



*Estrategias tecnológicas implementadas por China en el
ciberespacio entre 2014 y 2019*

Universidad Abierta Interamericana
Facultad de Derecho y Ciencias Políticas
Trabajo de Investigación Final - Relaciones Internacionales

Alumna: Valeria Yasmil Andretta
DNI: 35423221
Tutor de TIF: Martin Moretti
Año: 2023
Día de entrega: 22 de Agosto del 2023

Facultad de Derecho y Ciencias Políticas

AL DIRECTOR DE LA CARRERA DE
RELACIONES INTERNACIONALES DE LA
UNIVERSIDAD ABIERTA INTERAMERICANA
SEDE BUENOS AIRES

Mg. Juan Carlos Kleywegt
S/D

De mi consideración:

Me dirijo por intermedio de la presente con el objeto de NOTIFICAR la aceptación de tutoría sobre VALERIA YASMIL ANDRETTA para su trabajo de investigación final: “Estrategias tecnológicas implementadas por China en el ciberespacio entre 2014 y 2019”.

Sin otro particular, saludo a esa Dirección con mi consideración más distinguida.

Firma:



Aclaración: Martín Nahuel Moretti

Facultad de Derecho y Ciencias Políticas

Al DIRECTOR DE LA CARRERA DE
RELACIONES INTERNACIONALES DE LA
UNIVERSIDAD ABIERTA INTERAMERICANA
SEDE BUENOS AIRES

Mg. Juan Carlos Kleywegt

S/D

De mi consideración:

Me dirijo por medio de la presente con el objeto de NOTIFICAR el trabajo de investigación final llevado adelante por VALERIA YASMIL ANDRETTA, bajo el título “Estrategias tecnológicas implementadas por China en el ciberespacio entre 2014 y 2019”.

El trabajo explora conceptos sobre cibersoberanía, seguridad y proyección de poder a través de estrategias cibernéticas. Este cumple los requisitos de un trabajo de estas características y fue realizado bajo mi supervisión.

Sin otro particular, saludo a esa Dirección con mi consideración más distinguida.

Firma: 

Aclaración: Martín Nahuel Moretti

Índice:

<i>Introducción:</i>	5
<i>Marco metodológico</i>	6
<i>Marco teórico:</i>	9
<i>1: Estado del arte.</i>	9
<i>2: Conceptos (Soberanía, Soberanía digital, ciberespacio)</i>	17
<i>Capítulo 1 - Antecedentes del caso seleccionado.</i>	21
<i>1.1 Historia de China y su crecimiento como potencia.</i>	22
<i>1.2 : El trabajo de China para constituir su liderazgo en materia tecnológica.</i>	27
<i>1.3: El gran salto tecnológico de HUAWEI</i>	31
<i>Capítulo 2 - Hacia una ciber-soberanía.</i>	41
<i>2.1 : Avance de las TIC'S como capacidad de control en CHINA.</i>	41
<i>2.2: Ley de ciberseguridad China</i>	47
<i>2.4 : Desconexión China de la red mundial.</i>	56
<i>Conclusión.</i>	58
<i>BIBLIOGRAFÍA</i>	61

“No importa qué tan grande sea una compañía de internet, no importa qué tan alto sea su valor de mercado, si depende en gran medida de los países extranjeros para sus componentes principales, y si la "arteria principal" de la cadena de suministro está en manos de otros, es como construir una casa sobre los cimientos de otra persona. No importa lo grande y hermosa que sea, probablemente no soportará el viento y la lluvia, y es posible que sea tan vulnerable como para colapsar con la primera brisa" (Jinping, 2018, “ Foro sobre seguridad cibernética y trabajo informatizado”)

Introducción:

Con el advenimiento de la era digital y la creciente interconexión global, la ciberseguridad y la protección de la soberanía digital han emergido como desafíos cruciales para las naciones en todo el mundo. En este contexto, China ha desplegado una serie de estrategias tecnológicas entre los años 2014 y 2019, buscando salvaguardar su soberanía en el ciberespacio y potenciar su capacidad tecnológica. Estos años marcaron un período de transformación y consolidación en el enfoque de China hacia las cuestiones cibernéticas, marcado por el impulso de iniciativas destinadas a fortalecer su presencia en la esfera digital y protegerse contra posibles amenazas.

Durante este lapso de tiempo, China experimentó una intensa expansión de su infraestructura digital y tecnológica, posicionándose como un actor clave en el escenario cibernético mundial. La implementación de estrategias tecnológicas en el ciberespacio no solo obedeció a una búsqueda de autonomía y seguridad en un entorno digital cada vez más competitivo, sino que también respondió a la creciente necesidad de adaptarse a un contexto en constante evolución, donde la ciberseguridad se ha convertido en una prioridad nacional.

En este contexto, el presente estudio se propone analizar y examinar a profundidad las estrategias tecnológicas adoptadas por China entre 2014 y 2019, en su afán por proteger su soberanía digital y garantizar su capacidad tecnológica. A través del análisis detallado de documentos gubernamentales, investigaciones académicas y noticias relevantes, se busca arrojar luz sobre los objetivos, enfoques y resultados de estas iniciativas. Asimismo, se explorará cómo estas estrategias se entrelazan con el marco político y las relaciones internacionales, en particular con las dinámicas entre China y otros actores globales en el ciberespacio.

En última instancia, esta investigación se propone no solo comprender las estrategias tecnológicas implementadas por China en el ciberespacio durante este periodo crítico, sino también evaluar cómo estas acciones han influido en su posición en el escenario internacional y en las complejas relaciones entre la tecnología, la soberanía y la seguridad en la era digital.

Marco metodológico

Se presenta el marco metodológico utilizado para llevar a cabo el análisis de las estrategias tecnológicas implementadas por un país asiático entre 2014 y 2019 en relación a la ley de seguridad cibernética y el desarrollo de innovaciones tecnológicas. Además, se establecerá el objetivo principal de la investigación, que es analizar cómo buscó proteger su soberanía digital y capacidad tecnológica después de la salida de una empresa líder en tecnología del país en el periodo mencionado.

Para trabajar en ello se plantearon preguntas generales y de forma general se buscaron responder. ¿Cómo se constituyó la soberanía china en el periodo 2014-2019? A su vez, en términos específicos se planteó ¿Cuáles son las estrategias tecnológicas que implementó China para la protección de su Soberanía digital en el periodo 2014-2019?

La hipótesis que se persigue teoriza que China a partir de la implementación de estrategias tecnológicas buscó proteger su soberanía digital y su capacidad tecnológica a partir de la salida de Google del país asiático en el periodo 2014-2019. Las estrategias tecnológicas implementadas por China entre el lapso 2014-2019 se encuentran vinculadas a la ley de ciber seguridad, la desconexión de la red mundial, el crecimiento de Huawei y sus gestiones en el ciberespacio paralelo.

El siguiente estudio sobre China entre los años 2014 y 2019 resulta interesante debido a diversos factores que convergieron en ese periodo y que tuvieron un impacto significativo en su posición como actor relevante en el ciberespacio y las relaciones internacionales.

Durante esos años, China experimentó un rápido crecimiento económico y tecnológico, lo que la llevó a convertirse en una potencia mundial en constante ascenso. Su enfoque en el desarrollo de innovaciones tecnológicas y su búsqueda de la ciber-soberanía se destacaron como pilares fundamentales de su política exterior y su estrategia de seguridad nacional.

El desafío de ganar capacidad para defender su soberanía digital se presentó como una necesidad imperativa para China, especialmente tras la salida de Google del país debido a disputas sobre censura y libertad de expresión. Esto llevó a China a fortalecer su propio ecosistema digital y a desarrollar alternativas locales en áreas clave como motores de búsqueda, redes sociales y servicios en línea.

En este contexto, el periodo 2014-2019 se destacó por la creciente relevancia de China en el ciberespacio y la implementación de estrategias tecnológicas destinadas a proteger su soberanía digital y su capacidad tecnológica. El análisis de este periodo brinda una oportunidad única para comprender cómo China ha enfrentado los desafíos y oportunidades en el ámbito digital y su proyección como actor internacional en el escenario mundial.

Este estudio se basa en un enfoque cualitativo, que permitirá explorar en detalle las estrategias tecnológicas implementadas por el país y su relación con la ley de seguridad cibernética y el desarrollo de innovaciones tecnológicas. Se realizará un análisis exhaustivo de fuentes primarias y secundarias, incluyendo documentos gubernamentales, informes de investigación, artículos académicos y noticias relevantes.

Principalmente el trabajo recorre en analizar como China a partir de la implementación de estrategias tecnológicas buscó proteger su soberanía digital y su capacidad tecnológica a partir de la salida de Google del país asiático en el periodo 2014-2019 y analizar cuáles son las estrategias tecnológicas que implementó China para la protección de su soberanía digital en el periodo 2014-2019.

Para llevar a cabo esta investigación, se utilizaron diferentes métodos de recopilación de datos. En primer lugar, se realizaron una revisión bibliográfica para obtener información relevante sobre las estrategias tecnológicas del país, la ley de seguridad cibernética y el contexto en el que se llevaron a cabo estas acciones. Además, se recopilaron documentos gubernamentales, informes de investigación y otros recursos disponibles para obtener datos específicos sobre las medidas implementadas por el país.

Una vez recopilados los datos pertinentes, se procedió a analizarlos de manera sistemática y rigurosa. Se utilizó técnicas de análisis cualitativo para identificar patrones, tendencias y relaciones entre las estrategias tecnológicas implementadas por el país, la ley de seguridad cibernética y el desarrollo de innovaciones tecnológicas. Se prestará especial atención a los elementos relacionados con la protección de la soberanía digital y la capacidad tecnológica del país.

La interpretación de los resultados se llevó a cabo a partir del análisis de los datos recopilados. Se buscó establecer conexiones y relaciones entre las estrategias tecnológicas implementadas por el país y los objetivos de proteger su soberanía digital y capacidad tecnológica. Se realizaron comparaciones con la situación previa a la salida de la empresa líder en tecnología del país y se evaluó el impacto de las acciones tomadas por el país.

En este último apartado se presentó las conclusiones derivadas del análisis realizado. Se respondió al objetivo principal de la investigación, destacando las principales estrategias tecnológicas implementadas por el país para proteger su soberanía digital y capacidad tecnológica en el periodo 2014-2019. Se discutirán las implicaciones de estos hallazgos y se sugirió posibles direcciones para futuras investigaciones.

Es importante tener en cuenta las posibles limitaciones de este estudio. Entre ellas se encuentran la disponibilidad de datos, la confiabilidad de las fuentes utilizadas y la delimitación temporal establecida. Estas limitaciones se discutirán en el capítulo correspondiente para brindar una visión completa de la investigación.

Marco teórico:

1: Estado del arte.

El presente estudio investiga las estrategias tecnológicas implementadas por China en el ciberespacio entre los años 2014 y 2019, con un enfoque en la protección de su soberanía digital y su capacidad tecnológica. Se plantea la hipótesis de que a raíz de la salida de Google del país asiático, implementó estrategias tecnológicas con el objetivo de salvaguardar su soberanía digital y preservar su capacidad tecnológica.

El marco teórico se basa en una revisión de la literatura existente y aborda diferentes conceptos clave. Se exploró el concepto de soberanía, el concepto de soberanía digital, sociedad de red, ciberespacio, ciberseguridad, la relación de estos conceptos con la teoría de la soberanía estatal y la aplicación en el caso elegido, la relación del caso de estudio con teorías realistas que permitirán entender el contexto del mismo.

El estudio de China entre los años 2014 y 2019, con enfoque en el desafío de ganar capacidad para defender su soberanía, ganar terreno en el ciberespacio, fortalecer su soberanía digital y mejorar su ciberseguridad, se relaciona en los cimientos con diferentes teorías realistas, en este estudio particularmente veremos relación con dos teorías realistas que abordan aspectos relevantes en el ciberespacio y las relaciones internacionales.

La primera teoría realista relevante es la teoría de la seguridad nacional y el poder estatal. En este sentido, autores como Kenneth Waltz, en su obra "Theory of International Politics" (1979), enfatizan que los Estados actúan en función de sus propios intereses y buscan maximizar su poder para garantizar su seguridad y supervivencia. En el caso de China, su búsqueda de ciber-soberanía y capacidad tecnológica se alinea con esta teoría, ya que el país ha buscado consolidar su poderío económico, político y militar para proteger su integridad territorial y sus intereses nacionales en el ámbito digital.

La segunda teoría realista relevante es la teoría de las relaciones internacionales basadas en el poder y la competencia. Autores como John Mearsheimer, en su obra "The Tragedy of Great Power Politics" (2001), sostienen que en el sistema internacional existe una lucha por el poder y la influencia entre los Estados, lo que puede generar conflictos y rivalidades. En el caso de China, sus operaciones en el ciberespacio y su búsqueda de ciber-soberanía han entrado en conflicto con otros actores internacionales, como Estados Unidos, debido a la competencia por el control de recursos, información y la influencia en el ámbito digital.

El concepto de soberanía es fundamental en las relaciones internacionales y se refiere al principio de autoridad y poder supremo que un Estado tiene sobre su territorio, su gobierno y su población. La soberanía implica la capacidad de un Estado para tomar decisiones autónomas y ejercer su autoridad sobre asuntos internos y externos sin interferencia de otros Estados.

En términos generales la soberanía se basa, podríamos interpretar, en dos elementos principales: el poder de un Estado para gobernarse a sí mismo y la capacidad de actuar como una entidad política independiente. Esto implica que el Estado tiene el derecho y la responsabilidad de tomar decisiones en materia de política interna, legislar leyes, establecer políticas económicas, mantener el orden y la seguridad, y representar a su nación en el ámbito internacional.

El concepto de soberanía ha evolucionado a lo largo de la historia y ha sido objeto de debate en las teorías de las relaciones internacionales. Hay diferentes enfoques y perspectivas sobre la soberanía, como el enfoque realista que destaca el poder y la autonomía de los Estados, el enfoque liberal que considera la soberanía como un principio para la cooperación y el respeto mutuo, y el enfoque constructivista que enfatiza la construcción social de la soberanía.

Es importante destacar que la soberanía de un Estado no es absoluta y puede estar sujeta a ciertas limitaciones y responsabilidades en el ámbito internacional. Los Estados también están vinculados por el derecho internacional y los acuerdos y tratados internacionales que han ratificado, lo que puede restringir su capacidad de acción en ciertos asuntos.

Thomas Hobbes hizo importantes contribuciones al concepto de soberanía en las relaciones internacionales. Hobbes (1651) sostenía que el estado de naturaleza, caracterizado por la ausencia de un gobierno central y la presencia de un conflicto constante, era caótico y peligroso. Para evitar esta situación, el autor argumentó a favor de la creación de un poder soberano absoluto.

Según Hobbes (1651), la soberanía es la autoridad suprema y exclusiva que posee un Estado sobre su territorio y su población. Este poder soberano debe ser ejercido de manera absoluta y sin restricciones, ya que su objetivo principal es garantizar la paz y la seguridad de los individuos. Este argumentó que la soberanía es necesaria para mantener el orden y evitar la guerra constante que prevalece en el estado de naturaleza.

En el contexto de las relaciones internacionales, el autor consideraba que los Estados también están inmersos en un estado de naturaleza, donde la competencia, la desconfianza y el conflicto son inevitables. Por lo tanto, los Estados deben buscar la soberanía absoluta para establecer un orden y evitar la anarquía en las relaciones entre ellos.

Hobbes (1651) enfatizó la importancia de la autoridad soberana y su capacidad para tomar decisiones y mantener la estabilidad en el sistema internacional. Su teoría sirve como base para entender el principio de no intervención en los asuntos internos de otros Estados y la necesidad de un gobierno centralizado y fuerte para garantizar la paz y la seguridad en las relaciones internacionales.

Jean Bodin (1576) formula, respecto al concepto de soberanía, en las relaciones internacionales se basan en la idea de que el Estado debe tener un poder absoluto e indivisible sobre su territorio y población, sin estar sujeto a ninguna autoridad externa. La soberanía garantiza la independencia política y jurídica de los Estados y es esencial para su interacción en el ámbito internacional.

Este autor definió la soberanía como el poder absoluto e indivisible que recae sobre el Estado y que le otorga autoridad suprema sobre su territorio y población. Según Bodin(1576), el soberano es aquel que tiene el poder final de tomar decisiones y hacer cumplir la ley dentro de un Estado. Esta autoridad soberana no está sujeta a ningún poder superior ni a restricciones externas.

Uno de los fundamentos principales de Bodin (1576), en cuanto al concepto de soberanía es la idea de que el Estado debe tener la capacidad de ejercer su autoridad sin interferencias externas. Para el autor, la soberanía implica independencia política y jurídica, lo que implica que ningún otro poder o entidad puede imponer su voluntad sobre el Estado soberano.

Este autor también enfatizó la importancia de la unidad y la indivisibilidad de la soberanía. Sostenía que la soberanía no puede ser compartida, ya que cualquier división o fragmentación del poder soberano conduciría a conflictos y disputas internas.

En el contexto de las relaciones internacionales, Bodin (1576), estableció que la soberanía es esencial para la existencia de los Estados y su capacidad de interactuar entre sí. La soberanía implica la igualdad jurídica de los Estados y su derecho a tomar decisiones autónomas sin interferencias externas.

Además, se incluyen aportes de autores contemporáneos como Joseph Nye (2004), quien introduce el concepto de "soberanía inteligente" en el contexto digital, donde se reconoce la necesidad de equilibrar la soberanía estatal con la interdependencia y la gobernanza global en el ciberespacio.

Según Nye, la soberanía inteligente implica que los Estados deben adaptarse y utilizar de manera estratégica las herramientas de la globalización y la interdependencia para preservar y promover sus intereses nacionales. En lugar de una concepción tradicional de la soberanía que se basa en el control absoluto y la no interferencia en los asuntos internos, la soberanía inteligente implica la capacidad de los Estados para aprovechar las oportunidades que ofrece la interconectividad global. Argumenta que los Estados no pueden simplemente aislarse o resistir los flujos transnacionales de información, economía y poder en la era de la globalización. En cambio, deben desarrollar estrategias inteligentes para influir en estos flujos y proteger sus intereses nacionales. Esto implica utilizar herramientas como la diplomacia, la cooperación internacional, las alianzas y las redes de influencia para alcanzar objetivos y resolver problemas globales

En el contexto de la soberanía inteligente, Nye (2004) también destaca la importancia del poder blando (soft power). Según él, los Estados pueden fortalecer su posición y su influencia en el escenario internacional no solo a través del poder militar o económico, sino también mediante la atracción y la persuasión. El poder blando se basa en los valores, la cultura, la diplomacia, la tecnología y otros medios para generar apoyo y cooperación en lugar de recurrir a la coerción.

En cuanto al ciberespacio, se examina su impacto en las relaciones internacionales y en la soberanía digital. Se recurre a autores clásicos como Carl von Clausewitz, quien resalta la relevancia de la tecnología en el campo de batalla y su aplicación al ciberespacio. Asimismo, se consideran aportes de autores contemporáneos como Manuel Castells y Ronald Deibert. Castells introduce el concepto de "sociedad red".

La "sociedad red" se refiere a un nuevo tipo de estructura social y organización basada en las redes de comunicación y la tecnología de la información. Esta transformación ha sido impulsada por la revolución digital y ha tenido un impacto significativo en diversos ámbitos, incluyendo las relaciones internacionales.

En el contexto de las relaciones internacionales, la sociedad red ha alterado la forma en que los actores estatales y no estatales interactúan y se relacionan entre sí. Castells argumenta

que las redes de comunicación y la tecnología de la información han debilitado las fronteras geográficas y han facilitado la creación de nuevas formas de cooperación y conflicto a nivel transnacional.

En palabras de Castells: "La lógica de la red se ha infiltrado en todos los aspectos de la vida social, incluyendo las relaciones económicas, políticas y culturales. Como resultado, los actores y las instituciones se ven inmersos en relaciones que trascienden las estructuras jerárquicas y territoriales tradicionales" (Castells, 1996).

En el ámbito de las relaciones internacionales, la sociedad red ha permitido un mayor acceso a la información, la comunicación y la participación en asuntos globales. Los actores no estatales, como las organizaciones no gubernamentales (ONG), las redes transnacionales y los movimientos sociales, han encontrado nuevas formas de influir en la agenda internacional y ejercer presión sobre los Estados.

Al mismo tiempo, la sociedad red ha desafiado el monopolio tradicional del Estado-nación en la toma de decisiones internacionales. Castells argumenta que la sociedad red ha erosionado la autoridad y el poder de los Estados, ya que ahora los actores no estatales pueden organizar y movilizar recursos a nivel transnacional sin depender de las estructuras estatales convencionales.

Sin embargo, es importante tener en cuenta que el concepto de sociedad red de Castells no implica una desaparición completa de los Estados-nación o un declive total de la geopolítica. En cambio, sugiere que los Estados deben adaptarse a la nueva realidad de la sociedad red y encontrar formas de articular su soberanía y ejercer influencia en un entorno globalizado y altamente interconectado.

Mientras que Deibert aborda el tema de la sociedad red desde una perspectiva centrada en el ciberespacio y la política digital. Si bien Deibert se basa en los conceptos de Castells, agrega una dimensión crítica al analizar los desafíos y riesgos que surgen en la era de la información.

Se argumenta que, si bien la sociedad red ofrece nuevas oportunidades y formas de interconexión, también plantea importantes preocupaciones en términos de ciberseguridad, privacidad y derechos digitales. Según Deibert: "La era de la información ha traído consigo una nueva forma de poder, donde el control y la vigilancia son ejercidos no solo por los Estados, sino también por actores corporativos y grupos delictivos que operan en el ciberespacio" (Deibert, 2013).

En este sentido, Deibert destaca la importancia de comprender la dinámica política del ciberespacio y las implicaciones que tiene para las relaciones internacionales. La sociedad red, no solo ha generado oportunidades de cooperación y comunicación global, sino también desafíos en términos de seguridad y control.

Deibert (2013) se enfoca especialmente en el concepto de "black code" o "código negro", que se refiere a las prácticas de vigilancia y control que se llevan a cabo en el ciberespacio. Argumenta que, en la sociedad red, tanto los Estados como los actores no estatales utilizan tecnologías de vigilancia y censura para ejercer control sobre la información y restringir la libertad en línea.

En este contexto, las tecnologías como la censura en internet, la vigilancia masiva, los cortafuegos y los sistemas de filtrado se utilizan para ejercer control sobre el ciberespacio y proteger la soberanía digital. Estas herramientas tecnológicas permiten a los Estados regular y restringir el acceso a ciertos contenidos, supervisar las comunicaciones en línea y proteger su infraestructura digital.

Las teorías de la sociedad red de Castells y la perspectiva crítica de Deibert ofrecen un marco conceptual para comprender cómo se utilizan las tecnologías en el ámbito tecnológico para ejercer control y proteger la soberanía digital. Estas teorías resaltan la importancia de la gestión de la información, la comunicación y la conectividad en la sociedad actual, así como los desafíos y riesgos asociados con el control y la vigilancia en el ciberespacio.

El concepto de ciberespacio se refiere al ámbito virtual o digital creado por las redes de comunicación electrónica, especialmente Internet. Es un espacio en el que las interacciones humanas, la transferencia de datos y la comunicación ocurren a través de medios electrónicos y tecnologías de la información.

El profesor Manuel Castells, en su obra "La era de la información: economía, sociedad y cultura", amplía el concepto de ciberespacio y lo relaciona con la interconexión global de redes de comunicación. Según Castells, el ciberespacio es "el nuevo medio de comunicación y coordinación global basado en la interconexión de redes de computadoras a través de Internet" (Castells, 1996).

El ciberespacio es un espacio virtual en el que las actividades humanas, como la comunicación, el comercio, la información y el entretenimiento, se llevan a cabo utilizando tecnologías digitales. Es un espacio en el que las barreras físicas y geográficas se vuelven

menos relevantes, permitiendo la interconexión global y la transferencia instantánea de información.

En este aspecto dentro del marco del ciberespacio surge otras definiciones de soberanía, como la soberanía Digital. Este concepto que también acuña Deibert , implica que cada Estado tiene la capacidad y la responsabilidad de regular y gobernar su propio ciberespacio de acuerdo con sus leyes y políticas nacionales. Esto incluye el control y la gestión de infraestructuras de tecnologías de la información y comunicación (TIC), la protección de datos y la privacidad de los ciudadanos, y la implementación de políticas de ciberseguridad.

Según el profesor Christopher Balding, "la soberanía digital se basa en la capacidad de un Estado para desarrollar y mantener su propia infraestructura de tecnología digital y evitar la dependencia de empresas o países extranjeros" (Balding, 2018).

Es importante destacar que el concepto de soberanía digital está en constante evolución y enfrenta desafíos en un mundo interconectado. La soberanía digital puede entrar en conflicto con la libre circulación de información y el principio de neutralidad de la red, y plantea preguntas sobre los límites de la regulación estatal en el ciberespacio.

La ciberseguridad es otro aspecto fundamental en este estudio. Se aborda el concepto y se explora su relación con la protección de la soberanía digital y la capacidad tecnológica.

La ciberseguridad se refiere a la protección de los sistemas informáticos, las redes y la información digital contra amenazas, ataques y vulnerabilidades. Consiste en salvaguardar la confidencialidad, integridad y disponibilidad de los datos, así como garantizar la privacidad y protección contra el acceso no autorizado.

Según el National Institute of Standards and Technology (NIST) de Estados Unidos, la ciberseguridad se define como "la protección de la información y la propiedad intelectual de los sistemas informáticos, las redes y los servicios de información de las amenazas y los ataques digitales" (NIST, 2018).

Bruce Schneier, experto en seguridad informática, sostiene que la ciberseguridad es "la protección de los activos de información mediante la mitigación del riesgo de ataques a la confidencialidad, integridad y disponibilidad de esos activos" (Schneier, 2000).

En este punto se destaca la importancia de la colaboración entre expertos técnicos, que comprenden los aspectos técnicos de la ciberseguridad, y profesionales de políticas públicas, que pueden formular y promover políticas adecuadas para abordar los desafíos en este

ámbito. Destaca la importancia de integrar conocimientos en psicología y ciencias sociales en el campo de la ciberseguridad. Comprender el comportamiento humano, las motivaciones y las reacciones psicológicas frente a las amenazas cibernéticas puede ayudar a diseñar medidas de seguridad más efectivas. Schneier (2000) resalta la importancia de considerar los aspectos legales y éticos en el ámbito de la ciberseguridad. Esto implica evaluar las implicaciones de las medidas de seguridad en términos de privacidad, derechos individuales y justicia, buscando un equilibrio adecuado entre la seguridad y otros valores fundamentales.

En contrapartida, las teorías de Tim Maurer (2018) se basan en un enfoque multidimensional de la ciberseguridad, la promoción de una gobernanza inclusiva y cooperativa, la consideración de la dimensión humana y el equilibrio entre seguridad y derechos fundamentales. Estos pilares proporcionan un marco conceptual para abordar los desafíos en el ciberespacio y promover un entorno digital seguro y confiable. Propone un enfoque multidimensional de la ciberseguridad que abarca aspectos técnicos, políticos, económicos y sociales. Reconoce que la seguridad cibernética no se limita únicamente a la tecnología, sino que también implica considerar las dimensiones políticas, económicas y sociales que influyen en la seguridad en el ciberespacio. El autor enfatiza la importancia de considerar la dimensión humana en la ciberseguridad y la gobernanza digital. Reconoce que las acciones y decisiones humanas desempeñan un papel fundamental en la seguridad cibernética, y aboga por comprender y abordar los factores humanos, como el comportamiento, la conciencia y la educación, para mejorar la seguridad en el ciberespacio.

Este autor analiza cómo el ciberespacio puede ser tanto una herramienta para proteger como para amenazar la seguridad. Reconoce que el ciberespacio proporciona oportunidades sin precedentes para fortalecer la seguridad, la comunicación y el intercambio de información, pero también plantea riesgos y desafíos en términos de ciberataques, espionaje cibernético y delitos informáticos.

El ciberespacio ofrece nuevas formas de protección, permitiendo la implementación de medidas de seguridad avanzadas, la detección temprana de amenazas y la respuesta rápida a incidentes. También facilita la cooperación internacional en la lucha contra el cibercrimen y el intercambio de información sobre amenazas cibernéticas, lo que contribuye a mejorar la seguridad en general.

Sin embargo, el mismo ciberespacio que proporciona estas oportunidades también puede ser utilizado como una herramienta de amenaza. Los actores maliciosos pueden aprovechar las

vulnerabilidades y debilidades en los sistemas digitales para llevar a cabo ciberataques, robo de datos, sabotaje y espionaje cibernético. Además, el anonimato y la capacidad de ocultar la identidad en el ciberespacio dificultan la atribución de los ataques, lo que puede generar un ambiente propicio para la proliferación de amenazas.

La ciberseguridad es fundamental en la actualidad debido al crecimiento exponencial de las amenazas cibernéticas, como el malware, los ataques de hackers, el robo de datos y el espionaje cibernético. La protección de los sistemas y la información se ha convertido en una preocupación clave tanto para individuos como para organizaciones, gobiernos y entidades internacionales.

El siguiente marco teórico proporciona una base sólida para investigar las estrategias tecnológicas implementadas en el ciberespacio entre 2014 y 2019, centrándose en la protección de su soberanía digital y su capacidad tecnológica. El análisis de los conceptos de soberanía digital, ciberespacio, ciberseguridad y su relación con autores clásicos como Thomas Hobbes y con autores contemporáneos como Joseph Nye, Manuel Castells, Ronald Deibert, Bruce Schneier y Tim Maurer, permite una comprensión amplia y contextualizada de este fenómeno en el entorno contemporáneo.

2: Conceptos (Soberanía, Soberanía digital, ciberespacio)

La revolución tecnológico-digital, que se desarrolló, principalmente, durante la segunda mitad del siglo XX, provocó cambios radicales a nivel mundial. El avance en el ámbito de las tecnologías de la información y de la comunicación (TIC) ha conducido al mundo hacia una era donde la interdependencia y la globalización lideran todas las relaciones existentes. Al mismo tiempo, el ciberespacio ha acortado distancias, ha permitido que las fronteras puedan traspasarse y los límites se disuelvan.

Situados hoy en el siglo XXI, podemos decir que también, dicha revolución, ha inaugurado un nuevo escenario de disputa entre los Estados. Anteriormente, todas las guerras desatadas habían tenido lugar en territorios físicos, utilizando armas de fuego y el propio cuerpo para atacar y defenderse, hoy en día el territorio de lucha es virtual, y las armas utilizadas tomaron forma de software, utilizadas como virus para atacar a otros sistemas informáticos o para recolectar información que luego pueda ser utilizada con diversos fines.

En líneas con lo anteriormente expuesto nuestro caso de estudio abordará como la construcción de una soberanía digital es sinónimo de capacidad en un el orden mundial. El trabajo aborda conceptos desde las teorías de realismo clásico, realismo ofensivo y realismo defensivo. Para el realismo defensivo indicamos que “introduce el equilibrio ofensiva-defensiva en la explicación del comportamiento de los Estados” (J. Jordan, 2013).

Particularmente se abordarán las medidas tomadas por China que ha implementado a lo largo de su camino por obtener capacidad tecnológica. Varias estrategias tecnológicas para proteger su soberanía digital. A continuación, mencionaré algunas de las más relevantes:

El Gran Cortafuegos o "Escudo Dorado" es un sistema de filtrado y bloqueo de contenido en línea que impide el acceso a ciertos sitios web y servicios en línea considerados peligrosos o políticamente sensibles.

La regulación y censura del contenido en línea: Tiene una serie de leyes y regulaciones para regular el contenido en línea y proteger su seguridad nacional. Por ejemplo, la "Ley de Ciberseguridad" de 2017 establece requisitos de seguridad para las empresas tecnológicas y les exige almacenar los datos de los usuarios chinos en servidores ubicados en el país.

La promoción de una "internet soberana": como ya mencioné, busca establecer su propia "internet soberana" independiente, mediante la creación de su propio ecosistema digital y la reducción de su dependencia de las empresas y tecnologías extranjeras.

La inversión en tecnologías emergentes: Se ha invertido mucho en tecnologías emergentes como la inteligencia artificial, la computación en la nube y la tecnología 5G. Estas tecnologías pueden ser clave para el desarrollo de una "internet soberana" y la reducción de la dependencia de las tecnologías extranjeras.

La vigilancia en línea: el gobierno chino tiene un sistema de vigilancia en línea que monitorea y rastrea el comportamiento de los usuarios en línea. Esto puede ser utilizado para detectar y prevenir actividades consideradas peligrosas para la seguridad nacional.

China ha implementado varias estrategias tecnológicas para proteger su soberanía digital, incluyendo el Gran Cortafuegos, como mencionamos anteriormente. La regulación y censura del contenido en línea, la promoción de una "internet soberana", la inversión en tecnologías emergentes y la vigilancia en línea. Se han tomado diversas medidas para proteger su ciberespacio, como la promulgación de leyes y regulaciones sobre la seguridad cibernética,

la creación de fuerzas de ciberseguridad, la mejora de las infraestructuras y tecnologías de la información, entre otras.

Estas medidas tienen como objetivo proteger a esta potencia de las amenazas cibernéticas externas y garantizar que el país tenga un control sobre su ciberespacio y su información, lo que se considera una defensa. Sin embargo, también ha sido acusada de llevar a cabo actividades ofensivas en el ciberespacio, como ciber espionaje y ciberataques, lo que ha generado tensiones con otros países.

La aplicación del concepto de equilibrio ofensiva-defensiva (Jervis, 1976) en la política cibernética de este País implica encontrar un equilibrio entre su capacidad para proteger su ciberespacio y su capacidad para proyectar su poder en el ciberespacio, y mantener este equilibrio es crucial para garantizar la estabilidad y la paz en el sistema internacional.

El equilibrio ofensiva-defensiva es crucial en las relaciones internacionales, ya que si un Estado se vuelve demasiado ofensivo, otros Estados pueden sentirse amenazados y unirse en su contra. Por otro lado, si un Estado se vuelve demasiado defensivo, puede perder su capacidad para influir en los asuntos internacionales y puede ser considerado un Estado débil.

El concepto de equilibrio ofensiva-defensiva de Paul Jordan (2013) explica cómo los Estados buscan mantener un equilibrio entre su capacidad de expandirse y su capacidad de protegerse a sí mismos y cómo este equilibrio es fundamental para la estabilidad y la paz en el sistema internacional.

La idea de equilibrio ofensiva-defensiva de Jordan (2013) se puede relacionar con las medidas tomadas por China para proteger su ciberespacio, ya que el objetivo principal de estas medidas es garantizar la seguridad nacional y la soberanía en el ciberespacio, lo que se considera una defensa.

El país de estudio experimentado un rápido crecimiento económico y ha alcanzado una posición de liderazgo en la fabricación y exportación de productos electrónicos, incluyendo smartphones, tablets y otros dispositivos conectados a Internet. también ha promovido una estrategia de desarrollo económico basada en la innovación y la tecnología, lo que ha llevado a la creación de empresas tecnológicas chinas líderes como Huawei, Tencent y Alibaba.

Sin embargo, la competencia entre Estados Unidos y China en el ciberespacio se ha intensificado en los últimos años, ya que ambas potencias buscan proteger sus intereses

nacionales y promover sus agendas en el ciberespacio. Además, las acusaciones mutuas de ciberespionaje, ciberataques y otros delitos cibernéticos han contribuido a la creciente tensión entre ambos países.

Desde la década de 1990, Estados Unidos ha liderado el desarrollo y la expansión de la tecnología de la información y las comunicaciones, lo que ha llevado a la creación de empresas de tecnología líderes a nivel mundial como Google, Facebook, Amazon y Apple, entre otras. Además, Estados Unidos ha sido un líder en la promoción de la libertad de expresión, la privacidad en línea y la apertura de Internet.

En este contexto la disputa entre el gigante Asiático y Estados Unidos por el ciberespacio se ha vuelto cada vez más relevante en los últimos años. China, durante el periodo 2014-2019, ha buscado de manera activa defender su soberanía digital y proteger sus intereses nacionales en el ámbito de las tecnologías de la información y las comunicaciones. Para ello, ha implementado una serie de estrategias tecnológicas y políticas de ciberseguridad, como la ley de ciberseguridad promulgada en 2016, que le otorgan mayor control y capacidad de regulación sobre el ciberespacio dentro de su territorio.

En este proceso, se han identificado factores tanto externos como internos que han impulsado el desarrollo de estas políticas y estrategias. En cuanto a los factores externos, la rivalidad con Estados Unidos y otras potencias ha sido un factor determinante. China ha visto la necesidad de ganar autonomía y capacidad tecnológica en el ciberespacio para reducir su dependencia de las empresas de tecnología estadounidenses y salvaguardar su soberanía digital frente a posibles injerencias extranjeras.

Por otro lado, factores internos como el objetivo de mantener la estabilidad social y política, así como proteger su sistema ideológico, han llevado a China a reforzar su control en el ciberespacio. La ciberseguridad se ha convertido en una prioridad para el gobierno chino como parte de su estrategia para mantener la legitimidad del Partido Comunista y evitar el surgimiento de movimientos de protesta o críticas en línea que puedan amenazar la estabilidad del país.

Podemos indicar que la disputa por el ciberespacio entre China y Estados Unidos se ha convertido en un tema central en las relaciones internacionales debido a la competencia económica y tecnológica, así como a las tensiones políticas y estratégicas entre ambas potencias. La búsqueda de soberanía digital y capacidad tecnológica por parte de China se

enmarca en este contexto más amplio y refleja la importancia cada vez mayor que el ciberespacio tiene en la arena global.

Capítulo I - Antecedentes del caso seleccionado.

China ha experimentado un crecimiento impresionante en su capacidad tecnológica y económica a lo largo de su historia. Desde la década de 1970, el país ha llevado a cabo importantes reformas económicas y políticas que han impulsado su desarrollo tecnológico y su integración en la economía global. En particular, la adopción de políticas de apertura al comercio internacional y la inversión extranjera le han permitido convertirse en una potencia manufacturera y exportadora, con un enfoque cada vez mayor en la tecnología y la innovación.

Antes de 2014, China había implementado políticas de soberanía digital que buscaban proteger su ciberespacio de influencias externas y controlar el flujo de información en línea. La Gran Muralla Cortafuegos, un sistema de filtrado y censura de Internet, fue uno de los principales instrumentos utilizados por el gobierno chino para mantener el control sobre el acceso a la información en línea y restringir el contenido considerado políticamente sensible.

Entre 2014 y 2019, continuaron fortaleciendo su enfoque en la soberanía digital mediante la promulgación de la ley de ciberseguridad en 2016. Esta ley otorgó al gobierno amplios poderes para controlar y regular el ciberespacio dentro del país, lo que generó preocupaciones sobre la privacidad en línea y la libertad de expresión. Además, se intensificaron las medidas para bloquear y censurar contenido considerado perjudicial para los intereses nacionales.

El crecimiento económico y tecnológico del país de estudio durante este periodo le ha permitido posicionarse como un fuerte actor internacional en diversos ámbitos. La inversión en investigación y desarrollo, así como el fomento de la innovación tecnológica, han impulsado su capacidad para competir en el mercado global de tecnología. Esto ha llevado a China a desafiar la dominancia tecnológica de Estados Unidos, lo que ha generado tensiones y rivalidades entre ambas potencias.

La rivalidad entre China y Estados Unidos se ha manifestado en disputas comerciales, restricciones a la inversión y tensiones en materia de ciberseguridad. Ambos países han

adoptado políticas y estrategias para proteger sus intereses en el ciberespacio y garantizar la seguridad de sus redes y datos. La competencia por el dominio tecnológico y la influencia en el ciberespacio ha llevado a una nueva dinámica de relaciones internacionales y ha contribuido a la reconfiguración del orden mundial.

1.1 Historia de China y su crecimiento como potencia.

Durante los años 1960 y 1970 China experimentó un período de aislamiento y llevó a cabo la Revolución Cultural. El aislamiento se debió principalmente a la política de Mao Zedong y su deseo de mantener el control absoluto del Partido Comunista. Mao consideraba que el contacto con el mundo exterior, especialmente con las potencias capitalistas, era una amenaza para la revolución comunista y la pureza ideológica.

La Revolución Cultural que tuvo lugar entre 1966 y 1976 fue una campaña ideológica y política impulsada por Mao para reafirmar su liderazgo y erradicar a los elementos considerados burgueses o revisionistas dentro del Partido Comunista y la sociedad china. Se caracterizó por la movilización de las masas, la promoción de la lucha de clases y la supresión de la intelectualidad, lo que llevó a la persecución, represión y purga de millones de personas.

Durante este período se promovió la adoración a Mao como líder supremo, se fomentaron los cultos a su personalidad y se impulsó la juventud a participar en el movimiento revolucionario. Se crearon las llamadas "Brigadas Rojas" conformadas principalmente por jóvenes estudiantes, quienes se encargaron de llevar a cabo la persecución y la violencia contra aquellos considerados enemigos del régimen.

Según el historiador Roderick MacFarquhar en su obra "The Origins of the Cultural Revolution" (1983) la Revolución Cultural fue un intento de Mao Zedong de revitalizar el espíritu revolucionario y eliminar a los elementos burgueses dentro del Partido Comunista y la sociedad china.

Durante los años 1960 y 1970 las relaciones entre China y Estados Unidos experimentaron tensiones significativas. Estas tensiones se debieron en gran medida a diferencias ideológicas, la Guerra Fría y la rivalidad entre las dos superpotencias: Estados Unidos y la Unión Soviética.

Estos dos países se encontraban en diferentes polos ideológicos y políticos. Mientras Estados Unidos apoyaba a Taiwán y consideraba a la República de China como el gobierno legítimo de toda China, China continental estaba bajo el control del Partido Comunista y se consideraba a sí misma como la única China legítima.

La participación de Estados Unidos en la Guerra de Corea y su alianza con Taiwán generaron tensiones adicionales. China veía a Estados Unidos como un imperialista y un obstáculo para su objetivo de unificar China bajo un gobierno comunista.

A fines de los años 1960 las relaciones entre los hegemones comenzaron a experimentar un cambio. En 1972, el presidente Richard Nixon visitó China, lo que marcó un hito en las relaciones bilaterales y condujo a la normalización de los lazos diplomáticos entre ambos países.

Henry Kissinger en su libro "On China" (2011) indica que el acercamiento entre China y Estados Unidos fue motivado por intereses estratégicos y la percepción de que Este podía ser un contrapeso a la Unión Soviética.

La historia del crecimiento económico y tecnológico de China es fundamental para entender su posición actual como potencia mundial. A lo largo de las últimas décadas, ha experimentado un crecimiento impresionante, impulsado por reformas económicas y políticas gubernamentales que han fomentado la apertura y la modernización.

Han pasado de ser una economía agraria y centralizada a convertirse en la segunda economía más grande del mundo. Su crecimiento se ha basado en la promoción de la inversión extranjera, la industrialización y la apertura gradual al comercio internacional. Este proceso ha sido clave para la integración de China en la economía global y su ascenso como actor relevante en los asuntos económicos internacionales.

Paralelamente, el desarrollo tecnológico ha sido un componente crucial en el crecimiento de China. A través de inversiones en investigación y desarrollo, así como la adquisición de conocimientos y tecnología extranjera, ha logrado avances significativos en sectores clave como la inteligencia artificial, las telecomunicaciones y la tecnología digital. Estos avances tecnológicos han permitido a impulsar su competitividad y expandir su influencia en el escenario mundial.

China ha adoptado una serie de estrategias de soberanía digital para proteger su posición económica y tecnológica en el escenario mundial. Estas estrategias se han centrado en la

promoción de la autonomía tecnológica, la regulación del ciberespacio y el desarrollo de capacidades en áreas estratégicas.

Una de las iniciativas clave en este sentido es "Made in China 2025". Esta estrategia, lanzada en 2015, tiene como objetivo impulsar la transformación en un líder mundial en tecnología avanzada y manufactura de alto nivel. Busca mejorar la competitividad de las empresas chinas en sectores como la robótica, la inteligencia artificial, los vehículos eléctricos y la biotecnología. Esta iniciativa refleja la visión de avanzar hacia una economía impulsada por la innovación y la tecnología.

Por otro lado, "Internet Plus" es una estrategia que busca integrar las tecnologías de la información y la comunicación en todos los sectores de la economía china. Esta iniciativa pretende estimular la innovación, mejorar la eficiencia económica y fomentar la transformación digital de la sociedad. A través de "Internet Plus", busca aprovechar el potencial de las tecnologías digitales para impulsar el crecimiento económico y mejorar la calidad de vida de sus ciudadanos.

La relación entre el crecimiento económico y tecnológico y sus estrategias de soberanía digital puede analizarse a través del prisma de teorías clásicas de las relaciones internacionales. Thomas Hobbes, en su obra "Leviatán" (1651), plantea la importancia de la autoridad soberana para mantener el orden y la estabilidad en el ámbito político. En este contexto la soberanía digital representa la capacidad del Estado para ejercer control y salvaguardar la integridad de la información en el ciberespacio, lo que contribuye a la estabilidad y seguridad del país.

Autores como Hans Morgenthau (1948) y su enfoque realista de las relaciones internacionales pueden ofrecer perspectivas relevantes. El realismo destaca la importancia del poder y la competencia entre los actores estatales. En el caso seleccionado, su enfoque en el desarrollo tecnológico y la protección de su soberanía digital refleja la búsqueda de poder y la competencia por la influencia en el escenario global.

Además, se puede relacionar el enfoque de Antonio Gramsci (1929-1935) sobre la hegemonía con la posición de China como potencia mundial. Gramsci sostiene que el poder y la influencia se logran no solo a través de la fuerza, sino también mediante la construcción de consenso y liderazgo moral. Este país ha buscado consolidar su posición como líder en tecnología y desarrollo económico, lo que le permite influir en la definición de estándares y

regulaciones internacionales en el ámbito digital, y así ejercer una forma de hegemonía tecnológica.

El crecimiento económico y tecnológico de China ha influido en su enfoque de la soberanía del ciberespacio. Como potencia mundial emergente, Este reconoce la importancia de proteger su autonomía tecnológica y salvaguardar la integridad de la información en el ámbito digital. Para lograrlo, ha implementado estrategias de soberanía digital que le permiten ejercer control sobre sus sistemas de información y asegurar la protección de sus intereses nacionales.

En el caso de China, su crecimiento económico y tecnológico le ha permitido fortalecer su infraestructura digital y desarrollar capacidades en áreas como inteligencia artificial, ciberseguridad y tecnologías de la información. Estas capacidades son fundamentales para salvaguardar la autonomía tecnológica y proteger la integridad de la información en el ciberespacio.

El país analizado ha adoptado una postura firme en la protección de su soberanía en el ciberespacio a través de la implementación de regulaciones y políticas que controlan el flujo de información. Esto se manifiesta en medidas como la censura de contenido considerado perjudicial para la estabilidad del país. Si bien estas medidas han sido objeto de críticas por su impacto en la libertad de expresión, desde la perspectiva china son necesarias para garantizar la estabilidad interna y salvaguardar su soberanía en el ciberespacio.

En relación con la lucha por la hegemonía con Estados Unidos, el crecimiento económico y tecnológico de China ha generado tensiones y competencia entre ambos países. El gigante asiático ha desafiado la dominancia tecnológica de Estados Unidos, especialmente en áreas como la inteligencia artificial y las telecomunicaciones. Esta rivalidad se manifiesta en disputas comerciales, restricciones a la inversión y tensiones en materia de ciberseguridad.

La rivalidad tecnológica entre China y Estados Unidos se manifiesta en una serie de disputas comerciales y tensiones en materia de ciberseguridad. Ambos países han impuesto aranceles y restricciones comerciales como parte de una estrategia para proteger sus intereses económicos y tecnológicos. Además, se han acusado mutuamente de ciberespionaje y ataques cibernéticos, lo que ha generado repercusiones sobre la seguridad y la soberanía en el ciberespacio.

Manejando este contexto autores como Graham Allison (2017) y Robert Gilpin (1981) han argumentado sobre la posibilidad de un conflicto entre una potencia ascendente y una potencia establecida, señalando similitudes con la rivalidad histórica entre Atenas y Esparta en la antigua Grecia. Estos académicos plantean que las tensiones económicas y tecnológicas entre China y Estados Unidos podrían desembocar en un conflicto de mayor envergadura, y sugieren la necesidad de un manejo prudente de la rivalidad para evitar una confrontación directa.

Se puede identificar como en el ámbito de políticas económicas, políticas tecnológicas y políticas de Estado que se resumen en potenciar las capacidades damos cuenta que ambos países están involucrados en una intensa rivalidad en el ámbito digital, con sus respectivas estrategias y enfoques.

También podemos decir que el factor ciberseguridad se ha convertido en una preocupación fundamental para ambos países debido a la creciente dependencia de las tecnologías de la información y la comunicación. El país asiático ha adoptado un enfoque que prioriza la soberanía y la seguridad cibernética. Su enfoque se basa en el concepto de "soberanía cibernética", que busca controlar y regular el flujo de información en el ciberespacio dentro de sus fronteras. Esta perspectiva se fundamenta en la visión de que el ciberespacio debe ser regulado de acuerdo con las leyes y regulaciones nacionales para garantizar la estabilidad y la seguridad del país.

Estados Unidos, por otro lado, ha adoptado un enfoque más orientado hacia la libre circulación de información y la protección de la privacidad. Su enfoque se basa en la idea de la "libertad en línea" y la defensa de los derechos humanos en el ciberespacio. Estados Unidos ha defendido la importancia de la libertad de expresión y el acceso abierto a internet, y ha abogado por la cooperación internacional en la lucha contra las amenazas cibernéticas.

1.2 : El trabajo de China para constituir su liderazgo en materia tecnológica.

El posicionamiento del país como un fuerte actor internacional a través de sus estrategias tecnológicas en el ciberespacio tiene implicaciones significativas para las relaciones internacionales y el equilibrio de poder mundial. China ha logrado fortalecer su influencia y protagonismo global, lo cual ha generado tanto interés como preocupación por parte de otros actores internacionales. La creciente presencia en el ámbito tecnológico y su enfoque en la protección de la soberanía digital plantean desafíos en términos de seguridad cibernética, privacidad de datos y la competitividad entre las naciones.

Las relaciones internacionales clásicas y sus teorías continúan teniendo relevancia en el contexto anterior y sobre todo actual, especialmente cuando se analiza el posicionamiento de China como una potencia mundial. Al examinar estas teorías a la luz de la historia china y su proyección en el escenario internacional, podemos obtener una comprensión más profunda de los desafíos y oportunidades que enfrenta en su búsqueda de influencia global.

El análisis de China como actor internacional en el ámbito tecnológico no solo tiene implicaciones para las relaciones internacionales, sino también para el equilibrio de poder mundial. La creciente influencia en el ciberespacio y su enfoque en la protección de la soberanía digital plantean desafíos y oportunidades en términos de seguridad cibernética, privacidad de datos y la configuración de normas y valores en el ámbito digital.

En el mundo actual, la soberanía digital ha adquirido una relevancia significativa. Se refiere al derecho y la capacidad de un Estado para ejercer control y autoridad sobre el ciberespacio dentro de sus fronteras, asegurando así su seguridad y protección en el ámbito digital. Ha reconocido la importancia de la soberanía digital y ha implementado diversas medidas para protegerla.

La historia de China como una antigua civilización y su tradición de centrarse en su propia estabilidad y prosperidad han influido en su enfoque en las relaciones internacionales. Durante siglos, ha adoptado una política de no interferencia en los asuntos internos de otros Estados, conocida como el principio de no injerencia. Esta política se alinea con las ideas realistas, ya que busca preservar su autonomía y proteger su soberanía sin imponer su voluntad a otros países.

En el contexto del país asiático, su posicionamiento como una potencia global se basa en la protección de su soberanía y en la búsqueda de sus intereses nacionales en el ámbito internacional. Este país ha buscado consolidar su poderío económico, político y militar para salvaguardar su integridad territorial y proteger sus intereses nacionales. Esto implica adoptar una postura activa en la promoción de sus intereses y en la defensa de su soberanía tanto en su propia región como a nivel global.

Thomas Hobbes, reconocido filósofo político del siglo XVII, en su obra "Leviatán" (1651), plantea la importancia de la soberanía del Estado en el mantenimiento del orden interno y la protección contra amenazas externas. Si bien El autor no abordó directamente el tema del ciberespacio, sus conceptos sobre la soberanía y el poder estatal pueden aplicarse a la era digital y al papel de China en este contexto.

La protección de su soberanía digital es una prioridad para salvaguardar su estabilidad interna y protegerse de influencias externas indeseadas. En este sentido, el enfoque de China en la protección de su soberanía digital se alinea con las ideas de Hobbes (1651) sobre el papel fundamental del Estado en garantizar la seguridad y el orden. Se considera que la protección de su soberanía digital es esencial para salvaguardar su estabilidad interna y proteger sus intereses nacionales en el ciberespacio. A través de medidas como el "Gran Cortafuegos" y las políticas de ciberseguridad, ejerce su autoridad y control en el ámbito digital, garantizando su capacidad para tomar decisiones y proteger sus intereses.

En el ámbito de las relaciones internacionales, la potencia ha buscado construir alianzas estratégicas en el ciberespacio para fortalecer su posición como actor internacional. Ha establecido acuerdos de cooperación tecnológica con otros países, especialmente en áreas como las telecomunicaciones y la inteligencia artificial. Estas alianzas no solo le brindan acceso a tecnologías y conocimientos avanzados, sino que también le permiten influir en la gobernanza global del ciberespacio y participar en la configuración de las normas y estándares internacionales.

Dentro del marco teórico de las relaciones internacionales, Carl von Clausewitz, en su obra "De la guerra" (1832), destaca la importancia de la tecnología en la competencia internacional y el poderío de las naciones. En este sentido, el ciberespacio se ha convertido en una arena estratégica para la proyección internacional y el ejercicio del poder por parte de los Estados. En el caso analizado, su enfoque en el ciberespacio y sus estrategias tecnológicas tienen una conexión directa con los conceptos clausewitzianos.

La promoción de la cultura china a través del ciberespacio ha sido una herramienta efectiva para influir en la percepción global y proyectar una imagen positiva del país. China ha utilizado plataformas digitales, como las redes sociales y los sitios web, para difundir su idioma, su arte, su música y sus tradiciones culturales. Esto no solo ha contribuido a fortalecer su identidad nacional, sino que también ha generado una base de apoyo y simpatía en la comunidad internacional.

Además, ha utilizado el ciberespacio como una plataforma para promover su modelo de gobernanza digital, basado en la soberanía estatal y el control de la información. A través de políticas y regulaciones, como el control del flujo de información y la protección de datos, China ha buscado establecer un marco normativo que se ajuste a sus intereses y valores. Esta postura ha generado controversias y debates sobre la libertad en Internet y la privacidad de datos, especialmente en el contexto de las relaciones con países occidentales que defienden principios diferentes.

Para China, la ciberseguridad se ha convertido en una prioridad estratégica para proteger su soberanía digital y salvaguardar sus intereses nacionales. A través de políticas y regulaciones, como el control del flujo de información y la protección de datos, busca garantizar su capacidad tecnológica y mantener el control sobre su ciberespacio.

El gigante asiático ha empleado la diplomacia de "ganar-ganar" como una estrategia clave en sus relaciones internacionales. Esta noción, que enfatiza la cooperación mutuamente beneficiosa, encuentra conexiones con teorías clásicas como el liberalismo y el constructivismo.

Los descubrimientos en el ámbito de la inteligencia artificial (IA), han demostrado un rápido avance y una creciente capacidad de innovación. Ha invertido de manera significativa en el desarrollo de la IA y ha establecido un ambicioso plan para convertirse en líder mundial en esta tecnología para el año 2030. Esta expansión en el ámbito de la IA ha generado tensiones en Estados Unidos, que ve amenazada su posición dominante en este sector estratégico.

Por otro lado, en el área de las telecomunicaciones, China ha avanzado rápidamente en la implementación de tecnología 5G. Sin embargo, Estados Unidos ha expresado preocupaciones sobre posibles riesgos para la seguridad cibernética y la privacidad de los datos debido a la presencia de empresas asiáticas en la infraestructura de telecomunicaciones global. Esta situación ha llevado a una creciente rivalidad en el campo de las

telecomunicaciones y ha impulsado a Estados Unidos a tomar medidas restrictivas contra ciertas empresas chinas.

Deberemos resaltar un aspecto no menor en lo que respecta a la “deepweb”, que se refiere a la parte no indexada y no accesible públicamente de internet, ambos países han mostrado preocupaciones en cuanto a la actividad delictiva y la proliferación de contenido ilegal en esta parte del ciberespacio. Tanto China como Estados Unidos han implementado medidas para combatir la actividad ilegal en la “deep web”, incluyendo la cooperación internacional en el intercambio de información y la persecución de delitos cibernéticos.

Ambos países buscan establecer su liderazgo en la economía digital y la tecnología del futuro, lo que ha llevado a la implementación de políticas proteccionistas y estrategias para salvaguardar sus intereses nacionales que a su vez ambos países también están comprometidos en la lucha contra la actividad delictiva en la “Deep web”. La lucha por la hegemonía económica y tecnológica entre China y Estados Unidos es un tema crucial en las relaciones internacionales contemporáneas y tendrá un impacto significativo en el orden mundial.

Puntualmente, la rivalidad tecnológica entre China y Estados Unidos se manifiesta en una serie de disputas comerciales y tensiones en materia de ciberseguridad. Ambos países han impuesto aranceles y restricciones comerciales como parte de una estrategia para proteger sus intereses económicos y tecnológicos. Además, se han acusado mutuamente de ciberespionaje y ataques cibernéticos, lo que ha generado repercusiones sobre la seguridad y la soberanía en el ciberespacio.

La historia de China como una antigua potencia mundial y su búsqueda de influencia y estatus en el sistema internacional también se reflejan en las teorías clásicas de equilibrio de poder. El concepto de equilibrio de poder implica que los Estados buscan formar alianzas y contrapesos para prevenir la dominación absoluta de una sola potencia. Su creciente influencia y protagonismo han generado reacciones de otros actores internacionales, lo que ha llevado a la formación de coaliciones y la reconfiguración de alianzas estratégicas.

La rivalidad tecnológica entre China y Estados Unidos ha dado lugar a una serie de disputas comerciales y tensiones en ciberseguridad. A medida que ambos países compiten por el dominio en el ámbito tecnológico, han impuesto aranceles y restricciones comerciales para salvaguardar sus intereses económicos y tecnológicos. Esta contienda también se ha extendido al ciberespacio, donde han surgido acusaciones mutuas de ciberespionaje y

ataques cibernéticos. Estas tensiones han suscitado preocupaciones sobre la seguridad y la soberanía en el mundo digital. La historia de China como potencia histórica y su ambición por obtener estatus en el escenario internacional también se relacionan con las teorías clásicas de equilibrio de poder. El afán de equilibrar la influencia en el sistema internacional ha llevado a China a forjar alianzas y coaliciones para contrarrestar la dominación de otras potencias, configurando así un entorno geopolítico dinámico y complejo.

1.3: El gran salto tecnológico de HUAWEI

Huawei, fundada en Shenzhen, China, en 1987 por Ren Zhengfei, un exingeniero del Ejército Popular de Liberación de China, se ha convertido en una destacada empresa de telecomunicaciones a nivel mundial (Huawei Corporate Information). A lo largo de los años, Huawei ha experimentado un crecimiento significativo y una expansión internacional. Durante la década de 1990, la empresa estableció operaciones en varios países, centrando su enfoque en ofrecer equipos de redes y soluciones de telecomunicaciones a operadores de todo el mundo (Taylor & Qiao, 2008).

Un aspecto destacado de Huawei es su compromiso con la inversión en investigación y desarrollo. La empresa ha realizado inversiones considerables en este ámbito, lo que le ha permitido desarrollar tecnologías propias y competir en el mercado global de telecomunicaciones (Huawei, 2020). Sin embargo, Huawei también ha enfrentado una serie de controversias y preocupaciones de seguridad. Varios países, incluido Estados Unidos, han expresado inquietudes sobre la posible participación de Huawei en actividades de espionaje cibernético debido a sus vínculos con el gobierno chino (Shirk, 2019).

Estas preocupaciones llevaron al gobierno de Estados Unidos a imponer restricciones comerciales significativas a Huawei. En 2019, la empresa fue incluida en una lista negra comercial, lo que limitó su capacidad para hacer negocios con empresas estadounidenses y generó tensiones en la relación entre China y Estados Unidos (Parmar, 2019).

La historia de Huawei muestra su evolución desde una empresa local hasta convertirse en un importante actor global en el campo de las telecomunicaciones. Aunque ha experimentado un crecimiento notable, también ha enfrentado desafíos relacionados con la seguridad y las restricciones comerciales impuestas por Estados Unidos.

En cuanto a la facturación, en 2019 informó una facturación de aproximadamente 120 mil millones de dólares (Huawei Technologies Co., Ltd., 2020). Sin embargo, es importante tener en cuenta que estos números pueden variar anualmente debido a diversos factores económicos y comerciales.

En términos de producción se destaca por su amplia gama de productos tecnológicos. La empresa se dedica a la fabricación de equipos de red, dispositivos móviles, soluciones empresariales, dispositivos de Internet de las cosas (IoT) y más. Han invertido significativamente en investigación y desarrollo para impulsar la innovación y mejorar sus productos.

En cuanto a capacidad de producción tiene una presencia global con instalaciones de fabricación en diferentes partes del mundo. Sus principales instalaciones se encuentran en China, donde la empresa tiene una fuerte presencia. Además, Huawei ha establecido fábricas y centros de investigación en otros países, como Francia, Alemania y Rusia, para fortalecer su presencia global y satisfacer las demandas regionales (Huawei Technologies Co., Ltd., 2020).

La empresa ha evolucionado en el desarrollo y fabricación de una amplia gama de productos tecnológicos a lo largo de los años. Si nos centramos en su búsqueda por alcanzar el 5G, la empresa ha desempeñado un papel destacado en el desarrollo de tecnologías y equipos relacionados con esta nueva generación de redes móviles.

En cuanto a los productos tecnológicos han lanzado una serie de dispositivos móviles avanzados, como smartphones y tablets, que incorporan tecnología 5G. Estos dispositivos ofrecen velocidades de conexión más rápidas y mayor capacidad de transmisión de datos, lo que permite a los usuarios disfrutar de una experiencia móvil más fluida y enriquecedora (Huawei Consumer Business Group, 2020).

Además de los dispositivos móviles ha desarrollado equipos de infraestructura de red para el despliegue del 5G. Esto incluye estaciones base, antenas y otros componentes necesarios para construir y operar redes 5G de alta velocidad y capacidad. Huawei ha sido reconocido por su experiencia en esta área y ha trabajado en estrecha colaboración con operadores de telecomunicaciones de todo el mundo para implementar el 5G en diferentes regiones (Huawei Technologies Co., Ltd., 2021).

La empresa ha fomentado el desarrollo para impulsar la innovación en tecnologías clave relacionadas con el 5G. Esto incluye el desarrollo de soluciones de virtualización de red, inteligencia artificial, internet de las cosas y computación en la nube, que son componentes fundamentales para la implementación y el funcionamiento eficiente de las redes 5G (Huawei Technologies Co., Ltd., 2021).

Es importante destacar que Huawei se ha convertido en uno de los principales actores en la carrera por el despliegue del 5G a nivel mundial. Sin embargo, debido a las preocupaciones de seguridad y las restricciones comerciales impuestas por Estados Unidos y otros países, la empresa ha enfrentado desafíos en su expansión internacional y ha tenido que buscar alternativas y socios en diferentes mercados para seguir avanzando en el desarrollo y la implementación del 5G (Ding, 2019).

También es importante destacar la expansión internacional bajo la política de "Going Global" que ha jugado un papel importante en la expansión de la influencia tecnológica de China a nivel global, llevando sus productos y servicios a diversos países. Esta expansión ha sido parte de la estrategia de China para aumentar su presencia en el escenario internacional y proteger sus intereses en el ciberespacio a nivel mundial.

Como es de esperarse, la empresa se encuentra alineada con la ley de seguridad en su búsqueda por el desarrollo del 5G y en la protección de la soberanía digital y el ciberespacio. La empresa ha estado comprometida con el cumplimiento de las regulaciones y políticas de seguridad establecidas por el gobierno chino.

En relación con esto, Huawei ha señalado en varias ocasiones su adhesión a la ley de seguridad cibernética de y su compromiso con la protección de la seguridad de la información y la ciberseguridad (Huawei Technologies Co., Ltd., 2020). La empresa reconoce la importancia de garantizar la integridad y confidencialidad de los datos, así como la protección contra amenazas cibernéticas.

Además, han invertido significativamente en la mejora de su capacidad de seguridad y ha implementado medidas para proteger la integridad de sus productos y soluciones. La empresa ha establecido un sistema de gestión de seguridad integral y ha llevado a cabo auditorías y evaluaciones internas y externas para garantizar el cumplimiento de los estándares de seguridad (Huawei Technologies Co., Ltd., 2020).

En cuanto a la protección de la soberanía digital y el ciberespacio, han subrayado la importancia de construir una infraestructura de telecomunicaciones segura y confiable. La empresa ha trabajado en estrecha colaboración con los reguladores y operadores de telecomunicaciones en diferentes países para garantizar la seguridad y la confiabilidad de sus soluciones de red (Huawei Technologies Co., Ltd., 2020).

Esta empresa ha sido un actor clave en el establecimiento de cimientos soberanos para China en el ámbito de las tecnologías de la información y la comunicación. Como se menciona a través de sus avances tecnológicos y su crecimiento como empresa líder en telecomunicaciones, Huawei ha contribuido a varios aspectos de la soberanía digital de China.

Huawei, a lo largo de su historia, se ha convertido en una potencia tecnológica en el estado chino, logrando un crecimiento notable en el mercado global de telecomunicaciones. Este camino hacia el éxito se ha debido a una combinación de factores estratégicos y apoyo del gobierno chino. Según Sun Yafang, Presidenta de Huawei, "El apoyo del gobierno y la política industrial de China fueron críticos para el rápido desarrollo de Huawei" (Huawei Technologies Co., Ltd., 2015).

Sin embargo, este crecimiento ha generado conflictos con Apple, Google y Estados Unidos. Uno de los principales puntos de conflicto radica en la competencia en el mercado de smartphones. Huawei ha desafiado la posición de Apple y otras empresas tecnológicas en el sector de dispositivos móviles, logrando un crecimiento significativo en las ventas globales. Esto ha llevado a tensiones comerciales y rivalidad en la industria, generando entre estas dos potencias una acérrima rivalidad tecnológica, donde ambas potencias buscan posicionarse en la vanguardia de los avances tecnológicos a nivel global.

Además, Huawei ha enfrentado obstáculos con respecto a su relación con Google y el acceso a los servicios de Google en sus dispositivos. En 2019, debido a las restricciones impuestas por el gobierno de Estados Unidos, Huawei se vio afectada por la prohibición de acceder a las aplicaciones y servicios de Google en sus nuevos dispositivos. Esto ha generado una ruptura en la colaboración y ha llevado a Huawei a buscar alternativas y desarrollar su propio ecosistema de aplicaciones y servicios.

Estos conflictos y tensiones son resultado de diversos factores, incluyendo consideraciones económicas, competencia tecnológica, seguridad nacional y la rivalidad entre China y Estados Unidos en el ámbito geopolítico. La posición dominante de Huawei en el mercado

global de telecomunicaciones y su crecimiento continuo han llevado a una mayor atención y escrutinio por parte de otros actores internacionales.

Es importante destacar que Huawei ha enfrentado críticas y preocupaciones por parte de algunos países, principalmente Estados Unidos, en relación con la seguridad y la presunta influencia del gobierno chino en sus operaciones. Sin embargo, Huawei ha rechazado estas acusaciones y ha afirmado que es una empresa privada y que su enfoque principal es proporcionar tecnología segura y confiable a sus clientes (Huawei Technologies Co., Ltd., 2020).

En 2018, el gobierno de Estados Unidos incluyó a Huawei en una lista negra comercial, lo que impuso restricciones significativas a las relaciones comerciales de la empresa con empresas estadounidenses. Estas restricciones incluyeron la prohibición de que Google proporcionara licencias de software de Android a Huawei para sus nuevos dispositivos.

Según Zhang Pingan, Presidente del Departamento de Gestión de Riesgos de Huawei, "La inclusión de Huawei en la Lista de Entidades del gobierno de Estados Unidos ha tenido un impacto significativo en nuestra cooperación con socios estadounidenses, incluyendo Google" (Huawei Technologies Co., Ltd., 2019).

Debido a las restricciones mencionadas la Empresa perdió el acceso a los servicios y aplicaciones de Google en sus nuevos dispositivos, lo que incluye la falta de acceso a Google Play Store y a las actualizaciones de software de Android.

Como menciona Ren Zhengfei, Fundador de Huawei, "Nuestros teléfonos no pueden acceder a Google Mobile Services (GMS) debido a la prohibición impuesta por el gobierno de Estados Unidos. Esto ha supuesto un desafío para nosotros en el mercado internacional" (Huawei Technologies Co., Ltd., 2020).

A pesar de las restricciones impuestas por el gobierno de Estados Unidos y la pérdida de acceso a los servicios de Google, Huawei pudo encontrar algunas oportunidades y beneficios en esta situación desafiante.

La prohibición de acceder a los servicios y aplicaciones de Google motivó a Huawei a acelerar el desarrollo de su propio ecosistema de aplicaciones y servicios, conocido como Huawei Mobile Services (HMS). Esta iniciativa permitió a Huawei ofrecer una alternativa a los servicios de Google, brindando a los usuarios una experiencia similar en términos de aplicaciones y funcionalidades.

Según Ryan Ding, Presidente de Huawei Carrier Business Group, "Estamos construyendo nuestro propio ecosistema para brindar a nuestros usuarios una experiencia de usuario más integrada y completa, ofreciendo servicios y aplicaciones a través de Huawei Mobile Services" (Huawei Technologies Co., Ltd., 2019).

Las restricciones también llevaron a Huawei a centrarse aún más en el mercado interno chino, que es uno de los mercados de telefonía móvil más grandes y de rápido crecimiento en el mundo. Huawei pudo aprovechar su fuerte presencia y reputación en China para mantener su posición de liderazgo en el mercado nacional.

Como menciona Eric Xu, Presidente Rotativo de Huawei, "La prohibición de Estados Unidos no ha afectado significativamente nuestro negocio en China. Hemos mantenido un crecimiento constante en el mercado chino y estamos enfocados en ofrecer productos y servicios de calidad a nuestros clientes locales" (Huawei Technologies Co., Ltd., 2020).

Estos beneficios permitieron a Huawei enfrentar los desafíos planteados por las restricciones y seguir siendo competitivo en el mercado de dispositivos móviles.

La rivalidad tecnológica entre China y Estados Unidos no solo ha tenido implicaciones bilaterales, sino que también ha afectado el orden mundial y la cooperación internacional en temas tecnológicos. La competencia por el liderazgo tecnológico ha llevado a una polarización en el escenario global, con la formación de bloques y alianzas en torno a diferentes tecnologías y estándares.

La relación entre China y Estados Unidos en materia tecnológica ha sido compleja y dinámica, marcada por una fuerte competencia por el liderazgo en la industria y la protección de intereses nacionales. Esta competencia ha tenido importantes implicaciones para el orden mundial y ha llevado a tensiones comerciales y políticas entre ambas potencias.

La prohibición impuesta por el gobierno de Estados Unidos a Huawei y la cancelación de relaciones comerciales con Google se han fundamentado en preocupaciones relacionadas con la seguridad nacional y el espionaje cibernético. Estados Unidos sostiene que existe el riesgo de que Huawei, como empresa china, esté sujeta a la influencia y el control del gobierno chino. Esto plantea preocupaciones sobre la seguridad de las redes y los datos en Estados Unidos y en otros países que utilizan tecnología Huawei.

El argumento central es que Huawei podría ser utilizado como un medio para llevar a cabo actividades de espionaje o ciberataques en nombre del gobierno chino. Dado que Huawei es

uno de los principales proveedores de equipos de telecomunicaciones y servicios de redes a nivel mundial, su participación en infraestructuras críticas podría ser un punto de vulnerabilidad para la seguridad nacional.

En el informe del Comité Selecto de Inteligencia del Senado de Estados Unidos, se señala que "Las leyes chinas, como la Ley de Inteligencia Nacional de 2017, obligan a las organizaciones y ciudadanos chinos a apoyar, ayudar y cooperar en los esfuerzos de inteligencia del Estado. Por lo tanto, la preocupación radica en que Huawei, como empresa asiática, pueda verse obligada a facilitar el espionaje del gobierno chino" (United States Senate, 2018).

Es importante destacar que las preocupaciones sobre la seguridad nacional y el espionaje cibernético no se limitan exclusivamente a Huawei, sino que también se han dirigido a otras empresas chinas de tecnología. Sin embargo, debido a la prominencia de Huawei en el mercado global de telecomunicaciones, ha sido el centro de atención en esta disputa entre Estados Unidos y China.

La nación asiática en cuestión percibe las acciones tomadas por Estados Unidos como parte de una estrategia destinada a contener su ascenso como potencia tecnológica y proteger los intereses comerciales de las empresas estadounidenses. En particular, Huawei se ve afectada por estas medidas debido a su posición destacada en el sector de las comunicaciones y su estatus como símbolo del avance tecnológico de La potencia oriental.

Desde la perspectiva china, la prohibición de Estados Unidos y la cancelación de relaciones comerciales con Huawei son percibidas como medidas proteccionistas para frenar el crecimiento y el dominio de las empresas chinas en el mercado global de tecnología. Se argumenta que estas acciones se basan en motivaciones políticas y económicas más que en preocupaciones legítimas de seguridad.

Esta percepción se alinea con la teoría de la maximización de poder propuesta por Mearsheimer (2001). Según Mearsheimer, los Estados buscan aumentar su poder relativo en el sistema internacional para garantizar su seguridad y supervivencia. En este caso, China podría interpretar las acciones de Estados Unidos como un intento de contener su ascenso y reducir su influencia en el ámbito tecnológico, lo que podría amenazar sus intereses a largo plazo.

Además, la cancelación de relaciones comerciales con Huawei también podría ser vista desde la perspectiva china como una señal de amenaza percibida. En línea con la teoría de la percepción de amenaza de Mearsheimer (2001), las acciones de Estados Unidos podrían ser interpretadas por China como un intento de debilitar su capacidad tecnológica y, por lo tanto, su seguridad y autonomía en el ciberespacio. Esta percepción de amenaza podría llevar a una respuesta defensiva por parte de China, como fortalecer aún más sus capacidades tecnológicas y buscar alianzas con otros actores que compartan sus intereses en contraposición a la presión ejercida por Estados Unidos.

El país del Lejano Oriente ha defendido firmemente a Huawei, considerándola una empresa líder y un importante actor en la innovación tecnológica. En respuesta a las acusaciones de espionaje y las restricciones comerciales, el gobierno chino ha expresado su descontento y ha instado a Estados Unidos a tratar a las empresas chinas de manera justa y no discriminatoria.

En un comunicado oficial, el portavoz del Ministerio de Relaciones Exteriores de China afirmó: "La campaña de Estados Unidos contra las compañías chinas, incluida Huawei, es una supresión deliberada y sistemática, con el objetivo de frenar el desarrollo de las empresas chinas avanzadas y proteger los intereses de las empresas estadounidenses" (Ministerio de Relaciones Exteriores de China, 2019).

En palabras de Yu Chengdong, CEO de la unidad de consumo de Huawei, "La razón subyacente de la prohibición de Estados Unidos a Huawei no se basa en la seguridad, sino en la competencia económica" (Mozur et al., 2019).

El gobierno chino expresó su apoyo a Huawei y promovió medidas para fortalecer la industria tecnológica nacional y reducir la dependencia de tecnologías extranjeras. En respuesta a las restricciones, implementó políticas y estrategias para impulsar la innovación y el desarrollo de tecnologías clave en áreas como semiconductores, inteligencia artificial y telecomunicaciones.

También se han tomado medidas para promover el uso de productos y servicios de Huawei dentro del país. Por ejemplo, en 2019, se informó que el Ministerio de Industria y Tecnología de la Información estaba alentando a las empresas estatales a comprar más dispositivos y equipos de Huawei, con el objetivo de respaldar la industria nacional y reducir la dependencia de tecnologías extranjeras.

Estos sucesos reflejan una creciente rivalidad entre Estados Unidos y China en el ámbito tecnológico, donde la lucha por la hegemonía y la protección de los intereses nacionales se entrelazan. Además, la cancelación de relaciones entre Google y Huawei ha tenido un impacto significativo en la industria tecnológica y ha generado tensiones en el escenario internacional.

La posición actual de Huawei en el ámbito tecnológico es relevante, aunque ha enfrentado desafíos debido a las restricciones impuestas por Estados Unidos y la exclusión de algunos mercados. A pesar de esto, Huawei sigue siendo uno de los principales fabricantes de equipos de telecomunicaciones y dispositivos móviles a nivel mundial.

En términos de tecnología ha continuado desarrollando y lanzando productos innovadores. La compañía ha hecho hincapié en el desarrollo de redes 5G, siendo uno de los principales proveedores de equipos para esta tecnología a nivel global. Además, Huawei ha invertido en investigación y desarrollo en áreas como inteligencia artificial, nube y computación de borde, enfocándose en impulsar la transformación digital en diversos sectores.

No obstante, las restricciones impuestas por Estados Unidos han afectado la participación de Huawei en ciertos mercados internacionales. Algunos países han restringido o excluido a Huawei de sus redes de telecomunicaciones 5G debido a preocupaciones de seguridad y presiones políticas. Aunque Huawei ha negado repetidamente las acusaciones de espionaje y ha implementado medidas para mejorar la seguridad de sus productos, las preocupaciones persisten en algunos países.

En cuanto a la posición política la empresa ha sido objeto de un mayor escrutinio y se ha visto envuelta en tensiones geopolíticas entre China y Estados Unidos. Estados Unidos la ha considerado como una amenaza para la seguridad nacional y ha presionado a otros países para que limiten su participación en proyectos de infraestructura de telecomunicaciones.

Por otro lado, el gobierno chino ha apoyado y respaldado a Huawei, promoviendo su desarrollo y posición en el mercado: "Debemos acelerar la promoción del poder discursivo internacional de China y el poder de hacer las reglas en el ciberespacio y hacer esfuerzos infatigables para alcanzar el objetivo de construir una gran potencia cibernética" (Xi Jinping, 2016, foro CPC 36°). El gigante asiático considera a la empresa como un símbolo del progreso tecnológico y la capacidad de innovación del país. Además, el gobierno chino ha tomado medidas para proteger los intereses de esta y otras empresas tecnológicas chinas, promoviendo políticas de desarrollo nacional y buscando la autosuficiencia tecnológica.

Es importante destacar que la posición actual de Huawei es compleja y está influenciada tanto por consideraciones tecnológicas como políticas. La empresa continúa trabajando para superar los desafíos y diversificar sus operaciones en diferentes sectores, al tiempo que busca fortalecer la confianza y la seguridad en sus productos y servicios.

Huawei busca superar los desafíos actuales diversificando sus operaciones y fortaleciendo la confianza en sus productos y servicios. La empresa se enfoca en desarrollar su negocio empresarial y expandir su presencia en diferentes sectores.

Capítulo 2 - Hacia una ciber-soberanía.

En la última década, la revolución digital ha transformado radicalmente la manera en que las naciones interactúan comercialmente y se relacionan en el escenario global. En este contexto de creciente interconexión, la ciberseguridad y la protección de la soberanía digital han emergido como desafíos centrales para la seguridad nacional y la política internacional. Uno de los actores principales en esta dinámica es China, que entre los años 2014 y 2019 desplegó una serie de estrategias tecnológicas en busca de lo que podría denominarse una "ciber-soberanía".

El periodo entre 2014 y 2019 evidencia la búsqueda incansable de China por controlar su destino en el ciberespacio. A medida que la nación fortalecía su capacidad tecnológica y promulgaba leyes de ciberseguridad, sentaba las bases para ejercer su influencia en el ámbito digital y proteger su soberanía. Esta evolución no solo plantea preguntas cruciales sobre el equilibrio entre la seguridad y la apertura en el ciberespacio, sino también sobre cómo esta búsqueda de ciber-soberanía afectará las relaciones internacionales y la configuración del poder en el mundo digital.

2.1 : Avance de las TIC'S como capacidad de control en CHINA.

La potencia asiática experimentó un crecimiento económico significativo y se consolidó como una potencia mundial en varios aspectos, incluyendo el ámbito tecnológico y digital. En términos de geopolítica, es fundamental tener en cuenta la relación entre China y Estados Unidos, considerada una de las rivalidades más importantes en el escenario internacional.

Un autor clave para comprender esta relación es Graham Allison, quien en su libro "Destined for War: Can America and China Escape Thucydides's Trap?" explora el concepto de la "trampa de Tucídides". Allison plantea que la rivalidad entre una potencia en ascenso (China) y una potencia dominante (Estados Unidos) puede generar conflictos y tensiones geopolíticas significativas. En el contexto del ciberespacio, esta rivalidad se ha manifestado en disputas sobre el control y la seguridad de la infraestructura tecnológica.

La geopolítica del ciberespacio implica también las relaciones de China con otras potencias mundiales. Por ejemplo, Rusia ha sido un actor relevante en el ámbito digital y ha establecido estrechas relaciones con China en este sentido. Timothy Thomas, en su artículo "Russia-China Cybersecurity Cooperation: Power Politics or Liberalizing Norms?" examina la cooperación en materia de ciberseguridad entre ambos países y destaca su impacto en la geopolítica del ciberespacio.

En relación al crecimiento económico, es necesario tener en cuenta su influencia en la geopolítica y en el ciberespacio. Un autor relevante en este contexto es George Magnus, quien en su libro "Red Flags: Why Xi's China Is in Jeopardy" explora los desafíos y riesgos asociados al modelo de crecimiento económico de este País. Magnus argumenta que el rápido crecimiento ha generado tensiones geopolíticas, especialmente con Estados Unidos, en el ámbito de la tecnología y la ciberseguridad.

Se han desarrollado políticas y estrategias para proteger su soberanía digital y promover su desarrollo tecnológico. Autores como Rogier Creemers, en su artículo "The Creemers of China's Cybersecurity Law", analizan la Ley de Ciberseguridad de China y su impacto en la geopolítica del ciberespacio. Creemers destaca cómo esta legislación busca salvaguardar los intereses nacionales en el ámbito digital y promover su posición como actor clave en la economía digital global.

La geopolítica y el ciberespacio entre los años 2014 y 2019 estuvieron influenciados por su relación con Estados Unidos y otras potencias, así como por su crecimiento económico. Los aportes de autores como Allison, Thomas, Magnus y Creemers nos permiten comprender en profundidad los desafíos, las rivalidades y las políticas que han configurado la dinámica geopolítica y digital de China en ese período.

Las TIC, también conocidas como tecnologías digitales, se refieren al conjunto de herramientas, dispositivos y sistemas que facilitan la adquisición, procesamiento, almacenamiento y transmisión de información. En el contexto geopolítico, las TIC han adquirido una relevancia significativa debido a su capacidad de influir en la economía, la seguridad nacional y la proyección de poder de una nación.

Para comprender cómo las TIC conforman una capacidad en una potencia, podemos recurrir a la teoría del poder de Joseph Nye. Según Nye, el poder puede manifestarse de dos formas: el poder duro, que se refiere a la capacidad militar y económica de un Estado, y el poder blando, que se basa en la atracción y persuasión a través de la cultura, los valores y la

tecnología. En este sentido, las TIC se convierten en una herramienta clave para proyectar el poder blando de una potencia, al permitir la difusión de su cultura, valores y narrativa a nivel global.

El avance de las TIC ha sido importante durante el periodo 2014-2019. En términos de infraestructura de telecomunicaciones, Este ha desarrollado una red de banda ancha de alta velocidad y ha implementado tecnologías como 4G y 5G de manera significativa. Además, ha experimentado un rápido crecimiento en el ámbito de la inteligencia artificial (IA), convirtiéndose en uno de los líderes mundiales en esta área. Autores como Kai-Fu Lee, en su libro "AI Superpowers: China, Silicon Valley, and the New World Order", analizan el avance de la IA y su impacto en la competencia geopolítica con Estados Unidos.

En el paradigma de las TIC, es importante mencionar la estrategia "Made in China 2025", que busca impulsar la innovación y el desarrollo tecnológico en sectores clave como la inteligencia artificial, la robótica y la tecnología de la información. Esta estrategia, junto con la iniciativa "Internet Plus", que promueve la integración de internet y las tecnologías digitales en diversos sectores económicos, ha impulsado el avance de las TIC durante el periodo mencionado.

El avance de las Tecnologías de la Información y Comunicación (TIC) como una capacidad de control ha sido un elemento fundamental en su estrategia geopolítica. China ha reconocido la importancia del ciberespacio y ha implementado políticas y regulaciones específicas para proteger su ciberseguridad y salvaguardar la soberanía digital del país.

Rogier Creemers, en su artículo "Digital Nationalism in China" (2019), proporciona una perspectiva interesante sobre la relación entre la soberanía digital y el nacionalismo en un país asiático que ha experimentado un rápido crecimiento tecnológico y se ha convertido en una potencia mundial en el ámbito de las TIC.

En el contexto de este país, el enfoque de Creemers(2019) destaca cómo la noción de "soberanía digital" está estrechamente vinculada al nacionalismo y a la idea de proteger los intereses y la identidad nacional en el ciberespacio. La soberanía digital se refiere a la capacidad de un Estado para ejercer control sobre los asuntos cibernéticos dentro de su territorio y garantizar la protección de su infraestructura tecnológica y la integridad de la información que circula en línea.

Este país, al igual que otros actores en el escenario internacional, reconoce la importancia de la soberanía digital como una dimensión crítica de su seguridad y capacidad para influir en el ciberespacio. La soberanía digital implica el desarrollo de políticas y regulaciones que permitan al Estado ejercer control sobre la tecnología y los datos, con el objetivo de proteger los intereses nacionales y salvaguardar la integridad del ciberespacio.

La teoría de Creemers(2019) enfatiza cómo en este país el concepto de soberanía digital se ha utilizado como una herramienta para promover el nacionalismo y proteger la identidad cultural y política frente a influencias externas. Las políticas y regulaciones en materia de ciberseguridad y control de la información reflejan el deseo de este país de preservar su autonomía y mantener el control sobre su infraestructura tecnológica y datos, evitando así la dependencia de actores extranjeros.

La relación entre la soberanía digital y el nacionalismo en este país se manifiesta a través de medidas como la regulación de contenido en línea, el control de las redes sociales y el fomento de tecnologías nacionales. Estas acciones se enmarcan en la búsqueda de proteger la identidad y los valores nacionales, así como en fortalecer la capacidad de control del Estado sobre la tecnología y los datos.

La implementación de políticas y regulaciones en el ámbito de la ciberseguridad refleja la preocupación de China por salvaguardar su soberanía digital y proteger sus intereses nacionales en el ciberespacio. Considera que la seguridad en línea es vital para garantizar la estabilidad social y prevenir amenazas internas y externas.

En el orden mundial, el avance de las TIC en este hegemon en ascenso ha generado tensiones y rivalidades con Estados Unidos y otras potencias. La competencia por el dominio en áreas como la ciberseguridad, el desarrollo de tecnologías avanzadas y la protección de la propiedad intelectual ha sido una característica destacada de la relación entre China y Estados Unidos. Autores como Henry Farrell y Abraham L. Newman, en su libro "Of Privacy and Power: The Transatlantic Struggle over Freedom and Security", analizan cómo esta rivalidad ha configurado la gobernanza global de internet y ha planteado desafíos en términos de privacidad, seguridad y acceso a la información.

La salida de Google del país asiático estuvo motivada principalmente por las tensiones relacionadas con la censura y la libertad de expresión, mas un ataque cibernético de gran magnitud nombrado.

"En enero de 2006, lanzamos Google.cn con la convicción de que los beneficios de aumentar el acceso a la información para las personas en China y un internet más abierto superaban nuestra incomodidad al aceptar censurar algunos resultados. En ese momento dejamos claro que "monitorearíamos cuidadosamente las condiciones en China, incluidas las nuevas leyes y otras restricciones a nuestros servicios. Si determinamos que no podemos lograr los objetivos establecidos, no dudaremos en reconsiderar nuestro enfoque hacia China."

Estos ataques y la vigilancia que han revelado, combinados con los intentos durante el último año de limitar aún más la libertad de expresión en la web, nos han llevado a concluir que debemos revisar la viabilidad de nuestras operaciones comerciales en China. Hemos decidido que ya no estamos dispuestos a continuar censurando nuestros resultados en Google.cn, por lo que en las próximas semanas discutiremos con el gobierno chino las bases en las que podríamos operar un motor de búsqueda sin filtrar dentro de la ley, si es que es posible. Reconocemos que esto podría significar tener que cerrar Google.cn y, potencialmente, nuestras oficinas en China."
(Comunicado oficial Google, 2010)

El gobierno chino había impuesto restricciones y filtros en internet, lo que afectaba la capacidad de Google para ofrecer sus servicios de manera libre y abierta en el país. Como resultado, Google tomó la decisión de cesar sus operaciones en China continental y redirigió a los usuarios chinos a su sitio web en Hong Kong, donde la censura era menos estricta.

Este suceso tuvo implicaciones significativas desde una perspectiva geopolítica. Por un lado, representó un desafío para China, ya que la salida de Google dejó un vacío en el mercado de motores de búsqueda y servicios en línea, que en ese momento estaba dominado por la empresa estadounidense. Además, puso de manifiesto las tensiones existentes entre el gobierno chino y las empresas extranjeras en relación con la censura y el control de la información en internet.

Como respuesta también buscó fortalecer su propio ecosistema digital y desarrollar alternativas locales. Se fomentó el surgimiento de motores de búsqueda chinos, como Baidu, que se convirtió en uno de los principales motores de búsqueda en el país. También se promovieron redes sociales y servicios en línea locales, como Weibo y WeChat, que ganaron popularidad entre los usuarios chinos.

Este impulso a la creación de alternativas locales en el ámbito de las TIC tuvo importantes implicaciones geopolíticas. Por un lado, permitió al gobierno chino ejercer un mayor control sobre la información y mantener una mayor supervisión de las actividades en línea de los ciudadanos. Al promover el uso de plataformas y servicios bajo su control, China pudo fortalecer su capacidad para influir en la narrativa y la opinión pública dentro del país.

La salida de Google y el desarrollo de alternativas locales reflejaron el objetivo de este país de lograr una mayor independencia tecnológica y reducir su dependencia de empresas extranjeras en áreas clave como la búsqueda en internet y los servicios en línea. Esta estrategia se alineaba con los esfuerzos de China por fortalecer su soberanía digital y proteger su capacidad tecnológica frente a potenciales amenazas externas.

La geopolítica y el ciberespacio de China entre los años 2014 y 2019 estuvieron marcados por el avance de las TIC y su competencia con Estados Unidos y otras potencias. Las TIC se convirtieron en una capacidad clave para proyectar el poder blando, fortalecer su soberanía digital y promover su desarrollo tecnológico. Los avances en infraestructura de telecomunicaciones, inteligencia artificial y políticas de ciberseguridad reflejan el papel central de las TIC en la geopolítica china. Sin embargo, esta evolución también generó tensiones y rivalidades con otras potencias, especialmente con Estados Unidos, en el ámbito de la gobernanza digital y la competencia tecnológica.

2.2: Ley de ciberseguridad China

La Ley de Ciberseguridad de China, promulgada en el año 2016, ha tenido un impacto significativo en el panorama de la seguridad digital en el país . Antes de la implementación de esta ley, se enfrentaba a numerosos desafíos en materia de ciberseguridad, que iban desde amenazas cibernéticas y delitos informáticos hasta el acceso no autorizado a información confidencial (Creemers, 2019). Estos problemas planteaban riesgos tanto para el gobierno como para las empresas y los ciudadanos chinos.

Anterior a la promulgación de la Ley de Ciberseguridad, el entorno digital era más laxo en términos de regulación y control. Esto generaba preocupaciones en cuanto a la protección de la información sensible y la vulnerabilidad frente a ataques cibernéticos. Además, existían inquietudes sobre la privacidad y la libertad de expresión en línea, en medio de una creciente actividad digital en el país.

Antes de la implementación de esta ley, ya tenía regulaciones y políticas en materia de ciberseguridad, pero la nueva ley amplió y fortaleció su alcance.

Los pilares centrales de dicha ley son:

- Mayor regulación y supervisión: La ley estableció un marco legal más sólido para la regulación y supervisión de la ciberseguridad en China. Se estableció un sistema de revisión de seguridad cibernética, que requería que las compañías de tecnología y los proveedores de servicios en línea pasaran por una evaluación de seguridad antes de operar en el país.
- Protección de datos y privacidad: La ley puso un mayor énfasis en la protección de datos personales y la privacidad en línea. Introdujo disposiciones para el almacenamiento local de datos y estableció requisitos más estrictos para el manejo de información sensible.
- Control gubernamental y acceso a datos: La ley otorgó a las autoridades gubernamentales un mayor control y acceso a los datos y sistemas de información. Esto implicaba la posibilidad de inspeccionar, supervisar y acceder a los sistemas y datos de las empresas en casos de seguridad nacional.
- Responsabilidad de las empresas: La ley exigió que las empresas adoptaran medidas de seguridad cibernética, implementaran sistemas de gestión de riesgos

y reportaran incidentes de seguridad de manera oportuna. También estableció sanciones para las violaciones de seguridad cibernética.

En palabras de Jack Goldsmith y Andrew Keane Woods (2018), expertos en ciberseguridad y derecho internacional, "China enfrentaba un panorama complejo en materia de ciberseguridad, con la necesidad de abordar tanto amenazas internas como externas" (p. 123). La falta de una legislación integral y específica para la ciberseguridad planteaba desafíos para el gobierno chino en la protección de su infraestructura digital y la seguridad de los datos.

No obstante, con la promulgación de la Ley de Ciberseguridad en 2016, dio un paso importante para fortalecer su capacidad de protección y regulación en el ámbito digital. Esta ley estableció un marco legal que abordaba cuestiones clave como la protección de infraestructuras críticas, la gestión de datos y la seguridad de la información como se detalla anteriormente.

Según Deng Zhonghan (2017), experto en derecho y políticas de ciberseguridad, "la Ley de Ciberseguridad de China marcó un hito en el desarrollo de políticas de seguridad digital en el país, brindando un marco legal sólido para abordar los desafíos y riesgos asociados con el ciberespacio" (p. 45). Con esta legislación, China buscó proteger su soberanía digital y salvaguardar la integridad de su infraestructura tecnológica.

En el contexto de las tensiones con Estados Unidos y otros países, la implementación de la Ley de Ciberseguridad ha generado debates y preocupaciones en el ámbito internacional. Algunos críticos argumentan que esta ley puede restringir la libertad de expresión y aumentar el control del gobierno sobre el ciberespacio. Con respecto al plano internacional y la relación con otros actores internacionales dicha ley puede tener puntos de conflicto.

La implementación de dicha Ley ha generado tensiones particularmente por los siguientes aspectos (Creemers, 2017)

- Acceso y control de datos: La disposición de la ley que otorga al gobierno chino un mayor control y acceso a los datos y sistemas de información ha generado preocupaciones sobre la seguridad de los datos empresariales y la protección de la propiedad intelectual. Esto ha llevado a tensiones comerciales y disputas sobre prácticas de transferencia de datos entre China y otros países.

- Proteccionismo digital: Al requerir el almacenamiento local de datos y la revisión de seguridad para las empresas extranjeras que operan en China, la ley puede interpretarse como una forma de proteccionismo digital. Esto ha generado preocupaciones sobre la discriminación y las barreras comerciales para las empresas extranjeras, especialmente en el sector de la tecnología.
- Censura y control de la información: La ley también ha sido criticada por su impacto en la libertad de expresión y el control de la información en línea. Las disposiciones de la ley pueden ser utilizadas para restringir el acceso a contenidos considerados sensibles o críticos para el gobierno chino, lo que limita la libertad de expresión de los ciudadanos chinos y la capacidad de acceder a información independiente.

“El gobierno chino ha reconocido que el ciberespacio impacta inmediata y profundamente en muchos de los aspectos de la seguridad nacional, si no todos (..) Es un espacio nacional, un espacio para la intervención militar, para la acción económica relevante, para las actividades criminales y para el espionaje” (R. Creemers, Universidad de Leiden, en Países Bajos, 2017)

La disposición de la ley que otorga al gobierno chino un mayor control y acceso a los datos y sistemas de información ha generado preocupaciones sobre la seguridad de los datos empresariales y la protección de la propiedad intelectual intentando así incrementar su soberanía digital. Esto ha llevado a tensiones comerciales y disputas sobre prácticas de transferencia de datos entre China y otros países.

Al requerir el almacenamiento local de datos y la revisión de seguridad para las empresas extranjeras que operan sobre territorio asiático, la ley puede interpretarse como una forma de proteccionismo digital. Esto ha generado repercusiones sobre la discriminación y las barreras comerciales para las empresas extranjeras, especialmente en el sector de la tecnología.

La ley también ha sido criticada por su impacto en la libertad de expresión y el control de la información en línea. Las disposiciones de la ley pueden ser utilizadas para restringir el acceso a contenidos considerados sensibles o críticos para el gobierno chino, lo que limita la libertad de expresión de los ciudadanos chinos y la capacidad de acceder a información independiente.

En relación con las tensiones con Estados Unidos específicamente, esta Ley ha sido objeto de discusión debido al acceso a información y la protección de datos empresariales. Estados Unidos ha expresado su preocupación por las medidas de seguridad cibernética de China, argumentando que podrían dificultar el acceso de las empresas estadounidenses al mercado chino y generar barreras comerciales.

No obstante, es importante destacar que el gobierno ha defendido la Ley de Ciberseguridad como una medida necesaria para proteger sus intereses de seguridad nacional y garantizar la estabilidad del ciberespacio. Según Zhang Jian, "China considera que la Ley de Ciberseguridad es un componente crucial de su estrategia para salvaguardar su soberanía digital y proteger sus sistemas de información críticos" (Zhang, 2018).

Además de las tensiones con Estados Unidos, la Ley de Ciberseguridad también ha suscitado preocupaciones en otros países, especialmente en relación con la transferencia de datos y la seguridad de la información. Algunos críticos sostienen que esta legislación puede tener implicaciones para las empresas extranjeras que operan en China y para la libre circulación de datos. Las disposiciones relacionadas con el almacenamiento local de datos y la revisión de seguridad han generado preocupaciones sobre la protección de la propiedad intelectual y la privacidad de las empresas extranjeras. Algunas empresas han tenido que adaptar sus operaciones y prácticas para cumplir con las regulaciones de la ley.

Desde su promulgación el gobierno chino ha llevado a cabo acciones para fortalecer su implementación y asegurar el cumplimiento de las regulaciones por parte de las empresas y ciudadanos chinos. Se han establecido agencias y mecanismos de supervisión para garantizar el cumplimiento de las disposiciones de la ley.

La implementación de la ley ha impulsado el desarrollo de una infraestructura nacional de ciberseguridad en China. Se han establecido centros de ciberseguridad y se ha promovido la investigación y el desarrollo de tecnologías relacionadas con la seguridad cibernética. Esto refleja el compromiso del gobierno chino de fortalecer su capacidad de protección en el ámbito digital.

Sin dudas ha generado un debate en relación con la seguridad, la privacidad y la libre expresión en el ciberespacio. Aunque el gobierno chino argumenta que la ley tiene como objetivo garantizar la seguridad nacional y proteger los derechos e intereses legítimos de los ciudadanos y las empresas, sigue habiendo preocupaciones y críticas sobre su impacto en la libertad en línea y el acceso a la información.

2.3: Gestiones en el ciberespacio paralelo.

La ciber-soberanía es un concepto que ha surgido en el ámbito de las relaciones internacionales y se refiere al derecho y la capacidad de un Estado para ejercer control y gobernanza sobre su propio ciberespacio, protegiendo así su soberanía en el ámbito digital. En el contexto actual, donde la tecnología y las comunicaciones en línea desempeñan un papel cada vez más importante en las actividades económicas, políticas y sociales, la ciber-soberanía se ha convertido en un tema relevante y debatido.

El concepto de ciber-soberanía implica que cada Estado tiene el derecho de establecer y aplicar sus propias políticas, regulaciones y mecanismos de control en su ciberespacio, de acuerdo con sus intereses nacionales y objetivos estratégicos. Esto implica que los Estados buscan proteger sus sistemas de información y comunicación, salvaguardar su infraestructura digital crítica y garantizar la integridad de sus datos y la privacidad de sus ciudadanos.

En relación a las operaciones en el ciberespacio paralelo, el país en cuestión ha llevado a cabo diversas acciones para fortalecer su presencia y proteger sus intereses en el ámbito digital. Estas acciones son realizadas por la nación asiática a través de diversas entidades y actores relacionados, con el objetivo de ejercer influencia y mantener una posición estratégica en el ciberespacio.

Uno de los enfoques utilizados por este país es el desarrollo de capacidades cibernéticas avanzadas, como la creación de equipos de expertos en ciberseguridad y el establecimiento de unidades especializadas en operaciones en el ciberespacio. Estas unidades trabajan para salvaguardar la integridad de las redes y sistemas digitales, así como para detectar y responder a posibles amenazas cibernéticas.

En la obra "Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace" (2017), examina detalladamente la intersección entre la ciber-soberanía y la fragmentación de Internet. En su análisis, Mueller (2017) sostiene que la búsqueda de ciber-soberanía por parte de los Estados, incluido China, puede tener como consecuencia la fragmentación de Internet, lo cual implica la creación de redes y servicios controlados por cada Estado.

Mueller argumenta que los Estados en su afán de proteger su soberanía digital y ejercer control sobre su ciberespacio, pueden implementar políticas y regulaciones que limitan el flujo libre de información y restringen el acceso a ciertos contenidos en Internet. Estas acciones pueden generar una fragmentación de la red global, donde cada Estado establece sus propias normas y regulaciones en su propio segmento de Internet, formando así una especie de "Internet soberana".

En el caso seleccionado el gobierno ha implementado una serie de medidas para ejercer un mayor control sobre Internet, como el sistema de filtrado conocido como el Gran Cortafuegos y las restricciones en el acceso a ciertos sitios y servicios en línea. Estas acciones son ejemplos de cómo la búsqueda de ciber-soberanía puede llevar a la creación de una Internet más fragmentada, donde el acceso y la experiencia en línea pueden variar significativamente de un país a otro.

Mueller advierte que esta fragmentación de Internet puede tener implicaciones tanto para los Estados como para los usuarios individuales. Por un lado, la fragmentación puede permitir a los Estados ejercer un mayor control sobre la información y los flujos de datos, lo cual puede ser utilizado con fines de vigilancia y censura. Por otro lado, los usuarios individuales pueden experimentar restricciones en su acceso a información y servicios en línea, limitando su libertad de expresión y su participación en el ciberespacio global.

Este país ha llevado a cabo operaciones de vigilancia y recopilación de información en el ciberespacio paralelo, con el fin de monitorear y obtener datos relevantes para su seguridad nacional y sus intereses estratégicos. Estas operaciones incluyen el seguimiento de comunicaciones, el acceso a información sensible y la recolección de inteligencia cibernética.

Maurer (2019), en su investigación sobre la ciber-soberanía, ha realizado un análisis detallado del concepto y de cómo los Estados, incluyendo a la nación mencionada anteriormente, buscan ejercer control y proteger su soberanía digital a través de políticas y regulaciones que limitan la influencia externa y garantizan la autonomía en el ciberespacio.

Maurer (2019) sostiene que en un mundo cada vez más interconectado, los Estados están enfrentando nuevos desafíos en términos de seguridad y gobernanza en el ámbito digital. En este contexto, la ciber-soberanía emerge como un enfoque que busca preservar la capacidad de los Estados para tomar decisiones y ejercer control sobre sus propios asuntos en el ciberespacio.

En el caso específico de la nación en cuestión, se observa una clara voluntad de proteger su soberanía digital y ejercer un mayor control sobre su ciberespacio. A través de políticas y regulaciones específicas, se buscan limitar la influencia externa y garantizar la autonomía en la toma de decisiones relacionadas con la seguridad y el flujo de información en línea.

El gobierno ha implementado medidas como el sistema de filtrado y la regulación del acceso a ciertos sitios y servicios en línea, con el objetivo de mantener la integridad y la seguridad de su ciberespacio. Estas acciones son parte de la estrategia de ciber-soberanía que busca proteger la soberanía digital del país y salvaguardar sus intereses en el ámbito tecnológico.

Maurer (2019) destaca que el enfoque de ciber-soberanía plantea un desafío para la gobernanza global de Internet, ya que puede generar tensiones con los principios de apertura y libre flujo de información en la red. Sin embargo, sostiene que los Estados tienen el derecho y la responsabilidad de proteger sus intereses y asegurar su capacidad para gobernarse a sí mismos en el ámbito digital.

El concepto de "ciberespacio paralelo" fue acuñado por Timothy Thomas, un analista de inteligencia estadounidense, quien lo introdujo en su libro "Cyber Spoiling: The Chinese Threat to U.S. and Russian Security Interests" (2014). Thomas utiliza este término para describir las actividades cibernéticas realizadas por actores estatales y no estatales que operan fuera del alcance y control de los sistemas y regulaciones tradicionales.

En el caso de la nación mencionada anteriormente, la operación en el ciberespacio paralelo ha sido impulsada por su enfoque en la ciber-soberanía y la protección de sus intereses nacionales en el ámbito digital. A través de una serie de medidas y políticas, incluyendo la implementación de regulaciones específicas y el desarrollo de tecnologías y capacidades propias, la nación en cuestión ha buscado fortalecer su presencia y control en el ciberespacio.

Estas acciones incluyen la promoción de su propia infraestructura tecnológica y el desarrollo de servicios y plataformas digitales internos que ofrecen alternativas a los sistemas y servicios dominados por actores extranjeros. Además, se han implementado medidas de seguridad y ciberdefensa para proteger los activos y la información digital del país.

El objetivo principal de esta operación en el ciberespacio paralelo es salvaguardar la soberanía digital y proteger los intereses nacionales en el ámbito tecnológico. Al tener una presencia sólida en el ciberespacio, la nación mencionada anteriormente busca evitar la

dependencia de actores extranjeros y tener un mayor control sobre su propia infraestructura y recursos digitales.

Según Thomas (2014) , el ciberespacio paralelo se caracteriza por ser un ámbito en el que actores estatales y no estatales llevan a cabo acciones cibernéticas que están fuera del dominio de los sistemas y regulaciones convencionales. Estas actividades pueden incluir ciberataques, espionaje cibernético, sabotaje, propaganda en línea y otras acciones que tienen un impacto en el ámbito digital.

El término "paralelo" hace referencia a que estas actividades ocurren de manera simultánea y en paralelo al ciberespacio convencional, donde existen sistemas y regulaciones establecidas para regular el uso y la seguridad de las tecnologías de la información y la comunicación. El ciberespacio paralelo es una especie de "mundo virtual" donde los actores involucrados operan de forma más autónoma y eluden las restricciones y controles tradicionales.

La idea detrás del concepto de ciberespacio paralelo es resaltar la existencia de un espacio digital fuera del alcance de las estructuras y normas establecidas, lo que plantea desafíos en términos de gobernanza y seguridad. En el contexto específico de la obra de Thomas, se enfoca en la amenaza que representa para los intereses de seguridad de Estados Unidos y Rusia, destacando el papel de China en este panorama.

El concepto de ciberespacio paralelo ha sido objeto de debate y análisis en el ámbito de la seguridad cibernética y las relaciones internacionales. Proporciona una perspectiva para comprender las actividades cibernéticas que desafían las estructuras existentes y resalta la necesidad de abordar los aspectos de gobernanza y seguridad en el entorno digital.

Las operaciones cibernéticas de China han generado conflictos y tensiones con otros actores internacionales en el ámbito de la ciberseguridad y las relaciones internacionales.

En primer lugar, el gigante asiático ha sido acusada de llevar a cabo ciberataques y actividades de espionaje cibernético contra otros países. Estas acciones han sido objeto de preocupación y condena por parte de varios actores internacionales, quienes argumentan que representan una amenaza para la seguridad nacional y la propiedad intelectual.

las operaciones cibernéticas de China podrían ser interpretadas como estrategias para obtener ventajas competitivas y reducir la brecha tecnológica con otras potencias, como Estados Unidos (Li, 2016).. La apropiación de información confidencial y el robo de propiedad

intelectual han generado tensiones con otros países, especialmente con aquellos que son líderes en sectores tecnológicos y de innovación.

Con este foco se indica que las operaciones cibernéticas de China pueden considerarse como parte de su estrategia de ciber-soberanía, ya que buscan asegurar su capacidad de tomar decisiones y ejercer control sobre sus asuntos en el ámbito digital. Estas operaciones podrían ser interpretadas como esfuerzos para salvaguardar su seguridad y prevenir la dependencia de tecnologías extranjeras en áreas críticas. Las teorías expuestas permiten comprender las motivaciones y objetivos detrás de las acciones de China en el ciberespacio, así como sus implicaciones en las relaciones internacionales y la seguridad global.

Otro punto de conflicto surge en relación con la censura y el control de la información en línea. China ha implementado políticas y regulaciones que restringen el acceso a determinados contenidos y plataformas en internet, lo que ha generado críticas en términos de libertad de expresión y derechos humanos.

Estos conflictos y tensiones han llevado a confrontaciones diplomáticas y disputas comerciales entre China y otros actores internacionales, especialmente Estados Unidos. Las acusaciones de espionaje cibernético, la competencia en el ámbito tecnológico y las preocupaciones de seguridad han sido elementos clave en estas fricciones.

2.4 : Desconexión China de la red mundial.

La "Desconexión Digital" de un país se refiere a su intento de limitar o controlar el acceso a la red mundial de Internet y desarrollar una red digital interna con regulaciones y restricciones propias. Este enfoque ha sido utilizado por varios países, incluidos Irán y Rusia, con el objetivo de fortalecer la soberanía digital y la capacidad de control del Estado sobre el ciberespacio. Según Mueller (2010), la desconexión digital ha sido una estrategia adoptada por algunos Estados para mantener el control sobre el ciberespacio y proteger su soberanía digital.

El impacto de la desconexión digital en la economía ha sido mixto. Por un lado, esta política ha permitido a China desarrollar una poderosa industria de tecnología de la información y las comunicaciones, con empresas líderes en áreas como el comercio electrónico, los pagos móviles y la inteligencia artificial. La desconexión también ha protegido a las empresas chinas de la competencia extranjera en ciertas áreas, lo que ha contribuido al crecimiento económico del país. Sin embargo, según West (2016), la desconexión también ha tenido un impacto negativo en la economía china, al restringir el acceso a información y recursos en línea para las empresas que operan en el extranjero.

En cuanto al impacto en la sociedad, la desconexión digital ha dado lugar a un ecosistema digital único en China, con plataformas y servicios en línea específicos del país que no están disponibles en otros lugares. Esto ha llevado a una creciente brecha digital entre China y otros países, lo que puede afectar la forma en que las personas acceden a la información y se comunican en línea. La Gran Muralla Digital también ha restringido la libertad de expresión y la privacidad en línea, lo que ha generado preocupaciones sobre los derechos humanos y la censura gubernamental.

En el ámbito de las relaciones internacionales, la desconexión digital de China ha generado conflictos con otros actores internacionales, especialmente con los Estados Unidos. Según Creemers (2019), la política de censura y control del ciberespacio en China ha sido objeto de críticas por parte de Estados Unidos y otros países que defienden la libertad de expresión y la privacidad en línea. Además, las medidas de ciberseguridad implementadas por China han sido percibidas como una amenaza para la seguridad y la integridad de las redes y sistemas internacionales.

En resumen, la desconexión digital de China ha tenido impactos significativos en la economía y la sociedad del país, así como en sus relaciones con otros actores internacionales. Si bien ha permitido el desarrollo de una poderosa industria de tecnología de la información y las comunicaciones, también ha generado preocupaciones sobre la libertad de expresión, la privacidad en línea y el acceso a la información. En el escenario internacional, la desconexión digital ha llevado a tensiones y conflictos con otros países que defienden una visión más abierta y libre del ciberespacio.

Conclusión.

Durante la última década, China ha experimentado un avance en términos de capacidad tecnológica, lo que le ha permitido posicionarse como una potencia mundial en el ámbito de la tecnología de la información y las comunicaciones. Desde el 2010, el país ha realizado inversiones significativas en investigación y desarrollo, lo que ha impulsado la innovación en áreas clave como inteligencia artificial, 5G, internet de las cosas y tecnologías de la información. Este crecimiento tecnológico ha sido impulsado por una estrategia gubernamental ambiciosa que busca convertir a China en una "sociedad de innovación" y en una economía basada en el conocimiento (National Medium- and Long-Term Plan for Science and Technology Development 2006-2020).

En términos de soberanía digital, China ha desarrollado políticas y regulaciones para proteger su ciberespacio y garantizar la seguridad de la información. La promulgación de la Ley de Ciberseguridad en 2016 y la creación de la Gran Muralla Digital son ejemplos de las medidas que ha tomado el país para ejercer control sobre el ciberespacio y proteger su soberanía digital. La desconexión digital, aunque ha generado controversia, ha permitido a China desarrollar una industria de tecnología de la información y las comunicaciones fuerte y competitiva, así como proteger su ciberespacio de posibles amenazas externas.

La defensa de la soberanía digital de China ha estado motivada por varios factores. En primer lugar, el enfoque del gobierno chino en la capacidad tecnológica y la soberanía digital refleja una comprensión profunda de la importancia que tienen estas cuestiones en el escenario global actual. Este gigante ha experimentado un crecimiento económico impresionante en las últimas décadas y se ha convertido en una potencia económica de primer orden. La capacidad tecnológica no solo impulsa la innovación y la eficiencia en sectores clave como la manufactura, la inteligencia artificial y las comunicaciones, sino que también genera ventajas competitivas y aumenta la productividad. El gobierno chino ha demostrado una determinación constante para alcanzar la vanguardia tecnológica en áreas estratégicas, como el 5G, la inteligencia artificial, la impulsión de empresas chinas como Huawei y la ciberseguridad.

En segundo lugar, la ideología y la política del Partido Comunista Chino desempeñan un papel crucial en la formulación de la estrategia de China hacia el ciberespacio y la soberanía digital. Este partido ha gobernado China desde su fundación en 1949 y ha mantenido un

control centralizado sobre el país. Su énfasis en la estabilidad y el control social son fundamentales en la toma de decisiones.

En este contexto, esta política se refleja en la forma en que aborda el ciberespacio. Para el partido, mantener el control y la autoridad del Estado en todos los ámbitos de la sociedad es esencial para garantizar su permanencia en el poder y la estabilidad del país. Esto se traduce en una actitud cautelosa hacia las tecnologías de la información y la comunicación, donde el acceso a la información y la comunicación en línea se gestiona con el objetivo de prevenir cualquier amenaza potencial a la seguridad y estabilidad del régimen.

La política de mantener el control centralizado se combina para justificar la necesidad de la Ley de Ciberseguridad de China y otras medidas relacionadas con la soberanía digital. La percepción de que el control estatal es necesaria para garantizar la seguridad y estabilidad del país es un componente clave de la política cibernética de China, y esta política se ha desarrollado y perfeccionado a lo largo de los años para responder a las cambiantes amenazas en el ciberespacio.

En tercer lugar, las tensiones en las relaciones internacionales y la rivalidad con Estados Unidos han llevado a China a fortalecer su capacidad tecnológica y ciberseguridad como parte de su estrategia de proteger sus intereses nacionales y su posición como actor global. Por ejemplo, esta inversión y enfoque en la innovación han llevado a Huawei y a China en su conjunto a concentrarse en la competencia tecnológica y el resguardo soberano como una estrategia clave. Huawei ha capitalizado su liderazgo tecnológico para asegurar su posición en el mercado global y para garantizar la autonomía y la seguridad en su infraestructura tecnológica, en línea con los intereses de la nación en medio de un entorno internacional cada vez más competitivo y complejo, como también ha sabido aprovechar esta coyuntura para enfocarse en la autarquía tecnológica y en la independencia de los sistemas de información, reduciendo la dependencia de tecnologías extranjeras.

Aunque China ha logrado importantes avances en su capacidad tecnológica y en la defensa de su soberanía digital, enfrenta desafíos y críticas. Las medidas de censura y control del ciberespacio han sido objeto de controversia y han generado preocupaciones sobre la libertad de expresión y los derechos humanos en la comunidad internacional, particularmente desde los países pertenecientes al denominado “Occidente”. La desconexión digital ha llevado a tensiones con otros actores internacionales, especialmente con Estados Unidos, que defiende una visión más abierta y libre del ciberespacio.

El ciberespacio se ha convertido en un campo de juego en el que las naciones interactúan y compiten, y donde la amenaza de ataques cibernéticos y la pérdida de información sensible pueden tener consecuencias graves. La protección de la soberanía digital implica no solo salvaguardar los sistemas tecnológicos vitales del país, sino también prevenir intrusiones que podrían poner en peligro la integridad de la información gubernamental, económica y de seguridad.

La capacidad de participar de manera efectiva en las discusiones sobre gobernanza de Internet y ciberseguridad a nivel internacional es esencial para proteger los intereses de China en el ciberespacio y mantener su soberanía digital. Es esencial que China encuentre un equilibrio entre el control del ciberespacio y el respeto a los derechos y libertades fundamentales para garantizar su posición como una potencia tecnológica y mantener relaciones constructivas con otros actores internacionales.

A raíz de lo presentado, para concluir, se ratifican las hipótesis planteadas en este trabajo. Se determina que el aumento en la capacidad tecnológica y soberanía digital que implementó el gobierno chino refleja la comprensión de la importancia de estos elementos para el desarrollo económico, la seguridad nacional y la influencia global del país. Ha logrado hacer del eje de la competencia tecnológica y el resguardo soberano una parte central de su estrategia en un contexto marcado por las tensiones en las relaciones internacionales y la creciente rivalidad con Estados Unidos. El avance tecnológico y la ciberseguridad se han convertido en pilares fundamentales para China y su aspiración de proteger sus intereses nacionales y consolidar su posición como actor global.

Estos pilares no sólo son fundamentales para el presente de China, sino que también determinarán en gran medida su posición en el futuro en un mundo cada vez más digital y conectado. En esta encrucijada de desafíos y oportunidades, el resguardo de sus intereses nacionales y la consolidación de su posición como líder global han tejido la trama de su historia en el ciberespacio. A medida que la competencia tecnológica se convierte en el nuevo campo de batalla y la ciberseguridad en el escudo de la soberanía, China, a través de figuras como Huawei, ha forjado un camino audaz hacia un horizonte en el que el poderío tecnológico y la autonomía digital se alzan como estandartes de su visión futura. En esta convergencia de fuerzas y valores, China ha demostrado que, en la intersección de la cibernética y la soberanía, el futuro no solo se imagina, sino que se construye con determinación y visión.

BIBLIOGRAFIA

- Agnew, J. (1998). Geopolítica: una re-visión de la política mundial. Cap. 6.
- Arquilla, J. (2012). The Chinese People's Liberation Army and Information Warfare. *Journal of Strategic Studies*, 35(3), 381-407.
- Bamford, J. (2013). The Deep Web: An Ever-Changing World. *Wired*.
- Baños, P. (2018). El dominio mundial: Elementos del poder y claves geopolíticas.
- BBC News. (2019, May 22). US-China Trade War: Huawei Boss Says Company Will Not Be 'Silent Lamb'. <https://www.bbc.com/news/business-48368460>
- Buzal, G. D. (2014). Fronteras en el ciberespacio: el nuevo mapa mundial visto desde Buenos Aires (Argentina).
- Castells, M. (2009). *Communication Power*. Oxford University Press.
- Chow, E. (2021, February 1). Huawei Turns to Enterprise Business and Smartphones to Counter U.S. Sanctions. *Reuters*. <https://www.reuters.com/article/us-huawei-strategy-idUSKBN2A11SO>
- Creemers, R. (2019). China's Digital Nationalism. *Journal of Contemporary China*, 28(118), 75-90.
- Creemers, R. (2016). The global expansion of China's digital policy: An analysis of trade agreements, domestic laws and regulation. *Journal of Contemporary China*, 25(102), 382-397.
- Creemers, R. (2019). The Evolution of China's Cybersecurity Law.
- Deibert, R. (2013). *Black Code: Inside the Battle for Cyberspace*. *Signal*.
- Deibert, R. J. (2003). *Black Code: censorship, surveillance, and the militarization of cyberspace*. *Between the Lines*.
- Dunworth, T., & Walther, S. (2019). Cybersecurity in China: an emerging threat to the West?. *The RUSI Journal*, 164(6), 40-47.
- Finklea, K. M., & Theohary, C. A. (2013). *China's Cyber Espionage: The National Security Impact of Economics*. Congressional Research Service.

- Fuente Cobo, I. (2019) Un mundo globalizado regido por la geopolítica. Recuperado de Un mundo globalizado regido por la geopolítica - Dialnet (unirioja.es)
- Goldsmith, J. L., & Wu, T. (2006). Who controls the Internet?: Illusions of a borderless world. Oxford University Press.
- Hannas, W. C., Mulvenon, J. C., & Puglisi, A. M. (2014). Chinese Industrial Espionage: Technology Acquisition and Military Modernisation. Cambridge University Press.
- Hillman, J. E., & Meltzer, J. P. (2020). Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security (CSIS Report). Center for Strategic and International Studies.
- Huang, E. (2019, August 28). China to boost purchases of Huawei, other US tech products, state media says. South China Morning Post. <https://www.scmp.com/tech/policy/article/3024454/china-boost-purchases-huawei-other-us-tech-products-state-media-says>
- Jordan, J. (2013). Manual de estudios estratégicos y seguridad internacional. Cap.1
- Lawrence Freedman (2019) La guerra futura: Un estudio sobre el pasado y el presente.
- Li, X., & Janssen, M. (2019). Understanding China's Cybersecurity Law: Context, Compliance, and Legal Risks. Government Information Quarterly, 36(2), 323-335.
- Lipovetsky, G. El reino de la hipercultura: cosmopolitismo y civilización occidental.
- Liu, Y. (2020, July 16). How Huawei Survives: China and the Politics of Global Telecom. Council on Foreign Relations. <https://www.cfr.org/backgrounder/how-huawei-survives-china-and-politics-global-telecom>
- Lopez Rosso, I. (2021). La Guerra tecnológica entre China y Estados Unidos. Foreign Affairs Latinoamérica. Recuperado de La guerra tecnológica entre China y Estados Unidos | Foreign Affairs Latinoamérica | (revistafal.com)
- MacKinnon, R. (2009). Consent of the Networked: The Worldwide Struggle for Internet Freedom. Basic Books.

- Men, J. (2017). China's Cybersecurity Law: Potential Impacts on International Trade and Intellectual Property Rights. *Northwestern Journal of International Law & Business*, 37(3), 369-398.
- Moret Millas, V. (2019). El despliegue de las redes 5G, o la geopolítica digital. Real Instituto Elcano. Recuperado de El despliegue de las redes 5G, o la geopolítica digital - Elcano (realinstitutoelcano.org)
- Morgenthau, H. J. (1948). *Politics Among Nations: The Struggle for Power and Peace*.
- Morgenthau, H. J. (1973). "Scientific Man vs. Power Politics". *The American Political Science Review*, 67(4), 930-932.
- Mozur, P., & Mui, C. (2019, May 22). As Huawei Loses Google, the U.S.-China Tech Cold War Gets Its Iron Curtain. *The New York Times*. <https://www.nytimes.com/2019/05/22/technology/huawei-trump-china-iron-curtain.html>
- Mozur, P., & Ramsay, S. (2020, June 10). Huawei, 5G and China as Global Tech Threats. *The New York Times*. <https://www.nytimes.com/2020/06/10/technology/huawei-5g-china-threats.html>
- Mozur, P., Wakabayashi, D., & Zhong, R. (2019, 20 de mayo). Huawei Executive Accuses U.S. of Bullying as Tech War Heats Up. *The New York Times*. <https://www.nytimes.com/2019/05/20/business/huawei-trump-china-trade.html>
- Nye, J. S. (1990). *Bound to Lead: The Changing Nature of American Power*.
- Nye, J. S. (2004). *Soft Power: The Means to Success in World Politics*.
- Parmar, N. (2019). Huawei: The Story Behind the Ban. *Harvard Business Review Digital Articles*, 2-5. <https://hbr.org/2019/05/huawei-the-story-behind-the-ban>
- Shirk, S. L. (2019). The U.S. and China: Linked by Trade, Warily. *Journal of International Affairs*, 73(1), 15-30.
- Soble, J., & Mozur, P. (2019, May 21). Behind the Rise of Huawei: The Company's Own Story. *The New York Times*. <https://www.nytimes.com/2019/05/21/technology/huawei-trump-china-trade.html>
- Smith, G. (2016). The rise of China's cybersecurity law. *China Brief*, 16(19), 3-7.

- Taylor, P., & Qiao, Y. (2008). Huawei: From Local Champion to Global Player. *Knowledge, Technology, & Policy*, 20(3), 157-176. <https://doi.org/10.1007/s12130-008-9045-8>
- United States Senate. (2018). Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers. Committee on Commerce, Science, and Transportation. <https://www.commerce.senate.gov/2018/7/threats-to-u-s-networks-oversight-of-chinese-government-owned-carriers>
- "Huawei Corporate Information," Huawei) (Huawei. (n.d.). Corporate Information. Huawei. <https://www.huawei.com/en/about-huawei/corporate-information>)
- "2019 Annual Report," Huawei, 2020) (Huawei. (2020). 2019 Annual Report. Huawei. https://www-file.huawei.com/-/media/corporate/pdf/annual_report/annual_report_2019_en.pdf
- Waltz, K. N. (1979). *Theory of international politics*. Waveland Press.
- Yang, G., & Cui, L. (2018). The Belt and Road Initiative and China's National Cybersecurity: Challenges and Prospects. *Journal of Contemporary China*, 27(113), 646-660.
- Xiaobing Li : "China's Cyber Power" (2016)