, en el que la empresa abonó la cantidad que debía. En ese año hubo mayores ingresos por licencias de Huawei como consecuencia de los importes adeudados en virtud del acuerdo de conciliación y de las ventas realizadas en los trimestres de marzo y junio en virtud del nuevo acuerdo de licencia global de patentes.

Por lo que concierne a los principales clientes de Qualcomm, la empresa explica que los ingresos por país no son necesariamente indicativos del país en el que los dispositivos que contienen sus productos se venden finalmente a los consumidores. Por ejemplo, los ingresos de China pueden incluir los ingresos relacionados con los envíos de componentes de una empresa con sede en Corea del Sur pero que fabrica dispositivos en China, que luego se venden a los consumidores en Europa y/o Estados Unidos. Aún así, sorprende descubrir, como en el caso de Intel, que la mayor fuente de ingreso de esta empresa es China, seguida de Corea del Sur. Estos dos estados, ya sea por compra de componentes electrónicos, como por su fabricación, representan un enorme porcentaje de sus ingresos. Sin embargo, la presencia de China y Corea del Sur ha ido en descenso entre 2017 y 2020, otorgando un mayor porcentaje a EE. UU.

El análisis de esta empresa revela otro aspecto fundamental para este estudio: la aparición de Irlanda como principal fuente de ingreso. Este país, uno de los 17 Estados miembros de la UE, ingresó en este ranquin en 2018 ($1 millón) y tuvo una gran presencia en 2019 ($2 957 millones). A pesar de su descenso en 2020 ($867 millones), es un factor que podría estar directamente relacionado con las medidas adoptadas por la UE en términos de ciberseguridad. Sin embargo, la investigación de las medidas adoptadas por los cinco actores clave para este caso muestra que Irlanda ha mantenido sus relaciones comerciales con Huawei, por lo que se desestima que su aparición en las fuentes de ingresos de Qualcomm esté relacionada con el conflicto tratado en este trabajo.

Tabla 6. Principales compradores de productos de Qualcomm



Fuente: Elaboración propia a partir de los informes anuales de Qualcomm

Esta empresa ha mostrado una serie de irregularidades en cuanto a sus ingresos anuales y sus principales fuentes de ingreso. Sin embargo, no se considera que tengan relación con las medidas adoptadas por los cinco actores tratados en este trabajo en relación con el conflicto del 5G. Como explica Qualcomm en sus informes anuales, el gran aumento de ingresos en 2019 es consecuencia a las deudas de Apple, acumuladas durante los años anteriores y saldadas a partir de su acuerdo de conciliación. Teniendo en cuenta ese aspecto y los grandes ingresos de Huawei por el mismo motivo, la empresa habría evolucionado como el resto. Por lo que respecta a las fuentes de ingreso, este trabajo desconoce el motivo de la aparición de Irlanda como principal fuente de ingreso a partir de 2018, pero desestima su relación con el caso de Huawei, ya que se trata de un estado que no ha tomado medidas contra la empresa china.

5. CONCLUSIONES

La investigación y el análisis de datos llevados a cabo en este trabajo aportan una visión actualizada y novedosa del caso de Huawei. La hipótesis que plantea este estudio es que EE. UU. acusó a Huawei de ciberespionaje por motivos que van más allá de la protección de la seguridad en las redes. Este trabajo considera que la acusación está centrada en la rivalidad actual entre EE. UU. y China por la hegemonía mundial. La reflexión sobre este caso hace pensar que Washington acusó estratégicamente a Huawei con el fin de frenar los avances de esta empresa en el desarrollo del 5G y atraer a sus clientes hacia empresas de telecomunicaciones estadounidenses, como Intel y Qualcomm, para incrementar el poder económico del país.

La información tratada a lo largo de este estudio permite validar parcialmente la hipótesis. Por una parte, este estudio considera que EE. UU. ha utilizado su influencia mundial para instar a la mayoría posible de actores internacionales a tomar medidas restrictivas hacia Huawei. El hecho de que los estados que han tomado más medidas contra Huawei formen parte de una organización sobre inteligencia (FIORC) en la que se

encuentra EE. UU. puede suponer que se hayan visto condicionados por sus relaciones con este país. De hecho, el Reino Unido y la UE admiten haber tomado ciertas medidas a causa de la presión estadounidense. Además, este trabajo confirma que la economía de Huawei se ha visto afectada por estas decisiones. Los datos financieros muestran descensos en los ingresos de países extranjeros y los propios informes anuales lo vinculan a la prohibición de acceso a las redes 5G en ciertos territorios. Por otra parte, los datos demuestran que la acusación estadounidense no ha influido en el crecimiento de Intel y Qualcomm. El análisis económico de esas empresas permite ver su crecimiento financiero, pero no se puede relacionar con el conflicto entre Huawei y EE. UU., ya que su mercado se ha mantenido, en general, bastante constante. En el caso de Intel, no cabe duda de que la polémica del 5G no ha supuesto ningún cambio en sus relaciones comerciales. Sin embargo, en el caso de Qualcomm, hay ciertas irregularidades que dificultan su relación con el objeto de estudio, como las batallas legales con Apple y Huawei y la pequeña variación en sus fuentes de ingresos, con la aparición de Irlanda. Aun así, no se considera que los datos tratados puedan validar ese aspecto de la hipótesis.

Como conclusión, este trabajo plantea la posibilidad de que los cinco actores hubiesen optado por restringir a Huawei y dotarse de cierta autonomía estratégica en el ámbito tecnológico para no volver a encontrarse en una situación similar. El hecho de que el mayor socio comercial de las empresas de telecomunicaciones estadounidenses seleccionadas sea China puede suponer que Australia, Nueva Zelanda, el Reino Unido, Canadá y la UE hayan decidido invertir los recursos que ya no destinan a Huawei en empresas nacionales. Sin embargo, este es un aspecto pendiente de resolver para futuras investigaciones.

6. BIBLIOGRAFÍA

Arciniegas Londoño, L., & Corzo Ussa, G. D. (2021). *Contextualización de la cuarta revolución industrial, Industria 4.0, Industria 5.0 y tecnología 5G con el sector Defensa y Seguridad.* Perspectivas En Inteligencia, 12(21), 245-258. Recuperado el 14 de enero de 2022, de https://doi.org/10.47961/2145194X.225

Ayllón, B. (2007). *La Cooperación Internacional para el Desarrollo: fundamentos y justificaciones en la perspectiva de la Teoría de las Relaciones Internacionales.* Carta internacional, 2(2), 32-47. Recuperado el 10 de enero de 2022, de https://cartainternacional.abri.org.br/Carta/article/view/416

Baidu. (2022). *Actores transnacionales (非国家行为体).* Baidu (百度). Recuperado el 3 de mayo de 2022, de https://baike.baidu.com/item/%E9%9D%9E%E5%9B%BD%E5%AE%B6%E8%A1%8C%E4%B8%BA%E4%BD%93/7871878

Banco Mundial. (2022a). *Personas que usan Internet (% de la población).* Recuperado el 21 de abril de 2022, de https://datos.bancomundial.org/indicator/IT.NET.USER.ZS

Banco Mundial. (2022b). *Servidores de Internet seguros.* Recuperado el 21 de abril de 2022, de https://datos.bancomundial.org/indicator/IT.NET.SECR

Barbé, E. (1989). *Cooperación y conflicto en las relaciones internacionales. (La teoría del régimen internacional).* Revista CIDOB d'Afers Internacionals, 17, 55-67. Recuperado el 4 de enero de 2022, de https://raco.cat/index.php/RevistaCIDOB/article/view/27818

Blinken, A. J. (2021). *Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace.* Departamento de Estado de Los Estados Unidos. Recuperado el 21 de abril de 2022, de https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/

Buró Federal de Investigaciones (FBI). (2022). *The Cyber Threat*. Departamento de Justicia de Estados Unidos. Recuperado el 17 de marzo de 2022, de https://www.fbi.gov/investigate/cyber

Carmona, I. G. (2020). *La Unión Europea frente al ascenso de China como potencia tecnológica: el caso del 5G.* Boletín IEEE, (18), 383-406. Recuperado el 15 de marzo de 2022, de https://dialnet.unirioja.es/servlet/articulo?codigo=7552059

Carrillo, M. R. *Seguridad en Redes 5G: la acción de la Unión Europea.* Researchgate. Recuperado el 2 de febrero de 2022, de https://www.researchgate.net/profile/Marga-Robles/publication/351022681_Seguridad_en_Redes_5G_la_accion_de_la_Union_Europea/links/607fe6f4881fa114b416eda6/Seguridad-en-Redes-5G-la-accion-de-la-Union-Europea.pdf

Comisión Europea. (2021). *Geopolitical Commission builds on International Partnerships.* International Partnerships. Recuperado el 29 de marzo de 2022, de https://ec.europa.eu/international-partnerships/stories/geopolitical-commission-builds-international-partnerships_en

Comisión Europea. (2022). *Cybersecurity.* Shaping Europe's Digital Future. Recuperado el 17 de marzo de 2022, de https://digital-strategy.ec.europa.eu/en/policies/cybersecurity

Comité Permanente de la Asamblea Popular Nacional. (2012). *Decisión del Comité Permanente de la Asamblea Popular Nacional relativa al fortalecimiento de la protección de la información en Internet (全国人民代表大会常务委员会关于加强网络信息保护的决定).* Consejo de Estado de la República Popular China. Recuperado el 21 de marzo de 2022, de http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm

Consejo de Estado de la República Popular China. (2021). *Goal for 2023: 560 million 5G users in nation.* Comité Permanente de la Asamblea Popular Nacional. Recuperado el 29 de marzo de 2022, de http://english.www.gov.cn/statecouncil/ministries/202107/14/content_WS60ee1a81c6d0df57f98dcce7.html

Consejo de la Unión Europea. (2022). *Una Brújula Estratégica para reforzar la seguridad y la defensa de la UE en el próximo decenio.* Consejo de la Unión Europea - Prensa. Recuperado el 21 de abril de 2022, de https://www.consilium.europa.eu/es/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

Consejo de Seguridad Nacional de los Estados Unidos. (2010). *Transnational Organized Crime: A Growing Threat to National and International Security.* La Casa Blanca, Presidencia de Barack Obama. Recuperado el 22 de marzo de 2022, de https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat

Departamento de Cultura, Medios de Comunicación y Deporte. (2022a). *Government consults on legal direction to restrict Huawei in UK telecoms networks.* Gobierno del Reino Unido. Recuperado el 13 de junio de 2022, de https://www.gov.uk/government/news/government-consults-on-legal-direction-to-restrict-huawei-in-uk-telecoms-networks

Departamento de Cultura, Medios de Comunicación y Deporte. (2022b). *Telecommunications (Security) Act 2021: draft designated vendor direction consultation*. Gobierno del Reino Unido. Recuperado el 13 de junio de 2022, de https://www.gov.uk/government/publications/targeted-consultations-on-proposed-designated-vendor-direction-and-designation-notice/telecommunications-security-act-2021-draft-designated-vendor-direction-consultation

Departamento de Innovación, Ciencia y Desarrollo Económico de Canadá. (2022). *Policy Statement – Securing Canada's Telecommunications System.* Gobierno de Canadá. Recuperado el 13 de junio de 2022, de https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html

Departamento de Seguridad Nacional de los Estados Unidos. (2022a). *5G*. Cybersecurity & Infrastructure Security Agency (CISA). Recuperado el 15 de marzo de 2022, de https://www.cisa.gov/5g

Departamento de Seguridad Nacional de los Estados Unidos. (2022b). *China Cyber Threat Overview and Advisories.* Cybersecurity & Infrastructure Security Agency (CISA). Recuperado el 15 de marzo de 2022, de https://www.cisa.gov/uscert/china

Departamento de Seguridad Nacional de los Estados Unidos. (2022c). *Cybersecurity.* Cybersecurity & Infrastructure Security Agency (CISA). Recuperado el 15 de marzo de 2022, de https://www.cisa.gov/cybersecurity

González, C. G. J. (2003). *Las teorías de la cooperación internacional dentro de las relaciones internacionales.* POLIS: investigación y análisis sociopolítico y psicosocial, 2(3), 115-147. Recuperado el 4 de enero de 2022, de https://www.redalyc.org/pdf/726/72620305.pdf

Huawei. (s.f.). *¿Quién es Huawei?* Información corporativa. Recuperado el 29 de marzo de 2022, de https://www.huawei.com/es/corporate-information

Huawei. (2022). *Huawei Annual Report.* Recuperado el 20 de junio de 2022, de https://www.huawei.com/en/annual-report

Intel Corporation. (2022). *Financial Results*. Recuperado el 20 de junio de 2022, de https://www.intc.com/financial-info/financial-results

Jiménez, A. C., Pérez, J., & Rodríguez, P. (2020). *Descubriendo los desafíos técnicos para la seguridad en las redes 5G*. Análisis del Real Instituto Elcano (ARI), (140), 1. Recuperado el 4 de febrero de 2022, de https://dialnet.unirioja.es/servlet/articulo?codigo=7674266

Ministerio de Seguridad de la República Popular China. (2016). *Ley de Seguridad de las Redes de la República Popular China (中华人民共和国网络安全法)*. Consejo de Estado de la República Popular China. Recuperado el 22 de marzo de 2022, de http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

Ministerio de Seguridad de la República Popular China. (2021). *Reglamento de medidas de seguridad contra el espionaje (反间谍安全防范工作规定)*. Consejo de Estado de la República Popular China. Recuperado el 21 de marzo de 2022, de http://www.gov.cn/gongbao/content/2021/content_5609088.htm

Ministerio de Seguridad de la República Popular China. (2022). *Medidas de control de seguridad de las redes (网络安全审查办法)*. Consejo de Estado de la República Popular China. Recuperado el 22 de marzo de 2022, de http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666430.htm

Naciones Unidas. (2004). *United nations urged to pay more heed to role of 'non-state actors' in approach to global problems*. Coverage and Press Releases. Recuperado el 22 de abril de 2022, de https://www.un.org/press/en/2004/sg2089.doc.htm

Nhan Dan. (2021). *Vietnam y Singapur cooperan en prevención y lucha contra ciberdelito.* Nhan Dan - Órgano central del partido comunista de Vietnam. Recuperado el 24 de abril de 2022, de https://es.nhandan.vn/puente-de-amistad/item/2691480-vietnam-y-singapur-cooperan-en-prevencion-y-lucha-contra-ciberdelito.html

Oficina de Asuntos Exteriores. (2020). *Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets.* Departamento de Justicia de los Estados Unidos. Recuperado el 21 de marzo de 2022, de https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering

Oficina del Procurador de los Estados Unidos, distrito este de Nueva York. (2019). *Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud.* Departamento de Justicia de los Estados Unidos. Recuperado el 21 de marzo de 2022, de https://www.justice.gov/usao-edny/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged

Organización del Tratado Atlántico Norte (OTAN). (2022). *Cyber defence.* OTAN. Recuperado el 28 de marzo de 2022, de https://www.nato.int/cps/en/natohq/topics_78170.htm

Organización para la Seguridad y la Cooperación en Europa (OSCE). (s.f.). *Cyber/ICT Security.* Secretaría de la OSCE. Recuperado el 28 de marzo de 2022, de https://www.osce.org/secretariat/cyber-ict-security

Ortega, A. (2020a). *Geopolítica de la ética en Inteligencia artificial.* Real Instituto Elcano, 23. Recuperado el 10 de marzo de 2020, de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt1-2020-ortega-geopolitica-de-la-etica-en-inteligencia-artificial

Ortega, A. (2020b). *La carrera entre EEUU y China y el futuro de las relaciones transatlánticas.* Real Instituto Elcano, 12. Recuperado el 4 de febrero de 2022 , de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_

CONTEXT=/elcano/elcano_es/zonas_es/dt12-2020-ortega-la-carrera-entre-eeuu-china-y-el-futuro-de-relaciones-transatlanticas

Pauwels, E. (2019). *The New Geopolitics of Converging Risks.* Centro de Investigación de Políticas de la Universidad de las Naciones Unidas (UNU-CPR). Recuperado el 29 de marzo de 2022, de https://collections.unu.edu/eserv/UNU:7308/PauwelsAIGeopolitics.pdf

QUALCOMM Incorporated. (2022). *QUALCOMM Annual Reports*. Recuperado el 20 de junio de 2022, de https://www.annualreports.com/Company/qualcomm-incorporated

Rivas, S. M. (2021). *El ciberespacio como zona de control geopolítico y el papel de las potencias por la supremacía cibernética: China y Estados Unidos.* Revista Relaciones Internacionales, 89-107. Recuperado el 2 de febrero de 2022, de https://revistas.ues.edu.sv/index.php/reinter/article/view/2069

Rodríguez, A. G. (2021). *La UE necesita más diplomacia digital*. CIDOB opinión, 653. Recuperado el 15 de marzo de 2022, de https://www.cidob.org/publicaciones/serie_de_publicacion/opinion_cidob/2021/la_ue_necesita_mas_diplomacia_digital

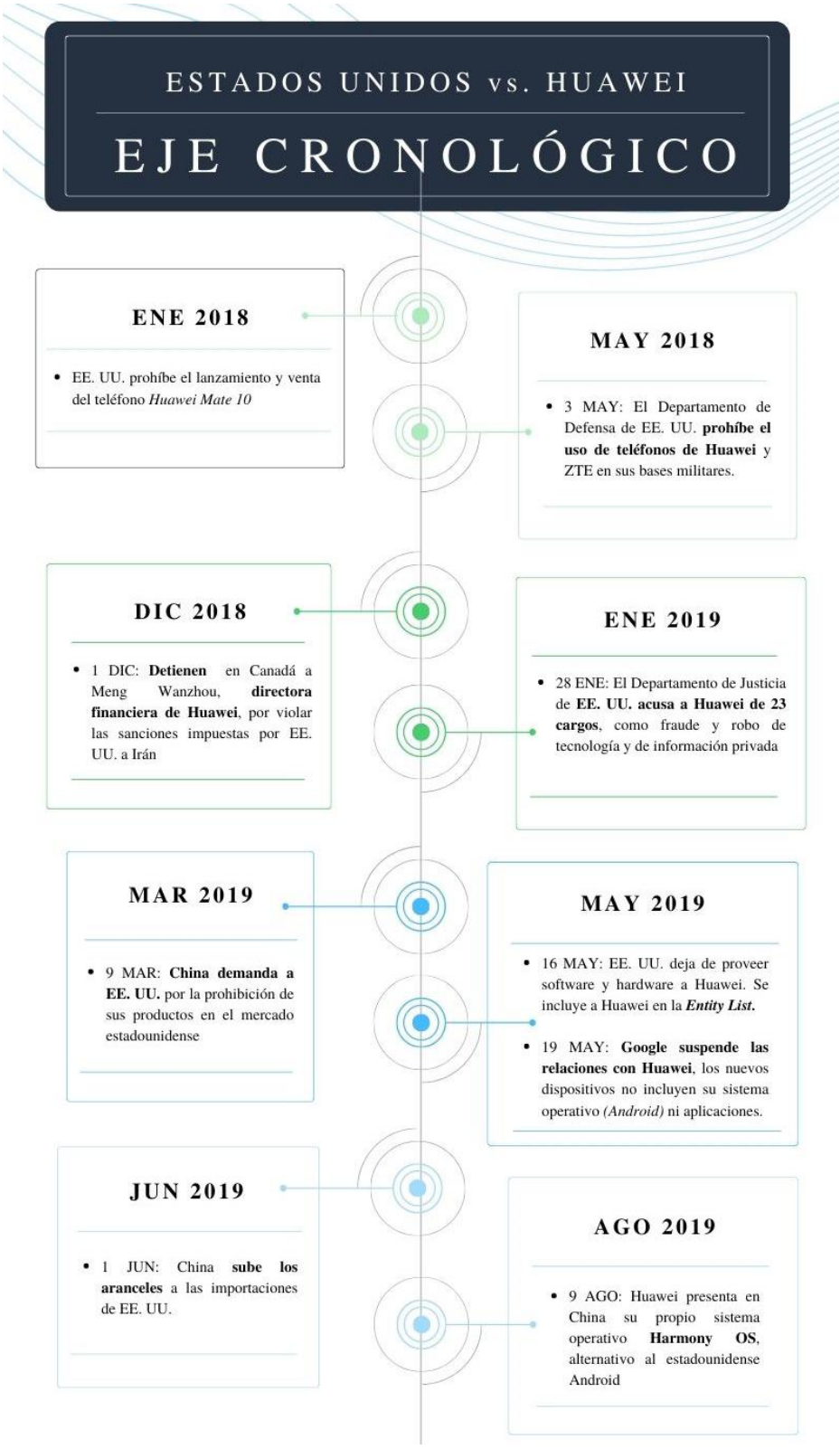
Salazar, A. S. (2020). *Huawei vs. Estados Unidos: seguridad estatal en el contexto internacional.* Hic Rhodus: Crisis capitalista, polémica y controversias, (19), 45-53. Recuperado el 16 de enero de 2022, de https://publicaciones.sociales.uba.ar/index.php/hicrhodus/article/view/6164

Tribunal de Cuentas Europeo. (2009). *The commission's management of non-state actors' involvement in ec development cooperation*. Recuperado el 22 de abril de 2022, de https://www.eca.europa.eu/Lists/ECADocuments/SR09_04/SR09_04_EN.PDF

7. ANEXOS

7.1. ANEXO I

Infografía 1. Eje cronológico del caso Huawei



Fuente: Elaboración propia