ACADEMIA DIPLOMÁTICA DEL PERÚ JAVIER PÉREZ DE CUÉLLAR

PROGRAMA DE MAESTRÍA EN DIPLOMACIA Y RELACIONES INTERNACIONALES

TESIS PARA OBTENER EL GRADO ACADÉMICO DE MAESTRO EN DIPLOMACIA Y RELACIONES INTERNACIONALES

TEMA DE TESIS:

“Oportunidades de Ciberdiplomacia para la Política Exterior del Perú”

PRESENTADO POR:

Esteban José Pacheco Araoz

ASESORES

Asesor temático: PS Julio Antonio Ubillús Ramírez

Asesor metodológico: Dra. Milagros Aurora Revilla Izquierdo

Lima, 09 de noviembre de 2020

Resumen

El ciberespacio tiene una influencia transversal a los intereses políticos, sociales y económicos de las naciones, por ello se ha convertido en un área clave para ejercer el dominio. En paralelo, en el contexto de la Cuarta Revolución Industrial, las grandes empresas tecnológicas han conseguido posicionarse y obtener una enorme influencia global en este ámbito. Las grandes potencias han diseñado asertivas políticas exteriores para defender y promover sus intereses en el ciberespacio. Con estos elementos, esta investigación pretende, a partir de las recientes iniciativas nacionales, plantear una propuesta para la política exterior del Perú que le permita promover y defender sus intereses en el ámbito del ciberespacio.

Palabras clave: Ciberespacio, ciberdiplomacia, grandes empresas tecnológicas, Cuarta Revolución Industrial, política exterior del Perú.

Abstract

Cyberspace has an influence that is transversal to the political, social and economic interests of nations, for this reason it has become a key area to exercise dominance. At the same time, in the context of the Fourth Industrial Revolution, large technology companies have managed to position themselves and gain enormous global influence in this area. The great powers have designed assertive foreign policies to protect their interests in cyberspace. With these elements, this research aims, based on recent national initiatives, to propose a foreign policy that allows for Peru it to promote and defend its interests in the field of cyberspace.

Keywords: Cyberspace, cyberdiplomacy, large technology companies, Fourth Industrial Revolution, Peruvian foreign policy.

ÍNDICE

Resumen 2
Abstract 3
INTRODUCCION 6
CAPÍTULO I: EL INTERÉS POR EL CIBERESPACIO 8
1. El actual orden mundial y la Cuarta Revolución Industrial 8
2. Ciberdiplomacia en la geopolítica del ciberespacio 12
2.1. Ciberdiplomacia: el ciberespacio y la política exterior 14
2.2. Prioridades de la ciberdiplomacia 16
2.2.1. Ciberseguridad y ciberdefensa 17
2.2.2. Economía digital y tecnológica 20
2.2.3. La Gobernanza Global Digital 26
3. Las grandes empresas tecnológicas y el ciberespacio 29
3.1. Las relaciones entre los Estados las grandes empresas tecnológicas 32
Las relaciones “bilaterales” de las grandes empresas tecnológicas 33
Las relaciones “multilaterales” de las grandes empresas tecnológicas 36
3.2. Los intereses de las grandes empresas de tecnología en el ciberespacio 37
Privacidad de la información 37
Ciberseguridad 38
Contenidos libres y excepciones al derecho de autor 39
Neutralidad en la red 39
Reglas antimonopolio 40
CAPÍTULO II: LAS POLÍTICAS EXTERIORES PARA EL CIBERESPACIO 41
1. Ciberdiplomacia y el liderazgo geopolítico del ciberespacio 41
1.1. EEUU: La superpotencia en el ciberespacio 41
1.2. China: Supremacía del Estado 44
1.3. Rusia: Un espacio de reivindicación 47
1.4. Francia: estrategia internacional para las tecnologías digitales 49
1.5. Intereses de la Unión Europea en la ciberdiplomacia 51
2. Experiencias de ciberdiplomacia, competitividad y liderazgos regionales 52
2.1. Ciberdiplomacia en Latinoamérica 53
2.2. Liderazgo digital de países pequeños 58
3. Marco institucional e intereses peruanos en el ciberespacio 65

3.1. La Ciberseguridad en el Perú 68
3.2. Economía digital y tecnológica 71
3.3. Gobernanza de internet 73
CAPÍTULO III: EL MINISTERIO DE RELACIONES EXTERIORES Y LA CIBERDIPLOMACIA 76
1. Marco institucional del Ministerio de Relaciones Exteriores y la Ciberdiplomacia 76
1.1. El MRE y el Convenio de Budapest 77
1.2. El MRE en la Organización de las Naciones Unidas 78
1.3. El MRE y el Llamamiento de Paris 80
1.4. Los asuntos del ciberespacio en la OEA 80
1.5. Ciberdiplomacia en APEC 82
1.6. Ciberdiplomacia en la Alianza del Pacífico 83
1.7. Ciberdiplomacia en la Comunidad Andina 85
1.8. El Grupo de Trabajo de la Cuarta Revolución Industrial 86
2. Necesidad de una Estrategia y Política Exterior para asuntos del ciberespacio 88
2.1. Determinación de posturas nacionales en la geopolítica del ciberespacio 89
2.2. El Acuerdo de Economía Digital (DEPA) 91
2.3. La Alianza del Pacífico como espacio prioritario en la Estrategia Política Exterior en asuntos del ciberespacio 91
2.4. Los Agregados de Ciencia, Tecnología e Innovación 92
2.5. Capacitación permanente del personal diplomático 93
2.6. Reconocimiento y vinculación con las grandes empresas tecnológicas 94
2.7. Defensa y promoción de las empresas tecnológicas nacionales 94
3. Estrategia de relacionamiento con las grandes empresas tecnológicas de Silicon Valley 95
3.1. Primeros pasos: un nuevo funcionario en Consulado General del Perú en San Francisco 97
3.2. Trabajo desde la Alianza del Pacífico con las grandes empresas tecnológicas en Silicon Valley 98
3.3. Centros de Innovación de la Alianza del Pacífico 100
CONCLUSIONES 101
BIBLIOGRAFÍA 103
ANEXO 114

INTRODUCCION

El mundo ha experimentado profundos y determinantes cambios en el ámbito tecnológico. Los principales intereses de los Estados se ven afectados por el uso universal del ciberespacio y, gracias a su dimensión transnacional se ha vuelto un territorio ingobernable para los Estados.

En el marco de la competencia entre China y Estados Unidos por la hegemonía mundial, el ciberespacio se ha convertido en un área clave para ejercer el dominio ya que es transversal a sus posiciones en lo político, social y económico. Sin embargo, estas potencias no son las únicas capaces de ejercer presión y dominio en este ámbito, otros Estados y actores no estatales han alcanzado un enorme nivel de desarrollo e influencia en este ámbito.

En este contexto, el Perú, cuya economía y desarrollos aún se basan en la exportación de materias primas, se ubica como un actor internacional de poco peso relativo en los temas vinculados al ciberespacio. Por ello, resulta importante plantear una estrategia de política exterior en el ámbito del ciberespacio, que le permita al Perú posicionarse de una manera conveniente en el escenario internacional y al hacer esto, potenciar los desarrollos nacionales.

La hipótesis que plantea esta investigación es que, el Perú, como parte de una estrategia de política exterior para asuntos del ciberespacio debería priorizar una mayor vinculación con las grandes empresas tecnológicas del mundo. Esto, le permitiría promover, defender sus intereses en este ámbito de manera transversal y originar la atracción de tecnología al ámbito nacional. De esta manera, el Perú se acercará a su objetivo de convertirse en una potencia regional emergente.

Para que el presente trabajo alcance este objetivo, se desarrolla una metodología basada en una investigación deductiva, debido a que se empezará abordando la importancia de las nuevas tecnologías y del desarrollo del ciberespacio en el escenario internacional, seguido por comprender el rol de las políticas exteriores por parte de las principales potencias para alcanzar el actual ordenamiento, para luego pasar al análisis focalizado en lo que concierne al Perú.

Asimismo, esta es una investigación descriptiva y analítica, ya que se centra en desarrollar la naturaleza del fenómeno y en lo que deberá hacer el Perú al respecto. Finalmente, la investigación será cualitativa ya que la investigación se basará en la recopilación de base de datos existentes y en entrevistas a expertos.

En ese sentido, se ha desarrollado la investigación en tres capítulos, teniendo en cuenta que la misma pretende analizar el fenómeno del ciberespacio desde una perspectiva de política exterior.

En el primer capítulo se muestra la relevancia que ha alcanzado el ciberespacio en el actual sistema internacional y cómo los Estados han encontrado en la diplomacia un medio adecuado para defender sus intereses en ese ámbito. Para ello, se desarrolla el término de la "ciberdiplomacia" como el recurso de las herramientas diplomáticas y el desempeño de funciones diplomáticas para asegurar los intereses nacionales con respecto al ciberespacio. Los principales desarrollos de este neologismo son André Barrinha y Thomas Renard. Esta parte finaliza mostrando cómo los intereses prioritarios para los Estados en este ámbito son equivalentes a los de las grandes empresas tecnológicas.

En el segundo capítulo se explica las estrategias que vienen desplegando las principales potencias mundiales en el ámbito del ciberespacio con el objetivo de defender y proyectar sus intereses en este dominio. Como se podrá ver en este capítulo, existe un predominio de Estados Unidos y de China en este ámbito, pero otras potencias más pequeñas han alcanzado cierto liderazgo y la capacidad de posicionarse adecuadamente. Finalmente, con el propósito de comprender la política que necesitaría el Perú en torno al ciberespacio se muestran los desarrollos, iniciativas e intereses nacionales en este ámbito.

En el tercer capítulo, se toma el marco institucional del Ministerio de Relaciones Exteriores y se llega a proponer que como uno de los integrantes del Sistema Nacional de Transformación Digital y en el marco de la elaboración de la actual Política Nacional de Transformación Digital y la Estrategia Nacional de Transformación Digital es necesario complementar esas iniciativas por medio de una Política Exterior para Asuntos del Ciberespacio. Finalmente, en el marco del planteamiento de la propuesta, se identifica la necesidad de profundizar el relacionamiento con las grandes empresas tecnológicas, como alternativa para promover y defender los intereses nacionales en este ámbito.

CAPÍTULO I: EL INTERÉS POR EL CIBERESPACIO

1. El actual orden mundial y la Cuarta Revolución Industrial

Preguntarse por cómo está establecido el orden mundial implica buscar comprender la organización que rige entre los actores estatales y no estatales. Mikael Baaz, sostenía que:

"El concepto de orden mundial resume el sistema de reglas formales e informales que imparte cierta conformidad legal y predictibilidad a las interacciones nacionales y transnacionales que se producen en ausencia del marco político y de la inequívoca autoridad que hasta ahora ha caracterizado al Estado-nación soberano en el orden westfaliano" (Baaz, 2005, p. 18).

Con esta definición se le reconoce a los Estados un rol privilegiado y se evidencia la característica anárquica del orden mundial. Para Bulls, a pesar de que el sistema no tiene un órgano central de poder y gobierno, se mantiene un orden entre los actores (Bulls, H., 2000, p.44).

Según Kissinger, refiriéndose al orden mundial después de la Segunda Guerra Mundial menciona que, "el sistema contemporáneo global ha logrado controlar esta naturaleza anárquica mediante una extensa red de estructuras legales y organizaciones internacionales destinadas a fomentar el libre comercio y un sistema financiero internacional estable" (Kissinger, H, 2014, p.8).

El nivel de desarrollo económico, político y militar de los Estados Unidos le permitió tener una posición privilegiada en la segunda mitad del siglo XX. Sin embargo, en el escenario de la Posguerra Fría, llegó a ser denominado la "superpotencia solitaria" (Mugica, 2018, p. 2), la "potencia hegemónica"(Borda, 2013, p. 72) y "potencia unipolar"(Alcalde, 2009, p. 10) y se presumía que el siglo XXI sería el "segundo siglo americano"(Zuckerman 1998, p. 146).

No obstante, el impresionante crecimiento de China desde las reformas económicas del año 1979, el incremento de su poder militar, sus desarrollos tecnológicos y sus aspiraciones geopolíticas motivan a Kissinger a mencionar que "China y Estados Unidos son actualmente las mayores potencias mundiales, por su peso económico, político,

cultural y militar, e incluso ciberbélico” Kissinger (2014, p. 198). Un nuevo orden se estaría desarrollando y se vislumbra un cambio en el orden mundial para los próximos años.

A pesar de que la emergencia china y su creciente rivalidad con Estados Unidos es uno de los temas centrales para entender el orden mundial actual, Kissinger menciona que la ciencia y la tecnología son los conceptos que guían nuestra época (Kissinger, H., 2014, p. 177).

Los desarrollos científicos y tecnológicos han originado el llamado “ciberespacio”, como el ámbito en donde interactúan los medios informáticos de todo el mundo. Este terreno puede ser considerado como un reflejo y extensión de la realidad física en donde se pueden realizar actividades tan distintas como el comercio, el delito, la medicina, la política y la seguridad tienen su contraparte en el mundo virtual.

Así como en la realidad física hay actores con más poder y capacidades que otros, esta situación se percibe en esta la realidad virtual. Además, tiene una naturaleza transnacional que no conoce fronteras físicas.

Las relaciones de poder que existen entre los Estados en la realidad física se ven sumamente modificadas en este ámbito. El poder de los Estados en el ciberespacio ya no se basa por el poderío nacional basado en territorio, geografía, ubicación, población, ejército. Por ello, incluso un Estado pequeño, pobre y con poca población puede alcanzar un elevado nivel de influencia mundial en este contexto.

En ese sentido, los importantes desarrollos en el ciberespacio no solo han desordenado completamente el panorama geopolítico, sino que en este escenario la emergencia e importancia de actores no estatales se ha incrementado considerablemente y su influencia abarca otros ámbitos y sectores.

Algunos de los actores no estatales relevantes en el ciberespacio, son los hacktivistas, los ciberterroristas, los ciberdelincuentes, personalidades influyentes, la sociedad civil, los medios de comunicación, las grandes empresas tecnológicas, entre otros.

Dentro de estos nuevos actores mencionados, sobresalen las grandes empresas tecnológicas quienes cuentan muchas veces con presupuestos para la inversión innovación y desarrollo más elevados que muchos Estados y regiones. De igual modo,

suelen disfrutar del personal más capacitado, compiten con la última tecnología y sus innovaciones alcanzan todos los rincones del mundo.

Por lo mencionado, estas empresas tecnológicas tienen una gran capacidad de influencia y, en gran medida, el poder necesario para defender y proyectar sus intereses en el ciberespacio, en la realidad física y se han constituido en actores *de facto* fundamentales del orden mundial. El nuevo orden mundial muestra que la digitalización y las grandes empresas tecnológicas desempeñan un papel cada vez mayor, y la diplomacia estatal debe adaptarse a esta nueva realidad.

Para Morozov (2017), el ascenso de Silicon Valley, como conjunto de las grandes empresas tecnológicas está intrincadamente ligado al ascenso de la supremacía de poder estadounidense, producto del vacío de poder que se produjo tras el repentino término de la guerra fría, y al entusiasmo y búsqueda de eficiencia y ahorro, que habría de ser proporcionada por la digitalización y la automatización, o una determinada combinación de ambas (Morozov, 2017, p. 22).

A lo dicho hasta el momento, se suma que la evolución de las tecnologías en las últimas dos décadas ha acelerado los cambios de una manera más vertiginosa y actualmente existen pocos ámbitos que no sean influenciados por el ciberespacio.

En ese sentido, la novedad del escenario en que los actores se desenvuelven es la llamada “Cuarta Revolución Industrial”. Ese término que fue acuñado por Klaus Schwab en la Feria de Hannover de 2011 y describe cómo los adelantos tecnológicos revolucionarán las cadenas globales de valor. Sin embargo, la Cuarta Revolución Industrial, tiene un alcance más amplio que la evolución de máquinas y sistemas inteligentes y conectados.

Según Schwab, la Cuarta Revolución Industrial “es la fusión de estas tecnologías y su interacción a través de los dominios físicos, digitales y biológicos lo que hace que la Cuarta Revolución Industrial sea fundamentalmente diferente de las anteriores” (Schwab, K. 2016, p. 13).

Según Schwab (2016, p.15), las razones que diferencian a la Cuarta Revolución de la Tercera son: 1) la velocidad de evolución de las innovaciones a un ritmo exponencial, 2) la amplitud y profundidad en los cambios de paradigma en economía, negocios, sociedad y las personas, lo cual genera cambios incluso en el “quienes somos”, y 3) el impacto en los

sistemas complejos entre y dentro de los países, empresas y la sociedad. Como este mismo autor indica, revolución implica un “cambio abrupto y radical” (Schwab, K. 2016, p. 15).

Un gran peligro de la Cuarta Revolución Industrial es la posibilidad de crear una exacerbada desigualdad. Al considerar que la segunda revolución industrial todavía no ha sido plenamente experimentada por más de mil millones de personas y que la tercera revolución industrial no ha llegado a la mitad de la población mundial, se evidencia que hay grupos humanos y regiones enteras que se están quedando rezagadas a la modernidad.

Por otro lado, la nueva revolución industrial está dirigida en primer lugar a las élites de los países desarrollados, lo que acentuaría aún más las diferencias con el resto de países y a los poderosos de esas naciones de los menos favorecidos. El escenario pone en riesgo el trabajo humano e incluso eliminará algunas actividades, lo que afectaría el empleo de millones de personas.

Más aún, esta situación es un riesgo para la seguridad de las regiones más atrasadas y es una gran desventaja para asegurar su desarrollo económico y social. Además, en palabras de Piketty “la desigualdad exacerbada es una amenaza a la democracia como la conocemos” (Piketty, 2014).

Ante este panorama, pareciera que los países de América Latina, incluyendo el Perú, están en riesgo de pretender afrontar esta nueva realidad mundial como meros abastecedores de recursos naturales y ser incapaces de posicionarse tanto en la realidad física como en la cibernética.

La poca inversión en educación, en investigación y desarrollo, ha generado que el peso relativo de la región latinoamericana en los temas tecnológicos y cibernéticos sea sumamente bajo, por lo que es más probable que las nuevas tecnologías y las innovaciones se concentran en otras regiones. Mientras que Corea e Israel invierten más del 4% del PBI en investigación y desarrollo, y Alemania y EEUU rondan el 3,03% y 2,79% respectivamente, la inversión promedio de los países latinoamericanos llega al 0,64% del PBI (RICTY, 2018, p.14).

Por ello, en el contexto de la Cuarta Revolución Industrial, se convierte en un ámbito de interés para los Estados en los ámbitos nacionales e internacionales y representa una amenaza y una oportunidad para los esfuerzos nacionales de desarrollo. Algunos Estados ya han articulado políticas exteriores en torno al ciberespacio

2. Ciberdiplomacia en la geopolítica del ciberespacio

El término “ciberespacio” proviene de la literatura de ficción y en la actualidad es un objeto de estudio y análisis que no cuenta con una definición universal. Para Aguirre (2001), lo determinante es entenderlo como un espacio virtual de interacción de información, que conecta todo el mundo. En este ámbito no existen fronteras, la aplicación de leyes se torna más compleja y prima en gran medida la capacidad de los actores.

Para Kuehl, el ciberespacio es un dominio operativo enmarcado por el uso de la electrónica para explotar información a través de sistemas interconectados y su infraestructura asociada (Kuehl, 2011, p. 23).

Como ha sido mencionado hasta el momento, en el ciberespacio convive una diversidad de actores internacionales. Sin embargo, no todos los actores son iguales, se tienen visiones diferentes, objetivos distintos e intereses contrapuestos en este ámbito.

Además, el anonimato que muchas veces permite este espacio hace difícil establecer reglas, determinar responsables y sancionar culpables. Finalmente, la anarquía es una de las características de este ambiente y depende en gran medida del poder de sus participantes (G. Barrios, 2015).

Los desarrollos y dependencia a las tecnologías han transformado al ciberespacio en un elemento determinante en la geopolítica mundial. Para Prado (2018), el ciberespacio se ha transformado en un nuevo escenario en donde se realizan las relaciones de poder, incluso reinterpreta la visión geopolítica de MacKinder, y la adapta al contexto actual: “quien gobierne los flujos comunicacionales gobernará el heartland cibernético y quien gobierne el heartland cibernético controlará el mundo”(Prado, 2018, p.1).

Para Segal (2020b), los Estados están usando el ciberespacio como arma, respaldan a hackers, atacan infraestructura crítica, interrumpen los sistemas democráticos con campañas de desinformación, roban datos personales, información de propiedad exclusiva

y secretos de estado y las reglas internacionales que rigen estas acciones no han sido eficientes. Por ello, existen riesgos para la estabilidad internacional, más aún con la rápida aparición de tecnologías que podrían cambiar el panorama estratégico, como la inteligencia artificial y las ciencias de la información cuántica (Segal, 2020b).

El poder para Weber (1944) consistía en “la probabilidad de imponer la propia voluntad dentro una relación social, aun contra toda resistencia y cualquiera que sea el fundamento de esa probabilidad”. Esa definición se puede aplicar al poder cibernético o ciberpoder como "la capacidad de usar el ciberespacio para crear ventajas e influir en eventos en otros entornos operativos y en los instrumentos de poder" (Kuehl, 2011, p. 24).

Si bien la información y la tecnología siempre han sido determinantes para el poder, en la actualidad, por medio del ciberespacio ahora son centrales para el manejo del poder. En ese sentido, el poder siempre ha dependido del contexto en el que se requiere, el poder en el ciberespacio depende de los recursos tecnológicos físicos, los conocimientos humanos en los procedimientos uso, el Know-How y la voluntad de ejercer el poder (Lazar, 2013, p. 6).

Para Joseph Nye, (2010, p.4) el ciberpoder consiste en “la capacidad de obtener resultados preferidos a través del uso de los recursos de información interconectados electrónicamente del dominio cibernético”.

Por otra parte, para Daniel Kuehl (citado por Nye, 2010) consistiría en “la capacidad de usar el ciberespacio para crear ventajas e influenciar eventos en otros medios operacionales y a través de los instrumentos de poder”. Por ello, se debe entender que el ciberpoder puede ser utilizado para obtener resultados deseados dentro del ciberespacio o para utilizar los instrumentos cibernéticos con el fin de producir resultados en otros dominios fuera de él (Eissa et al., 2014).

Según Segal (2016, pp. 31-38), el poder de los Estados en el ciberespacio depende (1) del tamaño, poder económico y uso de sus empresas nacionales, (2) de la capacidad del gobierno para trabajar con el sector privado, (3) del poder cibernético de las agencias militares y de inteligencia y (4) de la narrativa nacional sobre el ciberespacio.

El contexto de la Cuarta Revolución Industrial ubica a la información y la tecnología en el centro del poder y debate internacional. El dominio de las nuevas tecnologías se dirige a los Estados y grupos de poder más importantes y pueden ser una ocasión de acrecentar las diferencias entre Estados y entre grupos sociales.

2.1. Ciberdiplomacia: el ciberespacio y la política exterior

La diplomacia ha experimentado un fuerte impacto con la aparición del ciberespacio, la digitalización y las nuevas tecnologías. En los últimos años los estudiosos han acuñado una diversidad de neologismos como, “zoomplomacy”, “ciberdiplomacia”, “diplomacia digital” o “diplomacia tecnológica”, pues desde la diversidad de experiencias se ha querido categorizar la evidente relación e intereses entre las nuevas tecnologías y el ciberespacio con la diplomacia.

La “ciberdiplomacia” se refiere a la diplomacia del ciberespacio. Es decir, al recurso de la diplomacia, como herramienta pacífica y el desempeño de funciones diplomáticas para asegurar los intereses nacionales con respecto al ciberespacio (Barrinha & Renard, 2017, p. 355). Se convierte en una herramienta de política exterior para los intereses nacionales en el ciberespacio.

No debe confundirse con “diplomacia digital”, que se refiere al uso de herramientas digitales por parte de diplomáticos (Barrinha & Renard, 2017, p. 356). Es decir, a los nuevos métodos y modos de llevar a cabo la diplomacia con la ayuda de Internet, las Tecnologías de la Información y describe su impacto en las prácticas diplomáticas contemporáneas.

Para Barrinha (2017), la ciberdiplomacia la llevan a cabo los diplomáticos, reunidos en formatos bilaterales (como el diálogo entre Estados Unidos y China) o en foros multilaterales (como la ONU). Más aún, traspasa las fronteras de la diplomacia tradicional, ya que por la ciberdiplomacia se interactúa con diversos actores no estatales, como líderes de empresas de Internet (como Facebook o Google), empresarios tecnológicos u organizaciones de la sociedad civil (Barrinha & Renard, 2017, p. 355)

Para Tiirmaa-Klaar, a pesar que el término “ciberdiplomacia” está aún en evolución incluye las políticas de tecnología de la información y las comunicaciones (TIC), la ciberseguridad internacional, los diálogos cibernéticos bilaterales, la política económica vinculada al ciberespacio, los temas relacionados a la gobernanza de Internet, los derechos humanos en la era cibernética, la legislación en materia comercial y de propiedad intelectual, entre otros (Ziolkowski 2013, p. 509).

Para Danca, el ciberespacio se convierte en un componente fundamental de la política exterior y considera que:

> “debido a que las decisiones políticas sobre el ciberespacio tienen fuertes implicaciones internacionales, a pesar de lo anárquico de este ámbito, se requieren

> compromiso y colaboración internacionales… la actividad diplomática en el ámbito cibernético tiene una dimensión importante de cooperación, de celebración de compromisos diplomáticos y acuerdos multinivel, incluso con las partes interesadas del sector privado (Danca 2015, p. 94).

Para Riordan (2019b), existe una geopolítica del ciberespacio que proporciona un marco analítico para ayudar a los diplomáticos a comprender el comportamiento de los actores estatales y no estatales, y cómo es probable que respondan a los eventos tanto en el ciberespacio como en el espacio físico. Más aún, los diplomáticos pueden utilizar este análisis como base para desarrollar estrategias para el ciberespacio, incluido el diseño de protocolos para la gestión de crisis.

Los diplomáticos deben interactuar con el ciberespacio, es un ámbito demasiado importante como para dejarlo en manos de los técnicos o de los servicios militares o de inteligencia (Riordan, 2019b).

Por otro lado, el término “diplomacia tecnológica” nace en Dinamarca y manifiesta la preocupación por el impacto y poder de las nuevas tecnologías. Además, reconoce que las empresas tecnológicas multinacionales han obtenido un grado de influencia que desafía las estructuras de gobernanza tradicionales y se comportan cada vez más como actores globales de política exterior *de facto* (UDENRIGSMINISTERIET, 2019). En 2017, Dinamarca fue el primer país en reconocer la necesidad de una respuesta de política exterior al lanzar una iniciativa de diplomacia tecnológica.

Por medio de la diplomacia tecnológica, se explora la relación entre la diplomacia y las nuevas tecnologías y se realiza a partir de nombrar embajadores en el sector tecnológico privado, la mayoría del cual tiene una relación directa con el ciberespacio (UDENRIGSMINISTERIET, 2019).

Finalmente la “diplomacia científica” es una disciplina que no tiene una definición universal. Sin embargo, puede ser entendida como “el uso de colaboraciones científicas, tecnológicas y académicas entre países, regiones y sociedades para abordar problemas comunes y construir asociaciones internacionales sólidas”(Scitech Diplohub, 2015). Lo interesante de esta definición es que comprende distintos actores más allá de los Estados.

Como se puede notar, las prioridades y los enfoques de la ciberdiplomacia, la diplomacia tecnológica y la diplomacia científica están sumamente relacionadas y son complementarias para analizar los intereses nacionales en el contexto de la Cuarta Revolución Industrial.

Este trabajo se centra en el uso de la herramienta de la ciberdiplomacia y se le entiende como el uso de las herramientas diplomáticas para asegurar los intereses nacionales con respecto al ciberespacio. Además, nuestra definición entiende que por el tipo de relaciones que se realizan en el ciberespacio, la ciberdiplomacia no trata exclusivamente de las relaciones entre los Estados en torno al ciberespacio.

En el ámbito del ciberespacio las relaciones y los diálogos involucran a otro tipo de actores, tales como las organizaciones internacionales, los organismos no gubernamentales, las empresas tecnológicas, los actores subnacionales, la sociedad civil, personas influyentes, entre otros.

De igual modo, el fenómeno del ciberespacio y las nuevas tecnologías, en el contexto de la Cuarta Revolución Industrial, tienen una proyección indeterminada hacia el futuro, por lo que la ciberdiplomacia tendrá un rol cada vez más determinante en el futuro.

En el siguiente apartado se ampliarán los alcances y las prioridades de la ciberdiplomacia.

2.2. Prioridades de la ciberdiplomacia

Para el embajador Javier Pérez de Cuéllar, la política exterior es el conjunto de posiciones y acciones que adopta un Estado con la finalidad de preservar su seguridad, sus intereses e influencia y la diplomacia es el arte de poner apropiadamente en práctica esa política exterior (Pérez de Cuellar 1997, p.13).

Por ello, es fundamental definir de manera correcta y oportuna los intereses nacionales en el escenario mundial. Para Pearson, los Estados tienen al menos tres intereses fundamentales:

> “(1) asegurar la supervivencia física de la patria, lo que incluye proteger la vida de sus ciudadanos y mantener la integridad territorial de sus fronteras; (2) promover el bienestar económico de sus habitantes; y (3) preservar la autodeterminación nacional en lo que respecta a la naturaleza del sistema gubernamental del país y a la conducción de los asuntos internos” (Pearson, 2000, p. 159).

Si entendemos el ciberespacio como un reflejo y extensión de la realidad física, al considerar la definición anterior, se puede observar que los intereses nacionales de los Estados están presentes en este ámbito.

En primer lugar, por medio del ciberespacio, la seguridad de los Estados y su población puede ser vulnerada. De igual modo, el ciberespacio es en la actualidad un instrumento fundamental que permite oportunidades de desarrollo económico y social. Finalmente, el ciberespacio afecta los intereses en la autodeterminación nacional, y puede ser entendido como una nueva frontera a la cual dominar y gobernar.

Para Puente “el ciberespacio se ha convertido, además de en un instrumento, que es lo que le dio origen, en un espacio más, que junto a la tierra, el mar, el aire y el espacio exterior, constituyen un desafío en términos de soberanía y Estado”(Puente, 2018).

A continuación se profundizará en los temas que la ciberdiplomacia, como herramienta de política exterior, debe asumir como prioritarios. Se debe destacar que los temas a mencionar no es un listado exhaustivo.

2.2.1. Ciberseguridad y ciberdefensa

La ciberseguridad surgió como respuesta a la expansión del uso del ciberespacio, lo que pudo ser un enorme provecho para la sociedad se transformó en una herramienta para su perjuicio.

Si bien, el acceso al ciberespacio puede generar un enorme incremento de la productividad, riqueza nacional, mayores oportunidades de generar empleos y es un catalizador del crecimiento económico y social, es también un enorme riesgo a la seguridad nacional y social. El ciberespacio no está blindado contra delincuentes, grupos organizados, empresas y Estados pueden aprovecharse de esta herramienta a costa del resto (Lewis, 2016, p. 11). Por ello, es de interés del Estado.

Más aún, la dependencia tecnológica y la facilidad de acceso a las tecnologías hacen que la probabilidad de sufrir ataques informáticos sea más alta. En ese sentido, a mayor dependencia, mayor es el impacto que podría tener un ataque a los sistemas informáticos sobre los que se sostiene un país o una organización.

Para Leiva “la ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio” (Leiva, 2015, p. 2).

Para Riordan (2019), Los problemas de ciberseguridad no son solo cuestiones técnicas sobre cómo evitar las penetraciones cibernéticas, sino principalmente políticas sobre las motivaciones de los responsables y cómo limitar esas acciones (Riordan, S. 2019, p. 9).

Por medio de la ciberseguridad se debe velar por proteger en primer lugar las infraestructuras críticas de los Estados, que son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados.

Según Lewis “las infraestructuras críticas están presentes en numerosos sectores de la economía: actividades bancarias y financieras, transporte y distribución, energía, servicios, salud, abastecimiento de alimentos, comunicaciones, administraciones públicas clave” (Lewis, 2016, p. 12).

El ciberespacio tiene más de 3 mil millones usuarios, y debe ser considerado una infraestructura crítica para el mundo. Para Miranzo, “el sector financiero, los servicios gubernamentales, el sector de la seguridad, las escuelas, y los hospitales dependen cada vez más de la interconectividad y de la red global, una vulnerabilidad del ciberespacio significa una vulnerabilidad de la sociedad moderna” (Miranzo, 2014, p. 341).

La ciberseguridad forma parte de las prioridades de la ciberdiplomacia, ya que no es posible desarrollar una estrategia de seguridad en el ciberespacio sin que los Estados se relaciones con los demás actores que componen el ciberespacio. Los Estados, en el contexto del ciberespacio, no son islas. Más bien, están íntimamente relacionados.

La tecnología y el ciberespacio han evolucionado. De igual modo, la delincuencia se sofisticado y evolucionado. Por medio del ciberespacio, los delitos ya no conocen fronteras y las víctimas pueden ser gobiernos, negocios e individuos en cualquier parte del mundo. Las organizaciones delictivas han encontrado en Internet una herramienta que facilita sus actividades y maximiza los beneficios en el menor tiempo posible.

En el ciberespacio la mayoría de los delitos no son nuevos pero, como reflejo de la realidad física, tienen su contraparte en el espacio digital. Por ese motivo, no es posible enfrentar la ciberdelincuencia si las autoridades no están lo suficientemente capacitadas con las nuevas tecnologías.

A diferencia de la realidad física en donde los Estados tienen fronteras definidas y una soberanía clara en su propio territorio, en el ciberespacio no hay fronteras. Por ello, no es suficiente la inversión en capacitación, se ha hecho necesario promover la cooperación interestatal para combatir la ciberdelincuencia.

La ciberdiplomacia, en el espacio de la ciberseguridad, incluye responsabilidades como la atracción de las mejores prácticas, el desarrollo de confianza, el reporte casos de ataque, la colaboración en la identificación de vulnerabilidades y atacantes, acuerdos de cooperación y estrategias de ciberseguridad conjunta con un enfoque integral, entre otras responsabilidades.

En ese sentido, en el 2001 el Consejo de Europa promovió la creación y firma del Convenio de Budapest sobre la Ciberdelincuencia, con el cual se busca aplicar una política penal común contra la ciberdelincuencia, aspira que los miembros del convenio adopten una legislación adecuada y se mejore la cooperación internacional.

De igual modo, en el tratado se incluye que se mejoren las capacidades en la investigación, persecución y proceso penal. Más aún, mediante la cooperación internacional, se permite compartir pruebas electrónicas de los delitos cometidos. Actualmente, más de 60 Estados de distintas partes del mundo forman parte de este convenio. El Perú se adhirió, con reservas, al Convenio de Budapest, en febrero de 2019.

Recientemente, el Convenio de Budapest se ha complementado con medio de un Protocolo adicional que convierte cualquier publicación de propaganda racista o xenófoba en un delito penal, similar a las leyes de difamación. Finalmente, en la actualidad se estudia el ciberterrorismo en el marco de la Convención.

La negociación del Convenio de Budapest, los procesos de adhesión y su cumplimiento son los ejemplos de la ciberdiplomacia en torno a la temática de la ciberdelincuencia.

Ciberdefensa

En el año 2010 se conoció el virus Stuxnet, que fue el primer virus que tuvo la capacidad de espiar y reprogramar sistemas industriales, como lo sufrió la planta nuclear en Irán. A pesar de que nunca se aclaró con total seguridad quien perpetró el ataque, existe un consenso que Stuxnet fue creado en un laboratorio por Estados Unidos e Israel para sabotear el programa nuclear de Irán, pese a que las autoridades de esas potencias no hayan confirmado esa afirmación.

Ese mismo año, el expresidente de los Estados Unidos, Barack Obama, declaró que la infraestructura digital para su país debe ser “un activo nacional estratégico”. De igual modo, William J. Lynn III, quien fuera el Subsecretario de Defensa, publicó un artículo en el que declara que para Estados Unidos el ciberespacio es un territorio de dominio igual que la tierra, mar y aire en lo relativo a la guerra. Para Lynn:

> “La seguridad del ciberespacio debe ir más allá del mundo de las redes militares, sino en los dominios de redes comerciales y que estas deberán estar subordinados al concepto de Seguridad Nacional. En esa visión, el Departamento de Defensa debe contribuir al mantener e incrementar el dominio tecnológico de Estados Unidos y mejorar el proceso de adquisiciones y mantenerse al día con la agilidad que evoluciona la industria de las Tecnologías de la Información” (Lynn, 2010, pp. 97).

Desde ese momento, otros Estados iniciaron sus propias políticas de ciberdefensa. En el tiempo, los ataques cibernéticos tienen un fuerte motivo político, por lo que las consecuencias ya no sólo se centran en pérdidas económicas, sino es el espacio en el que Estados demuestran y miden sus fuerzas.

Para Arteaga (2019), el nivel de efervescencia en el ciberespacio en los últimos años, ha generado que diversos países democráticos hayan adoptado medidas ofensivas para disuadir a otros países y grupos de realizar. Menciona que “si bien esta situación puede generar una “carrera armamentística” en el ciberespacio, no se debe dejar de lado la realidad y el posible impacto a los países” (Arteaga, 2019, p. 2).

La ciberdiplomacia en el ámbito de la ciberdefensa tiene una función de estrategia, coordinación y geopolítica. Al igual que en la realidad física, en el ciberespacio los aliados comparten capacidades, protocolos, respuestas comunes y establecen instrumentos de cooperación conjunta para prevenir ataques contra infraestructuras críticas, ciberespionaje y vigilancia masiva de ciudadanos, campañas de desinformación, difusión de programas maligno, entre otros.

2.2.2. Economía digital y tecnológica

La economía digital hace referencia a cómo el uso de las nuevas tecnologías y herramientas de información y comunicación contribuyen a la economía (Rincón, 2007, p. 183).

Para Acosta (2018), en este tipo de economía los agentes de mercado confluyen por medio de las tecnologías; por medio de la digitalización de los canales de comunicación y comercialización se agrega valor a los bienes o servicios y se generan nuevos modelos de negocios (Acosta , 2018, p. 30).

Ahora bien, no debe dejarse de lado que, si bien las empresas tienen un gran campo de acción dentro de la economía digital, las normas que regulan la aplicación de la economía

digital dentro de los países son fundamentales para el desarrollo económico de estas empresas.

La diplomacia ha tenido la histórica responsabilidad de fomentar el comercio, negociar acuerdos y promover y defender los intereses nacionales en el ámbito económico global y multilateral.

Con la aparición del ciberespacio, de la economía digital y de los nuevos avances tecnológicos, la diplomacia se convierte en una herramienta para atraer inversiones tecnológicas, promover cooperación internacional para el desarrollo de las capacidades para la innovación, adopción y transferencia de mejoras tecnológicas, e informar sobre los adelantos nueva economía digital y tecnológica, con la finalidad de defender los intereses económicos nacionales.

Ejemplo de ello, es la estrategia china que, impulsa la modernización de su economía y aspira tener una autosuficiencia tecnológica. Para ello, impulsa un crecimiento centrado en la innovación, la reducción de la dependencia de tecnologías extranjeras y el control de las cadenas de suministro clave.

Los países deben crear las condiciones para insertar su economía en la Cuarta Revolución Industrial, a partir del desarrollo de nuevos modelos de producción basados en la economía del conocimiento, el uso de la ciencia y la digitalización de la economía como una fuente de mayor productividad y de mejor calidad de vida para los ciudadanos.

A consecuencia de ello, los Ministerios de Relaciones Exteriores, tienen la misión de facilitar la vinculación de las políticas nacionales de ciencia, tecnología, conocimiento e innovación con la política exterior. Para ello, son los responsables de generar alianzas estratégicas con Estados afines, organismos y actores relevantes, tanto en la esfera bilateral, como multilateral y regional, con el propósito de fortalecer y complementar las capacidades nacionales en los ámbitos de interés.

La introducción de las tecnologías ha generado extraordinarias oportunidades. Sin embargo, estas nunca se han producido de manera uniforme entre los Estados y sociedades. Las grandes transformaciones tecnológicas han sido la causa de los liderazgos en el orden internacional. Las primeras Revoluciones Industriales colocaron a Occidente en el centro del mundo y dejaron rezagadas a Oriente.

En la segunda mitad del siglo XX se produjo una extraordinaria intensificación de los avances tecnológicos. Estos avances han generado un desigual crecimiento entre las naciones.

La expresión “brecha digital” expresa la diferencia que existe en el acceso real a la tecnología entre países y entre grupos de personas dentro de cada país(CMSI, 2008). A pesar de que se suele mencionar la necesidad de “cerrar brechas”, no se cuestiona el modelo de desarrollo actual, en donde los que producen las tecnologías son los ricos y que los que ofrecen la materia prima no alcanzan el mismo nivel de desarrollo.

Sigue existiendo una enorme brecha entre los países desarrollados y en desarrollo en materia de innovación. Los países que han apostado por desarrollar tecnología han logrado modificar su situación en el orden internacional, tal es el caso de Singapur, Corea del Sur e Israel, quienes crecen cada vez más, mientras que los que son ricos en petróleo u otras materias primas no se desarrollan tanto.

En ese sentido, el Banco Mundial considera la vía tradicional de los países en desarrollo para estimular su crecimiento, basada en la industria manufacturera, podría estar en riesgo (Lederman, 2014, p. 14).

La razón principal para que los Estados presten atención a la innovación, especialmente en los países en vías de desarrollo, es que la innovación es el motor fundamental del desarrollo económico y la principal herramienta para sobrellevar los grandes retos mundiales (Robayo, 2016, p. 2).

En ese sentido, como parte de los intereses nacionales, se debe buscar potenciar y enlazar en las cadenas de valor globales a las empresas tecnológicas nacionales, promover la capacitación en temas digitales a la población.

Si los Estados diseñaran mejores políticas para la adquisición y explotación de esos conocimientos efectivamente, pueden mejorar enormemente su crecimiento y bienestar y su posición en el mundo. Para la CEPAL (2016, p. 105) el modelo actual de desarrollo es insostenible y la región requiere un cambio estructural progresivo si efectivamente quiere alcanzar el cumplimiento de los Objetivos de Desarrollo Sostenible al 2030.

Son funciones de la ciberdiplomacia el negociar acuerdos que incluyan la economía digital, regular promover la innovación y el cierre de brechas digitales, asegurar el crecimiento de las empresas nacionales y la atracción de las nuevas tecnologías. Estas actividades no

solo tienen la función de generar bienestar social a la población, sino que son determinantes para potenciar el prestigio de un país, tiene un rol geopolítico.

En la actualidad, en el contexto de la Cuarta Revolución Industrial, se están desarrollando nuevas tecnologías que serán la base de una nueva economía digital y que revolucionarán el mundo, el empleo y el peso relativo de los Estados y organizaciones. A continuación se mostrarán aquellas que por su impacto deben ser prioritarias para el análisis la ciberdiplomacia actual y futura.

La 5G

La quinta generación de redes móviles, conocida como 5G (IMT-2020), es la última generación de estándares de redes desarrollada por la Unión Internacional de Telecomunicaciones (ITU). Esta generación está compuesta por diversos elementos y sistemas que soportan los innumerables beneficios que se pueden realizar a través de ella (ITU, 2017, p. 5).

La 5G actuará como "la base de la próxima generación de infraestructura, incluidos miles de millones de dispositivos conectados a internet que alimentan ciudades inteligentes, nuevas aplicaciones de realidad virtual y vehículos autónomos"(ITU, 2017, p. 7). Asimismo, esta tecnología permitirá transformaciones socioeconómicas en ámbitos como la producción, desarrollo sostenible y bienestar de la población.

La 5G permitirá, entre otros, una mayor agilidad para actividades como mensajería de textos, acceso a internet, video llamadas en alta definición, videos en tercera dimensión y acceso a dispositivos de cosas inteligentes (internet de las cosas). Visto desde el lado económico, esta tecnología servirá como plataforma para el desarrollo de negocios y la evolución de los existentes como los que brindan grandes empresas tecnológicas otros. Asimismo, esta tecnología revolucionará la forma de hacer negocios desde sectores como la agricultura hasta la manufactura (ITU, 2017, p. 11).

En la actualidad la empresa Huawei, de origen chino, es el principal fabricante de tecnología 5G en el mundo (Iglesias, 2020), en el marco de la gran tensión entre Estados Unidos y China, esta tecnología en concreto es la piedra angular para el despliegue de tecnologías y la reconfiguración de las reglas e instituciones económicas bajo las cuales se rigen los actores internacionales actualmente.

Inteligencia Artificial

John McCarthy definió la Inteligencia Artificial como "la ciencia y la ingeniería de la fabricación de máquinas inteligentes, especialmente programas informáticos inteligentes"

(citado por Garcia Serrano, 2017, p. 6). En términos básicos, la IA se refiere a la actividad mediante el cual las computadoras procesan grandes volúmenes de datos utilizando algoritmos altamente sofisticados para simular el razonamiento o el comportamiento.

Inteligencia artificial implica el diseño y uso de programas que replican las actividades realizadas por la inteligencia humana. Los elementos más importantes que se replican son el razonamiento, el aprendizaje, el auto corregimiento y el aprendizaje por parte de las máquinas. Esta tecnología tiene una aplicación en actividades como reconocimiento de voz, identificación de imágenes, procesamiento de lenguaje, robótica, entre otros (Romero et al., 2007, p. 14)

Los alcances de esta tecnología son asombrosos, las computadoras “aprenderán” por su cuenta a partir de reconocer patrones en la data que reciben; además, podrán comunicarse, tendrán reconocimiento fácil y otras habilidades semejantes a la inteligencia humana (Romero et al., 2007, p. 16).

La inteligencia artificial permitirá incrementar la productividad y generar crecimiento económico para los países desarrollo. De igual manera, debido a la data que maneja, puede empoderar aún más a las grandes empresas tecnológicas.

La importancia de esta tecnología es tan relevante que, se ha vuelto central en los debates internacionales, indispensable en políticas públicas de países desarrollados e incluso Emiratos Árabes Unidos ha creado un Ministerio de Inteligencia Artificial, para ponerse a la vanguardia de la tecnología, considerando que, más de la mitad de los puestos de trabajo tecnológicos van a requerir de conocimientos en este campo (Larrañaga, 2019).

En junio del 2020, los gobiernos de Alemania, Australia, Canadá, Corea, Eslovenia, Estados Unidos, Francia, India, Italia, Japón, Reino Unido, México, Nueva Zelandia, Singapur y la Unión Europea, realizaron una declaración conjunta con la que crearon la Alianza Global sobre la Inteligencia Artificial (AGIA).

Por medio de ella se comprometieron a apoyar el desarrollo, así como el uso responsable y centrado en los seres humanos, de la Inteligencia Artificial (IA), con base en los derechos humanos, las libertades fundamentales y nuestros valores democráticos comunes, como se presentan en la Recomendación de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre la IA.

En colaboración con socios y organizaciones internacionales, la AGIA reúne expertos líderes de la industria, la sociedad civil, los gobiernos y la academia para en cuatro Grupos

de Trabajo temáticos: 1) el uso responsable de la IA; 2) la Gobernanza de los Datos; 3) el Futuro del Trabajo; y 4) la Innovación y la distribución.

Computación cuántica

La computación cuántica se basa en el desarrollo de algoritmos que pueden ser aplicados para los problemas de aprendizaje automático. Asimismo, puede ser utilizado para "transcribir conversaciones, identificar objetos en} imágenes, encontrar soluciones a problemas en medicina o química, identificar tratamientos óptimos a un paciente o estudiar las posibles estructuras de moléculas complejas" (Kleinman Ruiz, 2019, p. 23).

Esta industria se limita por 29 ahora a grandes empresas como IMB, Microsoft y Google, quienes se encuentran a la vanguardia. Sin embargo, existe un crecimiento de empresas de origen chino en esta industria.

Internet de las cosas

Internet de las Cosas (IoT) describe un sistema en el cual los objetos físicos están conectados a Internet y son controlados por ese medio (Fedele & Fedele, 2011, p. 12).

Esta tecnología permite ampliar la interconectividad de Internet de una manera, se espera que en el futuro el número de dispositivos inteligentes o "cosas" conectados a la IoT supere varias veces la población mundial. (Kurbalija, 2016, p. 175).

Los riesgos que se observan asociados a sistemas IoT van desde la mala configuración de éste en conjunto con sus servicios, lo que amenaza la seguridad, privacidad y seguridad de las personas; y por otra parte los dispositivos conectados a un sistema IoT que posean una configuración débil, pueden formar parte de ataques cibernéticos a gran escala (Kurbalija, 2016, p. 175).

Sería muy posible que los dispositivos móviles sean intervenidos con tal de registrar información a través del micrófono o la cámara. La información ahí conseguida es poder (Sepúlveda, 2019).

Big Data

Por medio de la tecnología Big Data, se puede administrar la gran cantidad de datos provenientes de diferentes fuentes y que se generan conclusiones con gran rapidez(Hernández-Leal et al., 2017, p. 2)

Lo interesante de esta tecnología es que, puede relacionar datos y generar información que permite a los poseedores segmentar de una manera muy precisa a los usuarios (Hernández-Leal et al., 2017, p. 3).

Para Oliveros y López, “el acceso a la Big data se convertirá en el recurso económico-político más valioso en el futuro, ya que aquella empresa o país que acceda a información sobre producción y consumo global, tendrá una ventaja competitiva en el marco de la Cuarta Revolución Industrial” (Ontiveros & López, 2017, p. 24).

2.2.3. La Gobernanza Global Digital

La Gobernanza Global Digital es una de las temáticas más complejas e importantes de la diplomacia en el ámbito del ciberespacio. Aunque el ciberespacio sigue siendo anárquico, existe un debate abierto sobre cómo el derecho internacional es aplicable en ese ámbito.

A diferencia de la realidad física, el ciberespacio no puede delimitarse y las fronteras, como las conocemos, son inexistentes. Por otra parte, a diferencia de la realidad física, el ciberespacio se encuentra inacabado, por lo que está en permanente cambio y evolución. Por ese motivo, las regulaciones serán siempre imperfectas.

Para el Grupo de Trabajo sobre Gobernanza de Internet de las Naciones Unidas, esta gobernanza se refiere al conjunto de principios, normas, reglas, procesos de toma de decisión y actividades que, implementados y aplicados de forma coordinada por gobiernos, sector privado, sociedad civil y comunidad técnica, definen la evolución y el uso (WGIG, 2005)

Por otro lado, la soberanía, entendida como absoluta, perpetua, indivisible, inalienable e imprescriptible y como parte esencial del Estado (Bavaresco, A. 2003, p. 60), entra en un escenario de incertidumbre y desafío, pues los Estados ya no ejercen el uso exclusivo del poder y no se ha podido determinar los aspectos que están bajo su dominio de manera exclusiva.

Para Lessig (2002, p. 175): “el ciberespacio es inevitable y, no obstante, el ciberespacio no puede ser regulado, ninguna nación puede vivir sin él, sin embargo, ninguna nación capaz de controlar completamente el comportamiento en él”.

El ciberespacio necesita de una infraestructura que abarca, los cables, las telecomunicaciones y se vincula con el soporte físico. De igual modo, existe un área técnica, que incluye los nombres de dominio y números de IP, los cuales son instrumentos sobre los cuales se transportan los contenidos, servicios y bienes digitales que están en la red. La gobernanza de esta área del Internet estaría a cargo de los técnicos especializados en ello, mientras que los temas de los usos

Al tener la infraestructura un soporte físico ubicado en el territorio nacional, la construcción y regulación de la misma depende exclusivamente de cada Estado.

Esta gobernanza se circunscribe también a un área jurídico-política que la regula, por medio de legislación nacional o por acuerdos internacionales. Este tipo de normativa ha buscado regular los contenidos, servicios y bienes digitales. La ciberdiplomacia encuentra un rol privilegiado al momento de regular esta área.

Es en este punto en el que la diplomacia en el ámbito del ciberespacio tiene un rol protagónico ya que existe una diversidad de posturas en torno en torno a la regulación que debía realizarse, pues como lo mencionan Watts y Richard:

> "los Estados consideran al ciberespacio como un espacio fundamental para ejercer influencia, muchas veces son los grupos que rechazan los gobiernos quienes realizan ciberataques, pero esta práctica también ha sido usada como política estatal aunque resulta difícil atribuir responsabilidad a ese hecho" (2018, p. 809).

En el 2005, durante la II Cumbre Mundial sobre la Sociedad de la Información (CMSI) en Túnez, organizado por la Unión Internacional de Telecomunicaciones, de la Organización de las Naciones Unidas (ONU), se definió que:

> "La gobernanza de Internet es el desarrollo y la aplicación por los gobiernos, el sector privado y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y la utilización de Internet"(WGIG, 2005, p. 4).

Con la definición antes mencionada, se les da un rol protagónico a otros agentes distintos del Estado.

Después de la Cumbre en Túnez se creó el Foro para la Gobernanza de Internet (FGI), el cual cuenta con un comité multiestamentario, que incluye representantes de los gobiernos, el sector privado y la sociedad civil. Este, es un espacio privilegiado para la actividad de la diplomacia, ya que muchas veces los intereses de los Estados en el ciberespacio se contraponen.

Una importante controversia en este tipo de gobernanza se dio por la Corporación de Internet para la Asignación de Nombres y Números (ICANN) una organización única en la gobernanza global y un típico producto del período de unipolaridad dominada por los Estados Unidos (Riordan, S. 2019, p.38).

ICANN es una corporación no gubernamental sin fines de lucro creada en California en 1998 que fue contratada por el Departamento de Comercio de los Estados Unidos para administrar nombres y direcciones de Internet.

La naturaleza no gubernamental e impulsada por expertos de ICANN refleja la cultura de la tecnología de la información. Sin embargo, genera un enorme rechazo para los gobiernos que creen que una red mundial como Internet debería tener de alguna forma de regulación gubernamental.

La reciente polémica en la decisión de ICANN sobre el control del domino ".amazon", que involucra a la corporación AMAZON y los países de la OTCA, incluido el Perú, es un ejemplo de cómo este tipo de gobernanza permanece latente y es que subsiste la necesidad de ejercer la defensa de los intereses nacionales en ese ámbito por medio de la ciberdiplomacia.

En la realidad física hubo luchas por garantizar las libertades individuales como derecho fundamental. El ciberespacio es un área que genera controversias sobre la aplicación de la libertad. La libertad de expresión individual, los derechos de autor, el acceso a la información pública, el respeto a la vida privada, el respeto a la confidencialidad en las comunicaciones y la neutralidad de la red son algunos ejemplos de temas recurrentes en torno a la libertad de Internet.

Por otra parte, por motivos de seguridad o intereses económicos o políticos, los Estados suelen tener posiciones antagónicas en torno a la libertad de Internet. Por medio de la diplomacia, los Estados pueden hacer valer su posición en las múltiples discusiones sobre este tema.

La geopolítica actual puede verse reflejada en las posiciones sobre la gobernanza del ciberespacio entre las naciones que promueven la libertad y los que promueven una mayor regulación por parte de los Estados.

Por un lado, Estados Unidos y sus aliados, buscan mantener el ciberespacio tal como es, global y en gran parte libre de interferencia del gobierno. En la medida en que se regule, especialmente a nivel físico y lógico, abogan por un modelo de múltiples partes interesadas, que incluya a los estados, el sector privado, la sociedad civil, las organizaciones gubernamentales internacionales, la comunidad técnica y los académicos.

Por otra parte, quienes promueven un mayor dominio del Estado sobre el ciberespacio, liderados por Rusia y China, creen que la gobernanza y la regulación de Internet deberían

incorporarse esencialmente a las organizaciones internacionales gubernamentales existentes.

Como se observa, la regulación del ciberespacio se torna particularmente compleja. Para Mateos (2015, p. 3)

> "algunos tratadistas creen que el ciberespacio debe ser considerado como un espacio que sirve para el tránsito de cualquier tipo de bien o servicio, y que no está bajo la soberanía directa de ningún Estado (Global Commons) y es candidato a unirse a los espacios que ya son considerados como tales: las aguas internacionales, el espacio aéreo y el espacio exterior".

No obstante, Reguera Sánchez (2015, p. 11) explica que

> "una gran diferencia entre la regulación del ciberespacio y el caso de las aguas internacionales es que en esta última siempre había imperado una costumbre internacional de libre navegación y que esta se plasmó en un tratado internacional en 1958 y sus posteriores reformas hasta la Convención del Derecho del Mar en 1982".

Para Riordan (2019), a pesar que el derecho internacional existente es aplicable en el ciberespacio, este ámbito sigue siendo anárquico. La regulación en el ciberespacio es un asunto que está mucho más allá del alcance de los ingenieros y necesitan más debate y decisión políticos. Para este autor, la ciberdiplomacia tendría margen para operar principalmente en las capas de datos o sociales (Riordan, 2019, p. 33).

Siguen vigentes muchas discusiones acerca de este tipo de gobernanza, las posturas nacionales deben dialogar en los foros y espacios apropiados, por medio de la ciberdiplomacia.

3. Las grandes empresas tecnológicas y el ciberespacio

La naturaleza del ciberespacio y las nuevas tecnologías ha permitido la difusión de actores estatales y no estatales. A pesar que los actores más importantes del ciberespacio siguen siendo los Estados (Lazar, 2013), se debe considerar que las barreras de entrada al dominio cibernético son tan bajas que los actores no estatales y los Estados que en el pasado no podían competir por el poder internacional pueden desempeñar papeles importantes a bajos niveles de costo.

Ante este panorama, son las grandes empresas tecnológicas las que parecen haber alcanzado una gran capacidad de influir en la sociedad, en la Gobernanza Global Digital, en la ciberseguridad y en el desarrollo económico. Por ello, han alcanzado un rol determinante como actor en el orden internacional.

No existe una definición universal para referirse a las empresas tecnológicas. Sin embargo, el estudio de Zakrzewska-Bielawska (2010, p. 97) sobre el concepto de empresas tecnológicas permite caracterizar a este particular tipo organización. Según esta autora, las características clave que las empresas tecnológicas suelen (1) ser fuente de nuevos conocimientos, invenciones e innovaciones, (2) están basadas en la recopilación y procesamiento del conocimiento, (3) utiliza las tecnologías de la información, (4) los usuarios suelen proporcionar información clave, (5) existe una estrecha asociación con la comunidad científica y técnica, (6) disfrutan una alta flexibilidad de las estructuras organizativas, (7) utilización de potencial de trabajo en equipo, (8) permiten la independencia y autonomía del personal altamente capacitado, (9) tienen una alta inversión en I + D (10) poseen una alta inversión en proyectos de alto riesgo (Zakrzewska-Bielawska, 2010, p. 97).

Dentro de este sector existen algunas empresas que por su nivel de desarrollo han logrado una enorme influencia, no solamente se han convertido en las más grandes del mundo, considerando que 6 de las 10 empresas más grandes son tecnológicas (Forbes, 2019), sino que por la naturaleza de sus negocios y emprendimientos, pueden afectar el dominio del ciberespacio. A esas empresas se las ha denominado “grandes empresas tecnológicas”.

Para Kissinger (2014, p. 184) “Las corporaciones que agregan y monitorean los datos intercambiados por estos individuos tienen un poder de influencia y vigilancia que excede al de muchos estados contemporáneos e incluso al de poderes más tradicionales”.

Más aún, por su ámbito de acción transnacional, tienen la capacidad de socavar la concepción de territorialidad de los estados. Por ejemplo, cualquier cambio que alguna de estas empresas realice en su configuración de privacidad afecta a más de mil millones de personas en todo el mundo. Estas decisiones suelen tomarse en Silicon Valley, sin la participación del gobierno de Turquía o Australia, a pesar de que afectan a decenas de millones de ciudadanos turcos e australianos.

En la Tabla 1 se muestran algunas de estas grandes empresas tecnológicas, y se considera que su giro de negocio, tamaño y la nueva tecnología que dominan, han logrado consolidarse como actores de primer orden en el ciberespacio.

Tabla 1
Nuevos actores del orden internacional: empresas tecnológicas más importantes

Empresas	Sede Central	5G	Inteligencia Artificial	Computación Cuántica	Internet de las Cosas	Big Data	Puesto en el Ranking Mundial
IBM	Nueva York, EEUU			X	X		76
Google	California, EEUU		X	X	X	X	5
Microsoft	Washington, EEUU		X	X	X	X	3
Huawei	Shenzhen, China	X				X	9
Nokia	Espoo, Finlandia y California, EEUU	X	X	X			-
Samsung	Seúl, Corea del Sur	X		X			17
Intel	California, EEUU	X		X	X		20
Apple	California, EEUU		X			X	2
Facebook	California, EEUU		X			X	6
Amazon	Washington, EEUU		X		X	X	4
Nvidia	California, EEUU		X			X	47
Cisco	California, EEUU		X		X		41
Alibaba	Hangzhou, China		X			X	7

Elaboración propia (2020)

Como evidencia el cuadro, las empresas tecnológicas que tienen o tendrán un fuerte peso en el gobierno del ciberespacio se encuentran en países desarrollados, y la mayoría de estas se localiza en la región de Silicon Valley, conocido por ser el centro líder para la innovación y desarrollo de alta tecnología en el mundo.

Dentro de las empresas tecnológicas, sobresalen las “Cuatro Grandes”, también llamadas “GAFA”: Google, Amazon, Facebook y Apple, quienes con un valor conjunto de US$ 5.6

trillones, representan casi una quinta parte del valor del índice S&P 500 de acciones estadounidenses (Gispert, 2020).

En China existen también grandes empresas tecnológicas que pueden rivalizar con las estadounidenses, "BATX" es el acrónimo de cuatro empresas tecnológicas chinas Baidu, Alibaba, Tencent, Xiaomi (Constanza, 2017).

Por otro lado, han aparecido empresas denominadas “unicornios tecnológicos”, que se refieren a empresas aún pequeñas, si se les compara con las grandes, pero que alcanzan un valor de mil millones de dólares en alguna de las etapas de su proceso levantamiento de capital (Castillo, 2017). Lo interesante de este tipo de empresas es que tienen una enorme capacidad de adaptación a los cambios y pueden dejar obsoletos a las empresas tecnológicas más grandes, lo que se conoce como “tecnología disruptiva” (Castillo, 2017).

El poder de las grandes empresas tecnológicas radica en su capacidad de influir en la ciberseguridad, en sus posibilidades de influenciar el ciberespacio o en ser grandes inversionistas. Para Tom Symons, quien es miembro del grupo de expertos Nesta, “estas plataformas se están preparando para reemplazar funciones enteras del gobierno, si las autoridades no están preparadas, es posible que la tecnología deje a los Estados sin mucho campo de acción”(citado por Champetier de Ribes, 2018, p. 131). Más aún, estas empresas han pasado de ser compañías con intereses comerciales a convertirse en actores de facto en la política exterior.

3.1. Las relaciones entre los Estados las grandes empresas tecnológicas

En las relaciones internacionales se estudia el trato interestatal desde la perspectiva del conflicto y la cooperación. Mientras que la teoría realista enfatiza el conflicto, teoría liberal acentúa la cooperación. Sin embargo, las demás teorías también son sumamente útiles para analizar las relaciones entre los actores internacionales.

En un modo semejante, se podría analizar las relaciones de conflicto y cooperación entre los Estados y las grandes empresas tecnológicas en el ciberespacio y en la realidad física. Para hacer esto, va a ser necesario utilizar la teoría de relaciones internacionales que más convenga, según sea la temática de análisis.

Por un lado, si se analiza la ciberseguridad, lo más probable es la mirada realista tenga una perspectiva de conflicto sumamente valiosa. Mientras que, la teoría liberal podría encontrar los espacios de cooperación entre Estados y empresas tecnológicas. Por otro lado, al analizar las nuevas tecnologías como herramienta para el desarrollo, los realistas se concentrarían en las ganancias relativas de los desarrollo, y los liberales en la ganancias absoluta. Mientras que los radicales enfatizarían la tecnología como una técnica de dominación y represión que surge del desarrollo económico desigual inherente al sistema capitalista.

Las grandes empresas tecnológicas tienen un alcance global y se relacionan con diversos actores. En la mayoría de oportunidades las relaciones versan particularmente en torno a los negocios. No obstante, como se comentó anteriormente, estas empresas tienen fuertes intereses en diversos temas que los colocan como actores poderosos en el ciberespacio.

Las relaciones "bilaterales" de las grandes empresas tecnológicas

La principal relación de las grandes empresas tecnológicas es con los Estados Unidos. Por un lado, en la mayoría de casos es el país de origen de las empresas tecnológicas y es el lugar en el que se encuentra su principal mercado. De igual manera, la relación que tiene con algunos países de Europa y con la Unión Europea se ha visto incrementada por los intereses que las empresas tienen en esa región y por la regulación europea en torno a protección de datos, seguridad y reglas sobre innovación tecnológica.

En el caso chino, empresas como Huawei son acusadas, por Estados Unidos, de tener profundos vínculos con el Partido Comunista Chino y con los militares de ese país, por lo que no tendrían la "independencia" que sí gozan las empresas tecnológicas occidentales. Esta situación se torna complejo ante las medidas que viene adoptando China, que podrían encaminarla a establecerse como un futuro hegemón del sistema internacional (Sandoval, D. 2019, p. 50).

De igual manera, China mantiene un control estricto de la tecnología y del acceso a los medios de comunicación de empresas de origen occidental, entre las que destacan Facebook y Google. De igual manera, potencia el uso de redes sociales y navegadores locales como Wechat de la empresa Tencent y el navegador Baidu (Reuters, 2020).

El rol de las grandes empresas tecnológicas tiene un valor fundamental en el proceso de transición del poder a Asia, mencionado al inicio de este capítulo y la competencia hegemónica entre Estados Unidos y China que se desarrollan en gran parte en el campo tecnológico.

En el trato entre los Estados y las grandes empresas tecnológicas se evidencian relaciones de conflicto o cooperación. Un acontecimiento sumamente interesante sucedió en mayo de 2019, cuando el fundador y CEO de Facebook, Mark Zuckerberg, llegó al Palacio del Elíseo en París para reunirse con el presidente francés, Emmanuel Macron. Las imágenes que se dieron a conocer a la prensa se parecían a las de una visita tradicional de trabajo del jefe de Estado, el protocolo fue muy similar; en la reunión se debatió sobre estrategias que ayuden a limitar la "viralidad" de las publicaciones con contenido de odio y violencia (Suárez, 2019).

Tras la reunión entre Zuckerberg y Macron se publicó un informe realizado entre el país galo y la red social en el que se aboga por la creación de una autoridad administrativa independiente en cada país que vele por la transparencia en la manera de regular las publicaciones dentro de las redes (Suárez, 2019).

Para Morozov las firmas de tecnología de Silicon Valley no se ven de ningún modo inferiores o subordinadas, y que porfían por dictar sus propias reglas y se niegan a acatar leyes y normas que juzgan inadecuadas o inútiles (Morozov 2017, p. 21).

Otra situación sugestiva es la reciente creación de la “embajada tecnológica” de Dinamarca en Silicon Valley en agosto del 2017. El gobierno danés después de reconocer que la influencia política y el impacto económico en la vida cotidiana de su población son mayor a la mayoría de países donde tienen embajadas más tradicionales, decidió nombrar a Casper Klynge, un embajador de carrera como representante ante las empresas tecnológicas.

No obstante, en una reciente entrevista ante The New York Times (2019), el embajador Klynge confesó que le tomó nueve meses sentarse con un alto ejecutivo en una de las compañías tecnológicas más grandes y que la receptividad para dialogar temas no ha sido la esperada. Sin embargo, el embajador Klynge considera que algunas empresas de tecnología han empezado a comprender mejor su trabajo y que el diálogo regular con Brad Smith, presidente de Microsoft le ha dado influencia a Dinamarca en temas de ciberseguridad y gobierno de Internet (Satariano, 2019). Sobre esta iniciativa se profundizará en el siguiente capítulo.

En mayo del 2019, el presidente colombiano, Iván Duque, realizó una gira por Estados Unidos para reunirse con altos directivos de las grandes empresas tecnológicas con la intención de buscar inversión en tecnología e innovación en su país; la gira incluyó a

empresas como Apple, Google, Amazon y Microsoft en California y Washington (Portafolio, 2019).

Dentro de los objetivos a concretar, el presidente buscó la participación de las grandes empresas tecnológicas en el Centro para la Cuarta Revolución Industrial de Medellín. Cabe precisar que este Centro se desarrolló en cooperación con el Foro Económico Mundial, habiéndose creado antes sucursales en San Francisco (EEUU), Tokio (Japón), Beijing (China) y Mumbai (India)(WEF, 2020). Este Centro tiene un valor para Colombia, no sólo tecnológico, sino también estratégico al ser el primer centro en un país de habla hispana y el primero en América Latina.

De igual modo, el presidente ha motivado el apoyo en la educación digital en Colombia, ha propuesto una cartera de inversiones en proyectos de conectividad en lugares remotos, ha buscado establecer convenios de cooperación en ciberseguridad, e incluso propuso inversiones en la industria de videojuegos (Portafolio, 2019).

En 2019, el Presidente Piñera realizó visitas a China y Corea del Sur, con una agenda cargada en el ámbito de cooperación tecnológica, que incluyó acuerdos de cooperación tecnológica y acuerdos con empresas innovadoras para atraer y desarrollar cadenas de valor en áreas como electromovilidad, inteligencia artificial, energías limpias y tecnología 5G (Vanguardia, 2019).

En los años recientes, la relación entre los Estados y las grandes empresas tecnológicas se han visto caracterizadas por mucha desconfianza y conflicto. A partir de los escándalos de filtración de información y por la capacidad que tienen las empresas de usar datos privados de los usuarios, las empresas han recibido innumerables juicios y multas en diversas partes del mundo.

Sin embargo, se han visto en el centro de la competencia entre Estados Unidos y China por la hegemonía tecnológica y han empezado a ser consideradas como importantes aliados de occidente en contra de las aspiraciones orientales (Mayer-Schonberger & Ramge, 2018).

El enfrentamiento entre Estados Unidos y China también tiene impacto directo sobre las empresas tecnológicas. Por ejemplo, las sanciones contra empresas chinas -como Huawei- prohíbe a empresas estadounidenses vender insumos tecnológicos necesarios para las empresas chinas; también, impide a las primeras de abastecerse de productos tecnológicos chinos (BBC, 2019).

En el campo político, Estados Unidos se lanzó desde el año 2018 en una campaña por Europa (aunque también en América Latina) para persuadir a líderes de estas regiones a no consumir productos chinos de Huawei, aduciendo razones de seguridad (Álvarez, 2018).

Las relaciones "multilaterales" de las grandes empresas tecnológicas

En la actualidad, las grandes empresas tecnológicas han encontrado espacios de relacionamiento multilateral. Un ejemplo interesante se da en el Foro Económico Mundial (FEM). El cual es un organismo internacional privado y sin ánimo de lucro, el cual trata de promover la cooperación público-privada. Con sede en Ginebra (Suiza), este foro trata de fomentar una cooperación entre los actores públicos y privados, y busca integrar a los principales líderes económicos, políticos y empresariales del mundo.

En este espacio, financiado por los organismos privados, las grandes empresas tecnológicas por su tamaño e importancia participan como socios estratégicos. En los últimos cinco años, las nuevas tecnologías en la perspectiva de la Cuarta Revolución Industrial han constituido el tema central de la Asamblea Anual del Foro. Por ello, es evidente que rol de las grandes empresas tecnológicas en este espacio es determinante.

Otro ejemplo valioso de relacionamiento multilateral es el Foro para la Gobernanza de Internet (FGI), mencionado anteriormente. Este Foro incluye representantes de los gobiernos, el sector privado y la sociedad civil, y es un espacio privilegiado para que las grandes empresas tecnológicas puedan relacionarse con diversos actores en torno al gobierno del Internet. En los últimos años, la temática ha versado en torno al desarrollo humano sostenible económico y social, la libertad y la ciberseguridad. Temas de particular interés para las grandes empresas tecnológicas.

En enero de 2020, Microsoft anunció la creación de una delegación permanente ante las Naciones Unidas en Nueva York con el fin de hacer avanzar los Objetivos de Desarrollo Sostenible a través de la tecnología y su impacto en la seguridad, desarrollo, medio ambiente y los asuntos humanitarios (Microsoft Corporate Blogs, 2020).

En la Conferencia de Seguridad de Múnich este año, se invitó a representantes de grandes empresas tecnológicas para ser ponentes en diversas sesiones sobre las relaciones transatlánticas o medidas para la resolución de conflictos. En la conferencia sobre política de seguridad internacional el presidente de Facebook, Mark Zuckerberg, planteó la necesidad de mejorar el sistema de gobernanza de Internet (Jorge-Ricart, 2020).

3.2. Los intereses de las grandes empresas de tecnología en el ciberespacio

Así como los Estados buscan su supervivencia y el desarrollo de su población, las empresas tienen el propósito de maximizar sus utilidades y de ser sostenibles en el tiempo. Las grandes empresas tecnológicas tienen claros sus intereses. En poco más de una década, solo las cinco empresas más grandes han invertido más de 580 millones de dólares en empresas de gestión de intereses (Lobby) en el Congreso de los Estados Unidos y solo en el 2019 invirtieron más de 15 millones de euros por ese mismo concepto ante la Comisión Europea, configurándose en uno de los sectores que más invierten en este servicio (Dellinger, 2019).

Si bien el principal tema de interés de estas empresas se relaciona con los impuestos y el acceso a mercados, existen otros temas vinculados a las empresas tecnológicas que son relevantes para el ejercicio de la diplomacia, como protección y promoción de intereses del Estado, en el ciberespacio (Dellinger, 2019). En este apartado se expondrán esos intereses.

Privacidad de la información

Las discusiones en torno al uso de la información privada solía centrarse en la capacidad que tenían estas empresas por segmentar a la población con la finalidad de ofrecerles publicidad personalizada. No fue hasta el escándalo de Cambridge Analytica, en el que se evidenció a nivel mundial del impacto social, económico, político y ético que podía tener la información privada en el ciberespacio en la realidad física(BBC, 2018a).

En la era digital la violación de datos-“data breach” consiste en la exposición intencional o involuntaria de información confidencial a terceras partes sin la debida autorización (Cheng et al., 2017). Esta acción puede afectar a personas naturales, a organizaciones y a gobiernos. Las empresas de tecnología se encuentran en una comprometida situación, pues pueden resultar una las víctimas de los ataques o los proveedores remunerados de estas filtraciones.

Para las empresas de tecnología la regulación sobre la privacidad de la información les afecta directamente su imagen, su giro de negocio e incluso su propia sobrevivencia. Ejemplo de ello es lo ocurrido muy recientemente con Facebook con el “Add Boycott”, más de 400 empresas están dejando de anunciar en la plataforma, por reclamos de activistas que acusan una falta de compromiso de la empresa en detener la proliferación de noticias falsas y tendenciosas, así como de grupos que incrementan la tensión social por motivos raciales, entre otros (The New York Times, 2020).

No existe una normativa mundial en torno a la privacidad de la información. Por ejemplo, solo en Estados Unidos no existe una única legislación de protección de datos. Más bien, coexisten cientos de leyes promulgadas a nivel federal y estatal al respecto de la protección de los datos personales(Redondo, 2019).

Por otro lado, en Europa se ha elaborado el Reglamento General de Protección de Datos (RGPD) que regula la protección y tratamiento de datos personales. Por medio de estas leyes, en distintos lados del mundo, las grandes empresas tecnológicas han sido demandadas, procesadas y multadas con sumas millonarias (BBC, 2018b).

Para Castells (2017, p. 74), la vigilancia electrónica y la invasión informática de la privacidad se ejercen, en lo esencial, por dos grandes grupos de actores: el Estado y las empresas de comunicación digital.

Ciberseguridad

Para las empresas de tecnología, la ciberseguridad se ha vuelto un asunto muy importante. En los últimos años ha habido acercamientos con el sector estatal para afrontar los riesgos a la seguridad. De igual modo, las empresas de tecnología han iniciado alianzas entre ellas a fin de proteger su negocio, recuperar una buena imagen ante el público y las autoridades y políticos.

Para Dobrygowski (2019), existen dos tipos de alianzas, las operativas y las normativas. Por un lado, las alianzas operativas buscan transparentar los ataques y amenazas recibidas y articular prácticas de seguridad, así como la adopción de nuevas tecnologías. Resaltan en particular las alianzas “Cyber Threat Alliance”, “the Global Cyber Alliance” y “Trusted Computing Group”. Por otro lado, las alianzas operativas hacen llamados a la paz digital, buscan el apoyo de los gobiernos para limitar el uso de sistemas digitales y redes en contra de los ciudadanos, instituciones y otros Estados. Resaltan las alianzas “The Cybersecurity Tech Accord” y “The Charter of Trust” (Dobrygowski, 2019)

Algunas grandes empresas tecnológicas han adoptan un enfoque diplomático para la ciberseguridad o la gobernanza de Internet. Por ejemplo, Google, Facebook y Microsoft, en el 2016 formaron el Foro Global de Internet para Contrarrestar el Terrorismo con el fin de combatir el contenido extremista y terrorista en las redes sociales(Romm, 2016).

Finalmente, el "Llamado de París para la confianza y la seguridad en el ciberespacio", propuesto por el presidente de Francia, Emmanuel Macron, que consiste en una declaración simbólica que busca mejorar las prácticas de seguridad cibernética y los estándares internacionales para Internet (Ministerio de Relaciones Exteriores, 2019).

A la fecha más de 90 Estados, incluida toda la Unión Europea, se han unido al llamado, junto con más de 400 empresas y 150 organizaciones internacionales y de la sociedad civil (Francia Diplomacia, 2018).

La lógica detrás de estas alianzas es que los ataques cibernéticos son cada vez más comunes y agresivos y que incluso las grandes empresas se han visto afectadas.

Contenidos libres y excepciones al derecho de autor

El desarrollo de las nuevas tecnologías ha generado efectos en los derechos de autor. Por un lado, el ciberespacio se ha vuelto la infraestructura a través de la cual se infringen a una escala sin precedentes. Por otro lado, por su alcance geográfico y la diversidad normativa de los Estados, ejercer control y sanciones resulta sumamente complicado. Finalmente, la innovación tecnológica ha generado que el consumidor sea también un productor de contenido, lo que genera que se incrementen las obras protegidas por derechos de autor.

En el año 2011, la Cámara de Representantes de los Estados Unidos presentó un proyecto de ley conocida como Stop Online Piracy Act o Ley SOPA. Por medio de este proyecto de ley se buscaba ampliar las capacidades del gobierno estadounidense para combatir el tráfico de contenidos con derechos de autor y bienes falsificados a través de Internet; el proyecto buscaba que se pudiera bloquear la publicidad y las redes de pago de los sitios infractores, así como regular a los proveedores de Internet (Arcos, 2012).

Este proyecto de ley hubiera afectado directamente los intereses de miles de empresas que usan el ciberespacio. Las empresas hicieron defender su postura mediante la gestión de intereses y la comunicación, argumentando que afectaba la libertad de expresión, de empresa, a los usuarios y la privacidad; finalmente el proyecto de ley se detuvo fue congelado (Arcos, 2012). Sin embargo, todavía existen promotores de este tipo de regulación.

Neutralidad en la red

Se entiende por neutralidad en la red como “el principio por el cual los proveedores de servicios de Internet y los gobiernos que la regulan deben tratar a todo tráfico de datos que transita por la red de igual forma indiscriminadamente” (Easley et al., 2018, p. 1). Para algunos, el giro de negocio de las empresas tecnológicas, como proveedores de internet, atenta directamente con la neutralidad de la red, y en los últimos años la intensidad de la legislación sobre el tema en Estados Unidos ha variado significativamente, dependiendo de quién está en el gobierno.

El reclamo a los proveedores de internet es que utilizan su posición de dominio en los mercados de búsqueda para favorecer sus propios productos y desvían artificialmente el tráfico de la competencia. Las empresas tecnológicas utilizan la gestión de intereses para desregular las búsquedas de información, al considerar que, se estaría violando la libertad de negocio.

Reglas antimonopolio

Uno de los riesgos más grandes para las grandes empresas de tecnología se centra en su propio éxito: Al haber logrado una gran participación de mercado, se enfrentar a la posibilidad de sufrir la aplicación de las "reglas antimonopolio". Estas leyes ya han sido usadas con empresas de tecnología, tal es el caso de Microsoft.

A pesar de lo mencionado anteriormente, las empresas tecnológicas defienden sus intereses negando una situación monopólica. Por otra parte, para Sitaraman (2020, p. 116) la actual situación de enfrentamiento tecnológico con China, obligaría a Estados Unidos a tener las empresas más grande de tecnología de su lado. En ese sentido:

> "en lugar de amenazar con socavar la seguridad nacional, rompiendo y regulando a las grandes empresas tecnológicas, es necesario proteger las libertades democráticas de los Estados Unidos y preservando su capacidad de competir y defenderse de las nuevas grandes potencias rivales" (Sitaraman, 2020, p. 116).

En el 2020 se generó una polémica por la investigación de la Cámara de Representantes de los Estados Unidos hacia las grandes empresas tecnológicas por posibles prácticas monopolísticas. En esa polémica se citó a Jeff Bezos, Director ejecutivo de Amazon, a comparecer ante una Comisión del Congreso (BBC, 2020)

CAPÍTULO II: LAS POLÍTICAS EXTERIORES PARA EL CIBERESPACIO

1. Ciberdiplomacia y el liderazgo geopolítico del ciberespacio

El ciberespacio, como reflejo y extensión de la realidad física, se convierte en un espacio de interacción, diálogo y conflicto entre sus usuarios. En el caso de los intereses de los Estados en este ámbito, Barrios comenta:

> "El ciberespacio no es una entidad neutra, a-histórica y supraestatal que avanza sobre los Estados. Muy por el contrario, forma parte constitutiva del Estado y en él se asumen nuevas formas de organización del poder y se reproducen las relaciones jerárquicas, asimétricas y nacionales que son propias del Estado"(M. Barrios, 2017).

Como parte de las estrategias estatales para defender y promover sus intereses en el ciberespacio, muchos Ministerios de Relaciones Exteriores en el mundo han potenciado el recurso de la ciberdiplomacia. La manera de organización y las funciones dependen del tamaño de la potencia, los intereses que desean proteger, la realidad de cada país, a la propia definición de ciberdiplomacia y al modo en cómo aborda al fenómeno de la Cuarta Revolución Industrial.

En el presente capítulo se mostrarán algunas iniciativas, alcances logros y tendencias de ciberdiplomacia, considerando las prioridades explicadas en el capítulo anterior, teniendo en consideración que "el control del ciberespacio es una nueva instancia geopolítica mundial" (Buzai, 2013, p. 88).

1.1. EEUU: La superpotencia en el ciberespacio

En el 2011, Estados Unidos estableció su primera Estrategia Internacional para el Ciberespacio y la presentó la Secretaria de Estado del momento, Hillary Clinton. La estrategia identifica una serie de prioridades que incluyen la economía digital, la protección de redes, los asuntos militares, la gobernanza de internet, el desarrollo internacional y la libertad de internet. Estas prioridades se basan en tres pilares: la diplomacia, la defensa y el desarrollo. Se incluyen además los siguientes pilares:

a. "Promover normas y construir seguridad internacional: Construir un consenso global con respecto al comportamiento responsable de los Estados en el ciberespacio, la aplicación del derecho internacional existente para mejorar la estabilidad, fundamentar las políticas de seguridad nacional, fortalecer las asociaciones y prevenir malas interpretaciones que pueden conducir a conflictos.

b. Combatir el cibercrimen: mejorar las capacidades de los Estados para combatir el delito cibernético, potenciar la promoción de la cooperación internacional y el intercambio de información, y la capacitación de las fuerzas del orden, los especialistas forenses, los juristas y los legisladores.
c. Fortalecer las políticas públicas de Internet y la gobernanza de Internet: Desarrollar políticas que promuevan la innovación y los estándares internacionales; mejorar la seguridad, confiabilidad y resistencia; ampliar la colaboración y el Estado de Derecho; y promover estructuras e instituciones de gobernanza de Internet inclusivas que incluyan a partes interesadas del gobierno, la sociedad civil y el sector privado y que atiendan eficazmente las necesidades de todos los usuarios de Internet.
d. Apoyar la libertad de Internet: preservar y expandir Internet como un espacio global abierto para la libre expresión y para la organización y la interacción en toda la gama de intereses y esfuerzos humanos; promover el consenso internacional sobre la aplicación de los derechos humanos en el ciberespacio; brindar apoyo político y técnico a las personas que enfrentan la represión en Internet; y alentar a las empresas a adoptar prácticas y políticas que respeten los derechos humanos en línea.
e. Realizar la debida diligencia en ciberseguridad: Desarrollar y fortalecer las relaciones con otros países para mejorar la ciberseguridad global mejorando la defensa de la red nacional y las capacidades de recuperación y gestión de incidentes; aumentar la participación en las estructuras de ciberseguridad regionales y mundiales existentes; y cooperar en los esfuerzos para abordar las amenazas de interés mutuo.
f. Desarrollar Internet y las tecnologías de la información y la comunicación (TIC) para el crecimiento económico: ampliar la infraestructura de las TIC, aumentar el acceso a Internet y fomentar la producción de contenido en línea atractivo y contextualmente relevante para los usuarios locales como medio de catalizar el desarrollo económico y social (White House, 2011).

Como parte de la estrategia en el plano de la Política Exterior, se creó la Oficina del Coordinador de Asuntos Cibernéticos dentro del Departamento de Estado de los Estados Unidos, la cual es la primera oficina centrada exclusivamente en los temas cibernéticos en una oficina asuntos exteriores en todo el mundo.

Estados Unidos ha estado presente en una gran cantidad de controversias interestatales vinculadas al ciberespacio. Uno de los casos más sonados de este tipo de actividades por

parte de un Estado fue la operación encubierta “Olympic Games”, atribuida al Gobierno de Estados Unidos, y que consistió en ciberataques para sabotear el programa nuclear iraní (Alandete, 2012).

Por otra parte, ha sido acusado cuando en el año 2012, se tomó conocimiento de que la Agencia de Seguridad Nacional (NSA) de Estados Unidos, a través de un programa llamado PRISM recolectó, a través de servidores de empresas como Google, Apple, Facebook y Microsoft, información privada de ciudadanos extranjeros, incluida una treintena de líderes mundiales como la entonces Presidenta brasileña Dilma Rousseff y la actual Canciller alemana Angela Merkel (BBC, 2013).

En la actualidad las principales empresas tecnológicas del mundo son de origen estadounidense y el nivel de desarrollo en el ciberespacio es el mayor en el mundo. Sin embargo, en el marco de la Cuarta Revolución Industrial, existe un escenario de competencia entre China y Estados Unidos por liderar el desarrollo de esta revolución.

Para Sandoval “Esto se debe a que la magnitud de los beneficios económicos y políticos que trae consigo este nuevo fenómeno hacen que su liderazgo a nivel global sea un elemento importante para aquel Estado que busque la hegemonía” (Sandoval, 2019, p. 6).

La actual tensión en el ciberespacio no es tan reciente. Un caso emblemático se remonta al 2013, durante la administración Obama, cuando se acusó al gobierno chino de usar hackers para atacar medios de comunicación estadounidenses. Esta fue la primera vez que Estados Unidos admite públicamente haber recibido un ciberataque (BBC, 2014).

Con ese evento, según Segal, “los ciberataques dejaron de ser una actividad discreta y velada a una estrategia pública con el capacidad para poner patas arriba lo que muchos consideran la relación bilateral más importante del siglo XXI” (Segal, 2016, p. 8).

Recientemente, durante la administración del presidente Donald Trump, el departamento de Estado ha lanzado el programa Clean Network, por medio del cual se busca “salvaguardar los activos de la nación, incluida la privacidad de los ciudadanos y la información más sensible de las empresas, de intrusiones agresivas de actores malignos, como el Partido Comunista Chino”(US Department of State, 2020). Con esta iniciativa se invita a participar a esta iniciativa no solo a Estados, sino también a empresas tecnológicas.

La iniciativa integra temas relacionados a la privacidad de los datos, la seguridad, los derechos humanos y la colaboración basada en principios que plantean al mundo libre los “actores malignos autoritarios” (US Department of State, 2020).

1.2. China: Supremacía del Estado

La visión china sobre el ciberespacio se basa en la noción de la supremacía del Estado como único garante de la seguridad en el ciberespacio (Bozhkov, 2020). Los intereses chinos en el ciberespacio están centrados en sus objetivos geopolíticos y su interés de convertirse en una "superpotencia cibernética" en el ámbito económico, normativo, militar (Bozhkov, 2020).

Por ello, impulsa una economía autosuficiente y un crecimiento impulsado por la innovación, la reducción de la dependencia de tecnologías extranjeras para asegurar y controlar las cadenas de suministro clave y el control de su propia población para garantizar la supervivencia del régimen.

China tiene la mayor cantidad de usuarios de Internet del mundo con más de 829 millones (Xia, 2019) y una economía digital en rápida expansión. China cuenta con grandes empresas tecnológicas, gigantes como Alibaba, Didi, Tencent y Baidu que pueden competir cada vez más con los de Silicon Valley en términos de valor de mercado e influencia en el ciberespacio.

Para Segal, China se centra en promover una visión de soberanía del ciberespacio en la que se aboga por un reconocimiento más significativo de los derechos y papel de los Estados en la gobernanza de Internet, los esfuerzos de Beijing para influir en la gobernanza global del ciberespacio se organizan en torno al concepto de soberanía cibernética (o de Internet) (wangluo zhuquan), existe el temor que esta visión genere un Internet menos abierto y libre (Segal, 2020, p. 87).

Para Segal, China busca promover esta visión es porque el posible riesgo a su sistema de gobierno y ve con particular preocupación la concentración del poder económico y político por parte de las grandes empresas de tecnología, la mayoría de origen estadounidense, quienes pueden ser una amenaza por la propagación de “desinformación”, y un riesgo a la privacidad de la población y del gobierno(Segal, 2020,p.88).

Según la última Estrategia Internacional para el ciberespacio expuesta en el 2017, y que fue desarrollada por el Ministerio de Relaciones Exteriores Chino, los objetivos de la diplomacia cibernética de China girarían en torno a:

1. “Salvaguardar la soberanía y la seguridad mediante la inversión en ciberdefensa y por medio de medidas de confianza
2. Desarrollar un sistema de reglas internacionales manteniendo la estabilidad en el ciberespacio.

3. Promover una gobernanza de Internet "justa" y abogar por un cambio hacia un sistema de gobernanza del dominio cibernético más inclusivo, democrático, transparente, pero también más intergubernamental.
4. Proteger los derechos e intereses legítimos de los ciudadanos mediante la aplicación de un ciberespacio "nacional" y "basado en normas" en el que los derechos de los ciudadanos y los derechos humanos fundamentales deben equilibrarse con otras prioridades, como el mantenimiento del "orden" social, la seguridad nacional e intereses públicos
5. Promover la cooperación en la economía digital impulsando el desarrollo de tecnologías digitales y la innovación para cambiar los motores del crecimiento económico
6. Construcción de plataformas para el intercambio cultural entre estados-nación"(FMPRC, 2017).

Según Bozhkov, por medio del Ministerio de Relaciones Exteriores, en particular el Control de Armas y Desarme y el Departamento de Tratado y Derecho, se ocupa de la ciberdiplomacia y la "reglamentación" internacional del ciberespacio (Bozhkov, 2020, p. 26).

China viene teniendo una mayor relevancia en la gobernanza del ciberespacio; en este aspecto, China ha buscado desarrollar su poder nacional y su capacidad tecnológica para eventualmente liderar el camino de la gobernanza del ciberespacio (Cuihong, 2018, p. 69).

El gobierno chino ha sido acusado en diversas oportunidades de realizar ciberespionaje con el objetivo de obtener propiedad intelectual e información de identificación personal. Ejemplo de ello fue en julio de 2017, cuando la agencia de inteligencia nacional de Alemania se quejó de ciberespionaje chino dirigido hacia la industria alemana, hacia el Ministerio de Relaciones Exteriores de Alemania y a institutos de investigación militar alemanes que critican el liderazgo político de China (Shalal, 2017).

Para Bozhkov "el ciberespacio representa un arma de doble filo que se encuentra en el nexo de tres preocupaciones para el Partido Comunista Chino: legitimidad del régimen, seguridad nacional y dependencia tecnológico-económica" (Bozhkov, 2020, p.14).

El 8 de septiembre de 2020, en el marco de la reunión de alto nivel del Seminario Internacional sobre "Aprovechar las Oportunidades Digitales y Buscar la Cooperación y el Desarrollo" el Ministro de Relaciones Exteriores, Wang Yi, dio un discurso de apertura

titulado “Adherirse al Multilateralismo, Defender la equidad y la justicia y Trabajar Juntos para la Cooperación de Beneficio Mutuo” y propuso la "Iniciativa Global Sobre Seguridad de Datos-GIDS".

La iniciativa GIDS presenta un conjunto de 8 compromisos, que el Gobierno chino espera puedan ser recogidos en los futuros acuerdos bilaterales, regionales o internacionales que sean suscritos por terceros Estados, y que normen el acceso, protección, almacenamiento, administración y uso de datos. Estos 8 compromisos contienen un conjunto de propuestas proactivas y no vinculantes, orientadas a generar un consenso global sobre la necesidad de:

1. “Manejar la seguridad de datos de una manera comprensiva, objetiva y en base a evidencias, y mantener una cadena de abastecimiento de productos y servicios digitales abierta, segura y estable
2. Evitar el uso de tecnologías para hurtar o vulnerar la infraestructura crítica, la seguridad nacional o el interés público de terceros Estados.
3. Prevenir la vulneración de la información personal y la vigilancia y recolección de información de Estados.
4. Evitar que los Estados obliguen a sus empresas locales a recolectar y almacenar en territorio nacional datos obtenidos del exterior.
5. Asegurar que los Estados respeten la soberanía, jurisdicción y gobierno de la data de terceros Estados, y no accedan a ella sin permiso previo.
6. Promover el uso de medios legales o de acuerdos bilaterales o regionales para acceder a información de terceros Estados.
7. Evitar que las corporaciones tecnológicas instalen “puertas traseras” en productos y servicios ofrecidos, a fin de acceder ilegalmente a los datos de sus usuarios, o controlar sus dispositivos.
8. Evitar que las corporaciones tecnológicas procuren objetivos ilegales abusando de la dependencia de sus usuarios a sus productos o servicios” (FMPRC, 2020).

En términos generales, la iniciativa china “*Iniciativa Global sobre la Seguridad de Datos*” (GIDS) china representa una propuesta proactiva que contiene un conjunto de principios y compromisos que pueden cooperar al desarrollo de un ciberespacio más seguro en circunstancias en la que no existe un marco de Gobernanza Digital Global, haciendo un llamado a que los Estados, empresas y la sociedad civil en general mantengan un comportamiento responsable en el ciberespacio (FMPRC, 2020).

Paralelamente, la iniciativa china debe mirarse desde una perspectiva geopolítica, en tanto se enmarca en un escenario internacional caracterizado por el escalamiento de las confrontaciones políticas y económicas entre Estados Unidos y China, primera y segunda economías mundiales y dos de los principales socios del Perú, en el que el componente tecnológico tiene una presencia cada vez mayor.

En su discurso de presentación de la iniciativa GIDS el 8 de setiembre pasado, el Canciller chino Wang Yi se refirió a la necesidad de proteger el multilateralismo para hacer frente al déficit en materia de gobernanza digital global, y para detener los ataques unilaterales que "cierto país" realiza en base a acusaciones sin pruebas y en nombre de una "red limpia", instrumentalizando la problemática de la seguridad en el ciberespacio como pretexto para atacar intereses de empresas y terceros países con los que actualmente compite (FMPRC, 2020).

Asimismo, el Canciller Yi agregó que es necesario que la protección de la seguridad en el ciberespacio se ejecute sobre la base de hechos y de la ley, indicando que la politización de del tema y los dobles estándares vulneran las normas básicas que gobiernan las relaciones internacionales (FMPRC, 2020).

Vista desde este punto de vista, la iniciativa GIDS representa también una respuesta política del Gobierno chino a la campaña estadounidense análoga denominada "*The Clean Network Program*", abierta a países aliados y presentada como una iniciativa orientada a proteger la privacidad de la información de la población y de las compañías de intrusiones de agentes malintencionados, haciendo referencia explícita al Partido Comunista chino.

1.3. Rusia: Un espacio de reivindicación

La ciberdiplomacia rusa ha sido sumamente activa en la ONU. Tuvo un temprano logro en 1998, cuando Moscú presentó el primer proyecto de resolución sobre tecnologías de la información y las comunicaciones en la Primera Comisión de Asuntos de la Asamblea General.

En el 2018, se adoptaron dos resoluciones contrapuestas respecto a la gobernanza global de Internet: la reafirmación patrocinada por Estados Unidos del Grupo de Expertos Gubernamentales de la ONU (UN GGE) y la propuesta rusa de un Grupo de Trabajo de Composición Abierta (OEWG). Ese mismo año, Rusia patrocinó con éxito otra resolución en la Tercera Comisión de la Asamblea General sobre ciberdelincuencia.

La propuesta de esta resolución sobre ciberdelincuencia formaba parte de una estrategia para poner en marcha una vía separada sobre el tema en la ONU, como alternativa al Convenio de Budapest sobre ciberdelincuencia, a la cual Rusia se opone.

Rusia publicó su Doctrina de Seguridad de la Información de la Federación Rusa en el 2010, la cual describe los intereses de Rusia en el ciberespacio. En esta se detalla que el interés nacional sobre la esfera de la información es:

1. “Proteger los derechos constitucionales humanos y civiles y sus libertades y mecanismos de interacción con el Estado.
2. Mantener operacional la infraestructura de la información, en especial la información crítica de la Federación Rusa y la red de telecomunicación durante la paz y en caso de una amenaza de agresión durante la guerra.
3. Continuar con el desarrollo del sector de las tecnologías de la información y mejorar la producción, la investigación y las comunidades sociales y científicas en el ámbito, y proveer servicios de seguridad de la información.
4. Proveer a la comunidad rusa e internacional con información confiable sobre las políticas de Estado de la Federación Rusa y su posición oficial sobre eventos significativos en Rusia y en el mundo, y utilizar las tecnologías de la información para asegurar la seguridad nacional del Estado ruso en la esfera de la cultura.
5. Facilitar el desarrollo de la seguridad de la información internacionalmente, crear alianzas estratégicas en el área del ciberespacio y proteger la soberanía de la información de la Federación Rusa” (Presidencia de Rusia, 2010).

Para Kurowska, Rusia busca el respeto y el reconocimiento que perdió en la década de 1990 y su estrategia en el en el ámbito del ciberespacio resulta sumamente coherente para una potencia se encuentra “remergiendo” (Kurowska, 2019, p. 6).

Rusia ha sido acusado numerosas veces de realizar ciberataques a países occidentales, siendo los más representativos, el ciberataque sufrido por Estonia en el 2007 y la intromisión en las elecciones de Francia y Estados Unidos. De igual modo, ha realizado un conjunto de acciones que lo colocar como un actor fundamental en el ciberespacio.

En el 2011, Vladimir Putin declaró que Rusia tenía la intención de utilizar la Unión Internacional de Telecomunicaciones para monitorear y controlar Internet, una visión que se opone mucho a la de la UE. De igual modo, ese mismo año, China y Rusia propusieron el Código de Conducta Internacional para la Seguridad de la Información a través de la Organización de Cooperación de Shanghai (OCS) (Barrinha, 2018, p. 37)

Para Segal (2016, p. 41), Rusia tiene todos los elementos para ser una superpotencia en el ciberespacio: tiene los mejores hackers del mundo, utiliza sus habilidades de manera táctica, pero sus empresas tecnológicas, a pesar de sus avances, no han alcanzado un desarrollo suficiente más allá de su espacio territorial.

Rusia busca un mayor control gubernamental sobre internet, en noviembre de 2019 entró en vigor la llamada ley de “internet soberano” que establece una serie de puntos de control sobre el tráfico de internet y podría llevar a una desconexión de Rusia de la red con un funcionamiento autónomo (Roth, 2019).

Finalmente, en el espacio multilateral, Rusia, quien no forma parte del Convenio de Budapest, busca como objetivo de política exterior crear las condiciones para y adoptar por Convención de las Naciones Unidas sobre Seguridad de la Información Internacional (SCRF, 2013).

1.4. Francia: estrategia internacional para las tecnologías digitales

La tecnología digital se ha convertido en un gran desafío para la política exterior francesa y la acción pública en su conjunto. El 15 de diciembre de 2017 se presentó la Estrategia Internacional Francesa de Tecnología Digital, propuesta por el Ministro de Europa y Asuntos Exteriores, la cual es el marco de referencia y la hoja de ruta diplomática para los próximos años(Francia Diplomacia, 2018).

La estrategia fue sometida a consulta pública para solicitar las opiniones de los ciudadanos franceses y compatriotas. Se basa en tres ejes principales: gobernanza de internet, economía y seguridad.

1. Promover un mundo digital, abierto, diverso y confiable

El gobierno francés considera que la gobernanza de Internet, la definición y aplicación de las reglas que gobiernan el ciberespacio deben tener como objetivo mantener su apertura y diversidad, al tiempo que aumenta la confianza de las personas en el uso de la red, que Internet debe seguir siendo una infraestructura abierta común para que las externalidades positivas que se esperan de la transformación digital desempeñen plenamente su papel y que la gobernanza multiactor ha demostrado eficacia, por lo que debe mantenerse y fortalecerse para preservar el equilibrio ante estas amenazas de fragmentación interna y externa (Francia Diplomacia, 2018).

Para el gobierno francés, el Estado, el sector privado y la sociedad civil, reconocen desde hace mucho tiempo la utilidad de los enfoques multilaterales. Por lo que apoyan los mecanismos de gobernanza en la que participen activamente. Por ello, promueven:

- Mantener un entorno digital internacional abierto
- Promover el acceso universal a múltiples tecnologías digitales.
- Fortalecer la confianza en Internet

2. Promover el desarrollo del Internet sobre la base del equilibrio entre la libertad pública, el crecimiento y la seguridad en el mundo digital.

El modelo digital que Francia espera impulsar se basa en una perspectiva europea, la cual tiene como grandes ejes:

- Garantizar la efectividad de la protección de derechos
- Fortalecimiento del ecosistema digital europeo
- Reforzar la seguridad europea y la autonomía estratégica en el mundo digital

3. Fortalecer la influencia, el atractivo y la seguridad en el campo digital.

Para Francia, la tecnología digital es una nueva oportunidad de desarrollo, crecimiento e intercambio. A través de la transformación digital se busca hacer de Francia una república digital. A partir de los siguientes ejes:

- Hacer de Francia un centro de excelencia en el mundo digital
- Garantizar la seguridad y la autonomía estratégica de Francia en el mundo digital
- Un mundo digital en el que su autonomía está garantizada, sus participantes económicos son competitivos y sus derechos están protegidos.

En el último tiempo, la relación de Francia con las grandes empresas tecnológicas ha sido sumamente compleja. Por un lado, Francia ha sancionado a empresas como Google y Facebook con millonarias multas tras incumplir las normas del Reglamento General de Protección de Datos europeo. Por otro lado, París ha instaurado una tasa a los gigantes digitales, conocida como "tasa Google" o "tasa GAFA" (por Google, Amazon, Facebook y Apple). Esta situación ha generado tensiones con Washington, quien en represalia por ese impuesto, sancionó la importación de productos galos(Deutsche Welle, 2020)

Para Francia, el único camino que queda sobre la mesa es alcanzar un acuerdo internacional para tasar a los gigantes de internet (Deutsche Welle, 2020).

El "Llamado de París a la confianza y la seguridad en el ciberespacio", propuesto por Francia, se plantea desde una lógica de inclusión de múltiples actores (Estados, empresas privadas, organizaciones de la sociedad civil). Entre los apoyos más representativos desde el sector de las empresas tecnológicas destacan Microsoft, Kaspersky, Google, Facebook y Huawei.

1.5. Intereses de la Unión Europea en la ciberdiplomacia

La Secretaría General del Consejo de la Unión Europea compartió las conclusiones del Consejo sobre la ciberdiplomacia adoptadas por el Consejo de Asuntos Generales el 10 de febrero de 2015. En este documento se considera esencial que la UE siga elaborando y ejecutando en el plano internacional un planteamiento común y global para la ciberdiplomacia que:

1. “promueva y proteja los derechos humanos y esté basado en los valores fundamentales para la UE de la democracia, los derechos humanos y el Estado de Derecho, incluido el derecho a la libertad de expresión, el acceso a la información y el derecho a la intimidad;
2. garantice que no se abuse de Internet para alimentar el odio y la violencia, y establezca salvaguardias para que Internet siga siendo, con escrupulosa observancia de las libertades fundamentales, un foro para la libre expresión con pleno respeto de la ley;
3. fomente una política del ciberespacio basada en la igualdad de género;
4. impulse el crecimiento, la prosperidad y la competitividad de Europa y proteja los valores básicos de la UE, entre otras cosas reforzando la ciberseguridad y mejorando la cooperación en la lucha contra la ciberdelincuencia;
5. contribuya a contrarrestar las amenazas para la ciberseguridad, así como a la prevención de conflictos y a una mayor estabilidad en las relaciones internacionales mediante el uso de medios diplomáticos y jurídicos;
6. potencie los esfuerzos para reforzar el modelo multisectorial de gobernanza de Internet;
7. fomente unas sociedades abiertas y prósperas mediante medidas de creación de cibercapacidad en los países terceros, de manera que se potencie la promoción y la protección del derecho a la libertad de expresión y el acceso a la información y se permita a los ciudadanos gozar plenamente de los beneficios sociales, culturales

y económicos del ciberespacio, inclusive mediante el fomento de infraestructuras digitales más seguras;

8. promueva el reparto de responsabilidades entre los interesados, incluso a través de la colaboración sobre cuestiones cibernéticas entre los sectores público y privado, así como con las instituciones universitarias y de investigación" (Secretaría General Consejo de la Unión Europea, 2015, p.4).

Este documento es particularmente interesante pues no solo se hace mención a los intereses en el ciberespacio, sino que, a diferencia de la mayoría de documentos, se hace una mención explícita de la "ciberdiplomacia".

El 16 de setiembre del presente año, la presidenta de la Comisión Europea, Úrsula von der Leyen en el discurso del Estado de la Unión mostró la necesidad de que Europa adopte posiciones claras y acciones rápidas en los asuntos globales. Para ello "buscan cambio, por diseño, no por destrucción"(von der Leyen, 2020) .

El tema digital fue central en su discurso como medio para potenciar el liderazgo europeo en el mundo y busca "hacer de esta Europa la Década Digital". Por ello, se exhortó a creación de un plan común para la Europa digital con objetivos claramente definidos para 2030, como conectividad, habilidades y servicios públicos digitales. Se busca seguir los principios de derecho a la privacidad y la conectividad, la libertad de expresión, el libre flujo de datos y la ciberseguridad"(von der Leyen, 2020).

En el discurso se enfatizó la necesidad de que Europa sea tecnológicamente independiente, la necesidad de alcanzar una soberanía digital europea, urgencia de potenciar la industria local de la data, centrarse en la innovación tecnológica, resaltó la necesidad de promover la inteligencia artificial, para lo que anunció una inversión de 8.000 millones de euros en la generación de vanguardia fabricada en Europa. (von der Leyen, 2020).

2. Experiencias de ciberdiplomacia, competitividad y liderazgos regionales

En el apartado anterior se mostró el rol de las principales potencias mundiales en torno al ciberespacio. En la siguiente sección se mostrarán experiencias e iniciativas actuales de potencias que tienen como objetivo desarrollar y potenciar su seguridad, economía e influencia en el gobierno del ciberespacio, en el contexto de la Cuarta Revolución Industrial.

2.1. Ciberdiplomacia en Latinoamérica

La política exterior hacia el ciberespacio de los Estados Latinoamérica se ha caracterizado por la defensa de los valores liberales y la inclusión, y está en proceso de crear medidas de fomento de la confianza, para combatir el ciberdelito, impulsar la economía digital y proteger los derechos humanos en línea.

Para Nathalie Van Raemdonck, una analista belga sobre temas de ciberdiplomacia:

> "A pesar de las alianzas cambiantes y las ideologías conflictivas en América Latina, existen mecanismos de cooperación regional efectivos que fortalecen la región contra las amenazas digitales… el programa de ciberseguridad de la OEA y el Grupo de Trabajo de Fomento de la Confianza contribuyen enormemente a esta cooperación eficazen la región"(Van Raemdonck, 2020, p. 4).

La posición de América Latina en el mundo tiene su reflejo en el ciberespacio. Existe una compleja relación entre esta región y las dos fuerzas cibernéticas dominantes en el mundo: Estados Unidos y China.

En el contexto de la Cuarta Revolución Industrial, esta región deberá encontrar una vía intermedia entre el peso histórico y cultural con Estados Unidos, y el creciente interés y dependencia hacia China, países que tienen visiones contrapuestas en el ciberespacio.

En el siguiente apartado se mostrarán algunas experiencias de ciberdiplomacia en la región y el impuso que se le ha dado al ámbito digital.

2.1.1. Chile y el Acuerdo DEPA

La política exterior chilena en torno al ciberespacio gira en torno al cumplimiento de la Agenda 2020, que coloca el desarrollo y la masificación en el uso de las tecnologías de información y comunicaciones como un eje transversal y un objetivo país prioritario.

En el 2018, la Cancillería chilena lanzó su Estrategia Nacional de Política Exterior al año 2030. La Ciencia, Tecnología e Innovación es uno de los tres temas estratégicos y emergentes de esta Estrategia. En este documento se menciona que:

> "el desafío para un país como Chile, con población y territorio pequeño y aparentemente distante, es cómo insertarse en dichas redes de I+I+D que son parte de un entramado de poder, relaciones y conocimiento, donde los gobiernos, las grandes empresas, y crecientemente las y los ciudadanos, juegan importantes roles"(Ministerio de Relaciones Exteriores de Chile, 2018, p.80).

De igual modo, reconoce la importancia de una economía cada vez más digital y directamente relacionada con el valor del conocimiento, en el marco de la Cuarta Revolución Industrial. Por ello, “El éxito ya no depende de la mano de obra barata o del capital físico, sino de quienes pueden innovar y crear nuevos productos, servicios y modelos de negocios, las proyecciones señalan que el capital digital primará por sobre el financiero o el físico” (Ministerio de Relaciones Exteriores de Chile, 2018, p. 94)

Para ello, se articulan una serie de acciones que incluyen ampliar, profundizar y aprovechar los acuerdos comerciales, incluir los temas de economía digital en todos los acuerdos comerciales, apoyar la atracción y promoción de inversiones y fomentar la exportación de servicios digitales(Ministerio de Relaciones Exteriores de Chile, 2018).

De igual modo, la Política Nacional de Ciberseguridad del año 2018, responde a los riesgos que conlleva la masificación de las nuevas tecnologías y que estos riesgos pueden afectar los derechos de las personas, la seguridad pública, las infraestructuras críticas, el gobierno digital, los intereses esenciales y la seguridad exterior de Chile.

Dentro de esta política se establece como uno de los objetivos de alto nivel la cooperación y relaciones internacionales en torno a la ciberseguridad en el contexto global. Para ello, se contemplan medidas específicas encargadas al Ministerio de Relaciones Exteriores, desde una visión que responde a las prioridades de la ciberdiplomacia.

Por otra parte, se prioriza la cooperación en ciberseguridad con otros actores y la participación activa en foros y discusiones internacionales. Por ello, Ministerio de Relaciones Exteriores deberá coordinar con el resto de los ministerios y agencias de gobierno, la política internacional en materia de ciberseguridad (Comité Interministerial sobre Ciberseguridad, 2018, p.16).

Más aún, el Ministerio de Relaciones Exteriores tiene la función de gestionar la cooperación internacional, asistencia, el intercambio de información y experiencias, la implementación y profundización de mecanismos de diálogo político en la materia, y el empuje de medidas de transparencia y construcción de confianza en el ciberespacio en el ámbito bilateral y multilateral (Comité Interministerial sobre Ciberseguridad, 2018, p. 16).

Finalmente, se detalla como prioritario el fomento de normas internacionales que promuevan la confianza y seguridad en el ciberespacio, desde una visión país sobre gobernanza de internet.

Por otra parte, desde la Dirección de Energía, Ciencia y Tecnología e Innovación del Ministerio de Relaciones Exteriores, se busca colaborar con la Agenda 2020 a partir de:

> "facilitar la vinculación de las políticas de Chile en energía, ciencia, tecnología, conocimiento e innovación con la política exterior, a través de la generación de alianzas estratégicas con Estados afines, organismos y actores relevantes, tanto en la esfera bilateral, como multilateral y regional, con el propósito de fortalecer y complementar las capacidades nacionales en dichos ámbitos"(Ministerio de Relaciones Exteriores, 2020a) .

Desde el año 1992, con la firma del Acuerdo Marco Básico sobre Ciencia y Tecnología, Estados Unidos y Chile tienen una asociación de cooperación en materia de ciencia, tecnología e innovación. En marzo de 2018 se creó el Consejo Chile-Estados Unidos para la Ciencia, Tecnología e Innovación (STIC), un foro público-privado destinado a fortalecer el ecosistema de CTI entre ambos países, que tienen como objetivo estratégico del Consejo conectar a los productores de CTI con los consumidores (STIC, 2019).

El Comité Ejecutivo de STIC ha establecido en seis grandes propuestas marco:

1. La vinculación de empresas y universidades para la actualización de contenidos y optimización de procesos de transferencia tecnológica desde las carreras y programas de ciencia, tecnología, e innovación.
2. Fortalecer y diseñar herramientas tributarias para incentivar la inversión abierta y en I+D desde las Start-up a las grandes empresas.
3. Crear mecanismos de financiamiento y fondos para el libre acceso a red de mentores en CTI nacionales e internacionales.
4. Fortalecer mecanismos y programas de vouchers para pequeñas y medianas empresas (PYMEs) dirigidos al acceso a recursos técnicos e intelectuales para desarrollar y hacer frente a desafíos tecnológicos.
5. Fortalecimiento de la educación a través de metodologías interactivas STEAM para la creación de habilidades en jóvenes del nuevo milenio.
6. Fortalecer y mejorar las capacidades, empleabilidad y nivel de ingresos de la fuerza laboral con formación técnico vocacional para la adaptación de nuevas tecnologías (STIC, 2019).

El último año ha sido particularmente emblemático para los intereses de Chile en el ciberespacio, en las nuevas tecnologías y en particular en el desarrollo de la economía digital. En junio del 2020 Chile firmó junto con Nueva Zelanda y Singapur firmaron, de manera remota, el Acuerdo de Asociación de Economía Digital (DEPA, por su sigla en

inglés), que busca aprovechar el potencial de la Economía Digital para incluir a las MIPYMES en la economía global.

Según la Subsecretaría de Relaciones Económicas Internacionales del Ministerio de Relaciones Exteriores:

> “el objetivo principal de este acuerdo es establecer ciertas reglas básicas para promover plataformas para la economía digital. Eso se realizaría marco amigable común para las empresas que exportan servicios y productos digitales. Más aún, permite explorar materias nuevas en el contexto tecnológico que sirvan a la sociedad en general garantizando un desarrollo económico inclusivo” (Subsecretaría de Relaciones Económicas Internacionales, 2020).

Para García (2020) “este Acuerdo representa un hito en la política de negociaciones comerciales y en la configuración de reglas globales para la nueva era del comercio internacional digital, es pionero porque propicia una economía digital global integrada, con una visión de futuro que señala la senda para las normas de futuras negociaciones comerciales”.

De igual modo considera que el DEPA establece normas claras que pretenden armonizar la interoperabilidad entre los países al crear oportunidades para la digitalización, y aborda cuestiones claves salvaguardando principios fundamentales en este ambiente. Entre ellas: i) el uso de dispositivos electrónicos; ii) no discriminación de productos digitales, trato nacional; iii) facilitación en la documentación de los negocios transfronterizos, e-invoicing, y promoción en el uso de pago electrónico; iv) protección de información personal; v) ciberseguridad, vi) protección del consumidor online, compromiso para trabajar en la eliminación de los mensajes publicitarios no solicitados (spam); vii) protección de identidades digitales seguras; viii) un marco de gobernanza ético en la implementación de la inteligencia artificial, ix) el libre flujos de datos, y x) abordar la brecha e inclusión digital con la garantía de acceso a una internet abierta” (García, 2020)

En agosto del 2020, el Presidente Sebastián Piñera anunció el inicio del proceso de licitación pública de la red 5G nacional, por el cual se pondrán a disposición un total de 1800 MHz en cuatro procesos independientes entre sí (Monasterio, 2020). Se esperan que la tecnología esté comercialmente disponible entre 2021 y 2022. Según el propio presidente la licitación permitirá a Chile "ser pioneros en América Latina y dar un gran salto adelante en la integración plena de Chile a la sociedad digital" (Monasterio, 2020).

Como se mencionó anteriormente, la empresa Huawei es la líder en el mundo en tecnología 5G y se encontraría posibilitada a participar en la licitación. Esta situación podría generar cierta controversia debido a la actual competencia entre Estados Unidos y China.

2.1.2. Uruguay: "Consulado tecnológico"

La política exterior uruguaya hacia el ciberespacio y la tecnología gira en torno al cumplimiento Plan Estratégico Quinquenal (2015-2020). Dentro de la temática de Promoción Económica, constituye un objetivo prioritario el "aumentar el prestigio del país a través de la promoción de su producción exportadora y la confianza que ofrece el marco de previsibilidad jurídica y seguridad en materia de inversión"(Ministerio de Relaciones Exteriores, 2020c). Para ello, se busca la promoción de las ventajas país en relación a las inversiones, en particular en lo que se refiere al desarrollo tecnológico, software, industrias creativas.

De igual modo, por medio de la Agenda Uruguay Digital 2020, se considera que Uruguay tiene las condiciones para abordar los retos actuales y anticiparse a desafíos futuros de la sociedad de la información y del conocimiento, y contribuir así a acelerar su desarrollo social y económico

El 14 de febrero del 2020, se realizó la apertura del Consulado General del Uruguay en la ciudad de San Francisco, Estados Unidos. Según el propio Ministerio de Relaciones Exteriores consiste en el primer consulado tecnológico uruguayo en el mundo, y que busca dar un fuerte énfasis a los asuntos digitales.

La oficina tiene como prioridad la generación de capacidades para una mejor inserción en el escenario global, con el objetivo de crear "oportunidades para el ecosistema innovador nacional, la instalación de esta nueva sede oficiará de experiencia piloto para la puesta en marcha de una Diplomacia en la era digital"(Ministerio de Relaciones Exteriores, 2020b).

La labor del consulado estará centrada en tres áreas claves: la vinculación con empresas tecnológicas, universidades y fondos de capital de riesgo, que apunta a obtener financiamiento para emprendimientos uruguayos, la atracción de inversión productiva, con énfasis en los servicios globales, las telecomunicaciones y el desarrollo digital, y la promoción de la cooperación con privados y autoridades locales, que buscará impulsar el desarrollo tecnológico y la innovación en el país (Ministerio de Relaciones Exteriores, 2020b).

Se busca fortalecer los vínculos con las grandes empresas tecnológicas que mantienen sus sedes centrales en el área de la bahía de San Francisco, presentando a Uruguay como

un socio estratégico para la provisión de servicios globales (Ministerio de Relaciones Exteriores, 2020b). Cabe precisar que solo había si bien esta institución realiza actividad consular, en California la población uruguaya es muy pequeña, así que su principal labor radica en esta nueva labor.

De igual modo, Uruguay es desde año 2017 miembro del D9, es una red intergubernamental que agrupa a 9 de los países más avanzados en lo relativo al llamado gobierno digital. En la actualidad, la red está conformada por Canadá, Corea del Sur, Estonia, Israel, México, Nueva Zelanda, Portugal, Reino Unido, Uruguay.

A través de la cooperación internacional, el D9 se orienta a aplicar lo mejor posible las herramientas y competencias digitales,para así enriquecer y facilitar la vida de los habitantes de sus respectivos países, y para colaborar en la resolución de problemas comunes. Asimismo, también se intercambian ideas y experiencias, con el objetivo de adoptar y perfeccionar estándares

2.2. Liderazgo digital de países pequeños

En el desarrollo de la ciberdiplomacia algunos países resaltan por su nivel de evolución y sofisticación. A continuación se mostrarán ejemplos particularmente vanguardistas de desarrollos en las herramientas para la defensa y promoción de intereses nacionales en el ciberespacio y la función de sus Ministerios de Relaciones Exteriores en tal desarrollo.

2.2.1. Dinamarca: líder en Diplomacia tecnológica

El Ministerio de Relaciones Exteriores de Dinamarca ha desarrollado diversas herramientas modernas para abordar los temas relacionados al ciberespacio, las nuevas tecnologías, a través de un relacionamiento más directo con las grandes empresas tecnológicas.

Además de tratar sus intereses en el ciberespacio por medio de sus relaciones bilaterales y multilaterales, han generado innovaciones por medio de oficinas que funcionan como embajadas ante las grandes empresas tecnológicas, consulados daneses que funcionan como centros de innovación y centros de innovación administrados en bloque por medio del Consejo Nórdico de Ministros.

A mediados del 2017, Dinamarca se convirtió en el primer país del mundo en elevar la tecnología y la digitalización a una prioridad transversal en la política exterior y creó la “Oficina del Embajador Tecnológico”, la cual tiene a su cargo de una oficina en Silicon Valley (California) y una oficina en Beijing. Ambas sedes tienen la función de recopilar

información, promover sus intereses y salvaguardar los valores en el extranjero.(UDENRIGSMINISTERIET, 2019).

La oficina en Silicon Valley tiene la responsabilidad de representar al gobierno danés ante las empresas de tecnología para intentar influir la dirección de la tecnología, buscar acuerdos, inversión en tecnología. Por medio de estas acciones, se busca poder influir en la agenda internacional en torno a cuestiones de política tecnológica, de acuerdo con los intereses y valores daneses, incluso a través de nuevas alianzas, foros multilaterales y asociaciones de múltiples partes interesadas.

De igual modo, la oficina supervisa diversos temas que van desde asuntos ciberseguridad y atracción de inversiones en negocios digitales, hasta la protección de la privacidad en el ciberespacio, el uso responsable de la inteligencia artificial.

El diplomático Casper Klynge se convirtió en el primer embajador destinado a representar los intereses daneses ante las grandes empresas tecnológicas en Silicon Valley. Este diplomático mencionó en una entrevista:

> "¿Qué tiene un mayor impacto en la sociedad actual? ¿Un país en el sur de Europa o en el Sureste Asiático o Latinoamérica, o tal vez las grandes plataformas de tecnología? En mi opinión, nuestros valores, nuestras instituciones, la democracia, los derechos humanos, están siendo desafiados por el surgimiento de las nuevas tecnologías"(citado por Hidalgo, 2019).

En otra entrevista el embajador Klynge comentaba cómo era la gestión de la "oficina tecnológica":

> "Operativamente, la oficina en Silicon Valley funciona como una embajada y cuenta con dos aspectos demarcados de operación. Por un lado, y de la misma manera que las embajadas tradicionales, las oficinas trasladan consultas por parte de las autoridades danesas hacia las compañías tecnológicas; con propósito de influir en la toma de decisiones en cuanto a desarrollo tecnológico y facilitar la preparación de implementación de dichas tecnologías en Dinamarca. Por otra parte, la oficina busca influir sobre la agenda tecnológica de políticas públicas, en acuerdo a los intereses primarios y valores de la sociedad danesa. En busca de dicha expansión de agenda propia, la embajada tiene como objetivo explorar el campo para la generación de nuevas alianzas estratégicas, el desarrollo de foros y el co-sponsoreo de proyectos junto a diversos partners institucionales, empresariales y de sociedad civil"(citado por Molina, 2020, pp. 3-4).

> “De cierta manera, se puede afirmar que el proyecto se encuentra tratando temáticas fuera de lo que puede ser considerado diplomacia tradicional. Ciberseguridad y desinformación, el combate del terrorismo digital, los efectos legales de los denominados deep fakes, los impuestos digitales, la protección de la privacidad online, la responsabilidad y ética respectiva al desarrollo de la inteligencia artificial, y el correcto uso ético de la big data; son los ejes centrales de tratativa a los que se enfrenta la oficina en su día a día” (citado por Molina, 2020, p.4)

En un artículo escrito por el embajador Klynge, explicaba que su trabajo responde a la idea de que en el mundo cada vez más digital de hoy que, las nuevas tecnologías como la inteligencia artificial, el big data, el Internet de las cosas y blockchain trascienden las fronteras con una velocidad sin precedentes y están transformando todos los sectores de la sociedad (Klynge, 2019).

Para Klynge, en la actualidad, un grupo de empresas tecnológicas multinacionales se han vuelto extremadamente influyentes, en la medida en que su influencia económica y política iguala o supera a la de nuestros socios tradicionales, los estados-nación. Por el contrario, es cada vez más difícil para los responsables de la formulación de políticas mantenerse al día con el impacto de las nuevas tecnologías. Por ello, no consideraron suficiente que un gobierno se base únicamente en las relaciones diplomáticas tradicionales para llevar el conocimiento a casa, promover sus intereses y salvaguardar los valores en el extranjero (Klynge, 2019).

Comenta Klynge que en su experiencia “algunas empresas se han mostrado enormemente abiertas al diálogo y otras se han mostrado más reacios a participar en discusiones políticas incómodas” (Klynge, 2019).

Para Klynge, la iniciativa danesa ha permitido inspirar a otros gobiernos nacionales, como Alemania, Francia y Eslovaquia quienes han nombrado a embajadores dedicados a estos temas, pese a que cada uno tiene mandatos diferentes, pero todos se basan en la misma comprensión de que necesitamos involucrar a la industria de una manera más estructurada (Klynge, 2019)

Uno de los logros de su gestión fue reunir por primera vez en abril de 2019 a los embajadores tecnológicos y cibernéticos de 22 países en Silicon Valley para conversar con la industria. Finalmente, considera que a partir del reconocimiento de la importancia de la tecnología y la digitalización, las Naciones Unidas y la Unión Europea han empezado a

priorizar los esfuerzos por promover la paz y la seguridad, el desarrollo global y los derechos humanos en este ámbito. (Klynge, 2019).

Después de cumplir con su gestión, el embajador Klynge fue contratado por Microsoft como su nuevo vicepresidente de asuntos gubernamentales europeos, con sede en Bruselas. Casper continuará fortaleciendo las relaciones externas de la empresa con las instituciones de la UE, así como con los gobiernos de toda Europa, y se asegurará de que Microsoft sea un socio constructivo para ayudar a los responsables políticos en Bruselas y las capitales europeas a lograr sus objetivos.

Recientemente, en la Estrategia danesa de ciberseguridad y de la información 2018-2021, se solicitó explícitamente al Ministerio de Relaciones Exteriores, que el embajador tecnológico también se encargue de ver los asuntos del ciberespacio, en lo concerniente al diálogo con las grandes empresas tecnológicas (Ministry of Finance, 2018, p. 42). Además, la estrategia danesa generó la reciente creación del Coordinador de asuntos cibernético en el Ministerio de Asuntos Exteriores.

Las iniciativas responden al nuevo orden mundial en el que la digitalización y los poderosos actores tecnológicos desempeñan un papel cada vez mayor, y la diplomacia debe adaptarse.

Dinamarca tiene además un proyecto denominado “Innovation Center Denmark” por medio del cual se busca conectar instituciones de investigación, empresas locales y fondos de inversión con empresas danesas, se busca facilitar la cooperación en investigación y proporcionar inspiración para impulsar la innovación y los objetivos digitales en Dinamarca con los principales focos tecnológico del mundo. (Ministry of Foreign Affairs, 2019).

La iniciativa es una cooperación entre el Ministerio de Relaciones Exteriores y el Ministerio de Educación Superior y Ciencia de Dinamarca. En la actualidad tienen 8 centros en todo el mundo, los cuales son gestionados por tiene empleados financiados por ambos Ministerios. Por tanto, la dirección suele tener representantes a ambos ministerios.

Uno de estos Centros de Innovación se encuentra en San Francisco y trabaja en conjunto con el Consulado General de Dinamarca. En este caso ocupan el mismo establecimiento físico, pero ubicarse en dos ciudades diferentes. Hoy en día, la actual Cónsul General, Katrine Joensen desempeña como Cónsul y CEO del Centro de Innovación en San Francisco.

En el caso concreto de las oficinas en San Francisco, ambas oficinas comparten el mismo espacio físico, y algunos empleados trabajan solo con tareas relacionadas con el Consulado, otros funcionarios trabajan únicamente con el Centro de Innovación y hay algunos que trabajan con tareas relacionadas tanto con el Centro de Innovación como con el Consulado.

El Centro ha contratado como parte del personal a especialistas en ciencia, tecnología en innovación que son incorporados como “agregados”, consejeros e investigadores (Nordic Innovation, 2020a).

Finalmente, como parte de un esfuerzo común, los cinco países nórdicos: Islandia, Dinamarca, Suecia, Finlandia y Noruega, crearon el Centro de Innovación Nórdica - Nordic Innovation que es una organización financiada por los que opera bajo el Consejo Nórdico de Ministros, que está compuesto por los cinco Ministros de Cooperación Nórdica (Innovation, 2013).

Cabe señalar que en el Ministerio de Relaciones Exteriores de Dinamarca es atendido por cinco ministros distintos: el Ministro de Relaciones Exteriores, el Ministro de Cooperación Nórdica, el Ministro de Comercio, Turismo e Inversiones, el Ministro de Asuntos Europeos y el Ministro de Cooperación al Desarrollo. Por lo que existe una vinculación entre el Centro de Innovación Nórdica y el Ministerio de Relaciones Exteriores de Dinamarca.

Nordic Innovation tiene como objetivo hacer de los países nórdicos una región pionera en el crecimiento sostenible y trabaja para promover el espíritu empresarial, la innovación digital y la competitividad en las empresas nórdicas (Nordic Innovation, 2020a).

Uno de sus proyectos emblemáticos se llama las “Nordic Innovation Houses”, que consiste en oficinas destinadas a colaborar con start-ups nórdicas mediante acciones que alientan la incubación de proyectos innovadores, como espacios de co-working, la construcción comunitaria y las actividades o eventos de networking, promoción comercial en los polos tecnológicos globales (Nordic Innovation, 2020b).

En la actualidad, se han establecido cuatro casas de innovación nórdicas en América del Norte y Asia. La primera casa se abrió en Silicon Valley en 2014, y la segunda en Nueva York en 2017, en el año 2018 se abrieron de dos casas más en Singapur y Hong Kong y se espera abrir una quinta en Tokio, Japón (Nordic Innovation, 2020b).

Se busca que los proyectos busquen dar soluciones a temas vinculados con salud, demografía y calidad de vida, movilidad y conectividad, y transformación empresarial

sostenible en los países nórdicos. A la fecha más de 200 empresas nórdicas han recibido el apoyo Nordic Innovation para conectar stakeholders en los mercados globales (Nordic Innovation, 2020b).

2.2.2. Estonia: Un Departamento de Ciberdiplomacia

Estonia es un pequeño país con poco más de 1.3 millones de habitantes, que ha alcanzado el liderazgo mundial en el gobierno y desarrollo digital. De igual modo, es reconocido como un pionero mundial en ciberseguridad y cuenta con una de las mejores prácticas para ciberseguridad. Su política exterior hacia el ciberespacio es fruto de su visión y desarrollo tecnológico y digital.

En 2007, luego de la reubicación del monumento al Soldado de Bronce de la era soviética, Estonia enfrentó ciberataques que han sido ampliamente reconocidos como la “primera guerra cibernética del mundo”. Actualmente, Estonia se ha convertido en un líder mundial en el conocimiento relacionado a la ciberseguridad, y asesora a muchos otros Estados al respecto.

En el 2008, se creó en Tallin el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, constituyéndose como una organización militar internacional operativamente independiente. Por medio de este Centro y de diplomáticos y especialistas estonios se promocionó la redacción del Manual de Tallin y del Manual del Tallin 2.0., que se centran en la validez del Derecho Internacional en el ciberespacio.

Estonia es considerado una de las naciones más innovadoras del mundo. En el año 2014 estableció la denominada “e-Residencia de Estonia”, que permite a los estonios acceder a diversos servicios gubernamentales como la iniciación y gestión de empresas, el manejo de cuentas y pagos a través de las instituciones bancarias locales, e incluso el ser contribuyente en el propio sistema impositivo local.

Estas innovaciones tienden a redefinir el significado de los Estado-nación en la era digital a medida que se pasa de un “Estado-Nación” a un “país como servicio” (Picron, 2018, p. 6). En ese sentido, la entrada del gobierno de Estonia en el sector de los servicios a partir de datos está abriendo el camino hacia nuevos sistemas de gobierno.

Estonia se ha convertido en el “Silicon Valley de Europa”, existen más de 400 startups, eso implica que posee la mayor proporción de este tipo de empresas en el mundo: 31 startups por cada 100.000 habitantes y ha conseguido tener el mayor número de empresas de unicornios per cápita que cualquier otro país del mundo: Taxify, Skype, Transferwise y

Playtech son empresas privadas valoradas en más de 1.000 millones de dólares (Ballesteros, 2020).

Para Linnar Viik, director de la e-Governance Academy de Estonia “los gobiernos se están dando cuenta de que están perdiendo las identidades digitales de sus ciudadanos ante empresas estadounidenses como Google, Facebook, Amazon y Apple; y se están dando cuenta de que tienen la responsabilidad de proteger la privacidad de estos ciudadanos”(citado por Keen, 2018). Esto podría resultar en una nueva rivalidad entre gobiernos soberanos y las superpotencias privadas de Silicon Valley.

En el 2019, aprovechando ser miembro no permanente del Consejo de Seguridad de las Naciones Unidas, el Ministerio de Relaciones Exteriores creó el Departamento de Ciberdiplomacia. Este Departamento tiene la responsabilidad de contribuir en las discusiones sectoriales en las organizaciones internacionales; promover las relaciones bilaterales y multilaterales, así como supervisar la cooperación para el desarrollo en el campo cibernético y participar en formatos relacionados con la libertad de internet.

La estrategia estonia responde a una mirada integral del ciberespacio, que incluye el acceso a internet como un derecho humano básico. Considera que toda su economía y sociedad depende de la infraestructura digital de alguna forma.

Para la embajadora Heli Tiirmaa-Klaar, quien es la directora del Departamento de Ciberdipomacia, los principios de la ciberdiplomacia estonia se resumen de la siguiente manera:

1. El derecho internacional aplica al comportamiento del Estado en el ciberespacio.
2. Los Estados son responsables de sus actividades en el ciberespacio.
3. Los Estados deben realizar esfuerzos razonables para garantizar que su territorio no se utilice para afectar negativamente los derechos de otros Estados.
4. Los Estados tienen derecho a atribuir las operaciones cibernéticas tanto individual como colectivamente de acuerdo con el derecho internacional.
5. Los Estados tienen derecho a responder a operaciones cibernéticas maliciosas, incluido el uso de medidas diplomáticas, contramedidas y, si es necesario, su derecho inherente a la legítima defensa (citado por Plantera, 2019).

Para la embajadora, lo central de la ciberdiplomacia son las cuestiones que tiene que ver principalmente con el comportamiento del Estado en el ciberespacio y el cumplimiento de las normas cibernéticas, las medidas de fomento de la confianza y el derecho internacional vigente. Por ello, Estonia ha fomentado la cooperación en este campo en la ONU, la UE,

la OTAN, el Consejo de Europa, la OCDE y otras organizaciones internacionales (citado por Plantera, 2019).

La embajadora Heli Tiirmaa-Klaar menciona también que Estonia ha asumido el liderazgo en la discusión sobre el derecho internacional existente y cómo aplicarlo en el ciberespacio. Para ellos, no es necesario crear leyes paralelas para el ciberespacio. Así como los estados deben comportarse de manera responsable en tierra, mar y aire, también deben hacerlo en el ciberespacio. Es otro dominio en el que confiamos cada vez más, y que conlleva su propio nuevo conjunto de complejidades. Por eso es importante estar de acuerdo en que el derecho internacional existente se aplica en el ciberespacio (citado por Plantera, 2019).

3. Marco institucional e intereses peruanos en el ciberespacio

La Cuarta Revolución Industrial trae consigo la masificación de tecnologías disruptivas que impactarán la economía, el trabajo, la educación, la política y las sociedades de cada país. Por ello la adecuada inserción del Perú en este fenómeno es un fundamental para el país y constituye un paso importante para el posicionamiento de este país como una potencia regional emergente (Sandoval, 2019). Dependerá de las acciones tome el país para que sea una oportunidad de desarrollo y se puedan gestionar las consecuencias negativas y las amenazas de una manera adecuada.

Los impactos de los nuevos avances tecnológicos en el ciberespacio son diversos y afectan directamente a los intereses más importantes de los Estados. Al considerar que los impactos la Cuarta Revolución Industrial tiene un impacto total en el país, todos los sectores nacionales deben tener un plan de reforma.

Como se comentó esta nueva revolución industrial tiene tres caras: i) la transnacionalidad, en el sentido de que no respeta fronteras, ii) la expansión simultánea -aunque diferenciada- alrededor del mundo, y iii) impacto multidimensional, pues afecta diversos ámbitos como economía, educación, economía, etc.(Schwab, 2016) Por ello, los esfuerzos nacionales de transformación digital, vistos bajo el prisma de estas tres características, solo serán eficaces si tienen un correlato directo con el accionar en el exterior.

El inicio de la conexión al digital en el Perú se remonta a febrero de 1994, cuando la Red Científica Peruana (RCP) usó satélites y fue brevemente el único proveedor de Internet en el país (Nishiyama, 2019). Desde ese momento se han desarrollado diversas iniciativas para potenciar el uso de las tecnologías digitales.

Un momento importante fue en junio del 2003, cuando se estableció la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información (CODESI), la cual desarrolló el "Plan de Desarrollo de la Sociedad de la Información en el Perú", denominada también, la Agenda Digital Peruana, publicada en el año 2006.

En el año 2011 se aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0". Esta Agenda Digital entiende a las Tecnologías de la Información y de la Comunicación (TIC), no como un fin en sí mismas, sino como un instrumento en la búsqueda de un desarrollo humano más equitativo y sostenible. De igual modo, "tiene como objetivo general, permitir que la sociedad peruana acceda a los beneficios que brinda el desarrollo de las tecnologías de la información y comunicación en todos sus aspectos"(Presidencia del Consejo de Ministros, 2011, p.7).

La formulación de la Agenda responde al esfuerzo que el sector público, el sector privado, la sociedad civil y la academia realizaron por medio de Comisión Multisectorial para el Seguimiento y Evaluación del Plan de Desarrollo de la Sociedad de la Información (CODESI) y se le designo el seguimiento y evaluación (Presidencia del Consejo de Ministros, 2011a).

Los integrantes de esta Comisión se incluyen a representantes de diversos sectores e incluye mesas de trabajo con las empresas, la academia y el sector privado (Presidencia del Consejo de Ministros, 2011a). De igual modo, tiene Grupos de Trabajo sobre Identidad Digital, Ciberseguridad y Agenda Digital. Sin embargo no existe registro de reuniones desde finales del 2017.

A partir de la aprobación del Decreto Supremo N° 022-2017-PCM, se crea la Secretaría de Gobierno Digital – SEGDI como "el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y de Gobierno Electrónico (PCM, 2017). Asimismo, es el órgano rector del Sistema Nacional de Informática y brinda asistencia técnica en la implementación de los procesos de innovación tecnológica para la modernización del Estado en coordinación con la Secretaría de Gestión Pública" (PCM, 2017).

Recientemente, a partir del anuncio en el discurso presidencial del 28 de julio de 2020, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en su calidad de ente rector en materia de gobierno, transformación y confianza digital, se encuentra elaborando la Política y Estrategia Nacional de Transformación Digital, para ello requiere

la participación de otros sectores para establecer las estrategias de un adecuado co-diseño.

Según Marushka Chocobar, Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros (PCM), dicha las estrategias digitales están basada en “impulsar la ciudadanía digital de todos los peruanos a nivel nacional con un enfoque orientado a garantizar el despliegue de la educación digital, el gobierno digital, la economía digital y la conectividad en todas las regiones del país” (citado de Rodriguez, 2020).

Más aún, para la Secretaria de Gobierno Digital para conseguir los objetivos, se considera como habilitadores los siguientes elementos:

“Innovación Digital: Impulso de la digitalización de servicios públicos mediante procesos disruptivos y que prioricen la innovación y diseño centrados en los ciudadanos y con los ciudadanos.

Gobierno de Datos: Los datos son reconocidos como un activo estratégico de las entidades públicas y empresas privadas para diseñar políticas, tomar decisiones, así como crear y entregar servicios digitales. Asimismo, la gestión transparente y ética de los datos se soporta en procesos, roles y estructuras de gobernanza.

Transformación Cultural: Impulso al desarrollo de competencias digitales de los servidores públicos para el despliegue de servicios públicos digitales desde el diseño y el uso de las tecnologías digitales en todos los procesos públicos.

Confianza Digital: Despliegue de acciones y tecnologías para garantizar entornos digitales seguros para los ciudadanos.

Tecnologías transformadoras: Uso y aprovechamiento de la inteligencia artificial, el big data, blockchain, impresión 3D, internet de las cosas y las tecnologías digitales en general al servicio de la población”(citado de Rodriguez, 2020).

Por otra parte, el día 22 de octubre del presente año se presentó la Política Nacional de Transformación Digital. En esta ocasión la señora Chocobar, fue la encargada de presentar el diseño de la política (El Peruano, 2020).

En esa ocasión se mencionó que las aspiraciones de la política se dirigen a un Perú Innovador, un Perú Integro, un Perú Competitivo, un Perú Confiable y un Perú Cercano. Para ello, la política se centra en cinco objetivos estratégicos: (1) garantizar el acceso a Internet de calidad para todos los ciudadanos en todo el territorio nacional, (2) vincular la

economía digital a la reactivación y la competitividad de los procesos productivos del país, (3) desarrollar en la administración pública servicios digitales empáticos con la ciudadanía, (4) fortalecer el talento digital, (5) incentivar la cultura de innovación y una gestión segura, ética e inteligente de las tecnologías digitales y de los datos (TVPerú Noticias, 2020).

En el siguiente apartado, se desarrollarán los intereses peruanos en el ciberespacio, a partir de la herramienta de la ciberdiplomacia y la incidencia en el rol del Ministerio de Relaciones Exteriores.

3.1. La Ciberseguridad en el Perú

Como se mencionó en el capítulo anterior, la ciberseguridad debería ser una prioridad para los Estados. Más allá de la normatividad, la ciberseguridad en el Perú no está suficientemente desarrollada. Según el Índice Global de Ciberseguridad 2018 (GCI – Global Cybersecurity Index), de la Unión Internacional de las Telecomunicaciones, en la que usando 25 indicadores agrupados en 5 pilares, menciona que Perú tiene un nivel bajo en Ciberseguridad y ocupa el puesto 12 de la región latinoamericana y 95 del mundo (ITU, 2019).

En el 2018, la Presidencia del Consejo de Ministros (PCM) remitió el Decreto Supremo Nº 050-2018-PCM que aprueba la definición de ciberseguridad o “Seguridad Digital” de la siguiente manera:

“La Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno”(Presidencia del Consejo de Ministros, 2018a).

Si bien se puede considerar esta definición como un avance, la definición solo incluye los aspectos nacionales y no supone la relación con los demás actores internacionales que participan y afectan en el ciberespacio.

En el 2018, el congreso aprobó el Proyecto de Ley (04237/2018-CR) – Ley que promueve la Seguridad Informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad, pero fue observada por el ejecutivo. Cabe mencionar que En este Proyecto de ley se menciona que los principales objetivos de la ciberseguridad en el Perú y estos no fueron observados por el ejecutivo. Estos objetivos son:

1. Resguardar la seguridad de las personas en el ciberespacio.
2. Proteger la seguridad informática del país.

3. Promover la colaboración y coordinación entre instituciones.
4. Gestionar los riesgos del ciberespacio.
5. Identificación y jerarquización de las infraestructuras críticas de la información.
6. Protección de las infraestructuras críticas de la información.
7. Desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.
8. Establecer relaciones de cooperación en ciberseguridad con otros actores y participar activamente en foros y discusiones internacionales de la materia.
9. Promover el desarrollo de la industria de ciberseguridad y el desarrollo digital del país, dando énfasis en la generación de oferta por parte de la industria local y demanda por parte del sector público en base a los intereses estratégicos del Estado.

Por otra parte, el mencionado proyecto de ley buscaba la conformación de un Consejo Nacional de Ciberseguridad en el marco de las competencias de la Presidencia del Consejo de Ministros y la Secretaría de Gobierno Digital, como ente rector de la materia en el país. Este Consejo estaría integrado por 18 entidades y no incluía al Ministerio de Relaciones Exteriores.

Por medio del Decreto Legislativo 1412 (2018), mediante el cual se aprueba la Ley de Gobierno Digital. En este decreto, se elabora el Marco de Seguridad Digital del Estado Peruano a partir de los siguientes ámbitos:

a. “Defensa: El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa.

b. Inteligencia: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.

c. Justicia: El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. Institucional: Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI)”(Presidencia del Consejo de Ministros, 2018b).

En enero del 2020, mediante el Decreto de Urgencia Nº 006-2020, se creó el Sistema Nacional de Transformación Digital, conformado por un conjunto de principios, normas, procedimientos, técnicas e instrumentos mediante los cuales se organizan las actividades de la administración pública y se promueven las actividades de las empresas, la sociedad civil y la academia orientadas a alcanzar los objetivos del país en materia de transformación digital.

Por medio de este Decreto de Urgencia, se establecieron los siguientes fines:

1. Fomentar e impulsar la transformación digital de las entidades públicas, las empresas privadas y la sociedad en su conjunto, fortalecer el uso efectivo de las tecnologías digitales, las redes y los servicios digitales por parte de los ciudadanos y personas en general.
2. Impulsar la innovación digital, el fortalecimiento de una sociedad digital inclusiva y el ejercicio de una ciudadanía digital con deberes y derechos digitales de los ciudadanos.
3. Promover la economía digital, la competitividad, productividad e inclusión financiera en una sociedad digital.
4. Fortalecer el acceso y la inclusión a las tecnologías digitales en el país y la confianza digital fomentando la seguridad, transparencia, protección de datos personales y gestión ética de las tecnologías en el entorno digital para la sostenibilidad, prosperidad y bienestar social y económico del país.

Bajo este Decreto, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector del Sistema Nacional de Transformación Digital, y el Ministerio de Relaciones Exteriores es uno de los integrantes.

A los pocos días del Decreto de Urgencia antes mencionado se aprobó el Decreto de Urgencia Nº 007-2020, por el que se establece el Marco de Confianza Digital y dispone medidas para aumentar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

En este Decreto de Urgencia, se menciona la necesidad de que se coordine con el Ministerio de Relaciones Exteriores las acciones vinculadas a la política exterior que contribuyan a fortalecer la confianza en el entorno digital.

Con esto, se hace patente que la ciberseguridad en el Perú debe ser parte de una estrategia integral y desde una visión amplia, que incluya los asuntos internos, así como las relaciones internacionales con los demás actores que se manifiestan en el ciberespacio.

Desde los objetivos de política exterior del Perú, la ciberseguridad debe tener un énfasis en la protección de la infraestructura crítica, la lucha contra el ciberdelito y la mejora de la competencia en seguridad de la información. El desarrollo legislativo debe garantizar la cooperación internacional y el desarrollo economía digital. En ese sentido el objetivo 8 del mencionado Proyecto de Ley 04237/2018-CR, que se encuentra observado en este momento, son los adecuados y deberían retomarse.

Por otro lado, se debe propiciar una mayor relación con los demás Estados y actores que participan en un ciberespacio que no conoce fronteras. En ese sentido el Perú requiere de cooperación internacional para conocer y acoger las mejores prácticas de ciberseguridad. De igual modo, mediante el intercambio internacional de información de los ciberataques y ciberamenazas es de gran ayuda para anticipar los riesgos.

Como parte de la política exterior, el Perú podría potenciar sus relaciones bilaterales y multilaterales centradas en el ciberespacio, se puede compartir experiencia, promover la confianza mutua, proteger los derechos humanos y las libertades fundamentales en el ciberespacio. Más aún, por medio de la ciberdiplomacia, el Perú podría ampliar sus relaciones con el sector privado, la sociedad civil internacional y los socios académicos a nivel mundial.

Finalmente, se debe considerar que el artículo 3 del Reglamento de Organización y Funciones (ROF) reserva para la Cancillería el ejercicio de un conjunto de funciones rectoras, tales como la formulación, ejecución y evaluación de la Política Exterior, y la representación permanente del Estado en el ámbito internacional. No se debe olvidar que en el ciberespacio se desarrollan acciones, situaciones y acuerdos ejecutados por actores públicos y privados fuera de nuestro territorio, que tienen impacto interno con o sin nuestro consentimiento.

3.2. Economía digital y tecnológica

En el 2006, el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica - CONCYTEC, institución rectora del Sistema Nacional de Ciencia y Tecnología e Innovación Tecnológica - SINACYT presentó el primer Plan Nacional Estratégico de Ciencia, Tecnología e Innovación para la Competitividad y el Desarrollo Humano 2006-2021 del Perú.

En este Plan resalta el objetivo de “promover el desarrollo y la transferencia de innovaciones tecnológicas en las empresas elevando la competitividad productiva y el valor

agregado con criterio de sostenibilidad económica y ambiental" (CONCYTEC, 2006, p.59). Este Plan se mantiene vigente.

Más recientemente en el Plan Nacional de Competitividad y Productividad 2019-2030, se reconocen los intereses nacionales en los cambios tecnológicos por los cuales atraviesa el mundo requieren una transformación digital a lo largo del país. En específico el Objetivo Prioritario 3 menciona "la necesidad de Generar el desarrollo de las capacidades para la innovación, adopción y transferencia de mejoras tecnológicas"(Ministerio de Economía y Finanzas, 2019, p.29).

Para ello, se establecen acciones estratégicas para fortalecer la gobernanza del Sistema Nacional de Ciencia, Tecnología e Innovación Tecnológica (SINACYT) como base para el desarrollo de capacidades, el incremento de la eficacia de la inversión pública y del aceleramiento de los procesos de innovación, absorción tecnológica y digitalización.

Por otro lado, es prioritario el desarrollo del Gobierno Digital, pues se considera un elemento esencial para favorecer una economía digital y tecnológica. La Presidencia del Consejo de Ministros, por medio de la Secretaría de Gobierno Digital publicó en el año 2018 publicó los Lineamientos para la Formulación del Plan de Gobierno Digital – PGD, que serviría como un documento de referencia para que las entidades formulen sus Planes de Gobierno Digitales, a partir de un listado de principios comunes.

De igual modo, en setiembre del 2018 la Presidencia del Consejo de Ministros, por medio de la Secretaría de Gobierno Digital, publicó el Decreto Legislativo N°1412, por medio del cual se aprueba la ley de Gobierno Digital. El objeto de este decreto es "establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno"(Presidencia del Consejo de Ministros, 2018b).

En el 2018 se aprobó el Decreto Supremo N° 118-2018-PCM, que declara de interés nacional el desarrollo de gobierno digital, la innovación y la economía digital con enfoque territorial y crea el Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo.

El Perú tiene el reto de organizar las condiciones que lo permitan insertarse exitosamente y de manera protagónica en la Cuarta Revolución Industrial, a partir del desarrollo de nuevos modelos de producción basados en la economía del conocimiento, dar un fuerte

salto en materia de ciencia y digitalizar su economía como fuente de mayor productividad y de mejor calidad de vida para los ciudadanos y no depender únicamente de la exportación de productos primarios.

Una gran dificultad consiste en la enorme diferencia de desarrollo digital y tecnológico en un mismo país. Por un lado hay casos de desarrollo de software y uso de drones para el sector minero y agroindustrial y por otro lado hay regiones sin acceso a internet. El Perú tiene un acceso a internet cercano al 60% y aun se carece de industria y servicios tecnológicos de calidad (Laureano, 2020).

De igual modo, el Perú gasta el 0,08 % del PBI en investigación y desarrollo, una cifra muy inferior a la de países como Colombia (0,25 %), Chile (0,38 %) y Brasil (1,24 %). En el 2019 el Perú invirtió cerca de 406 millones de dólares en investigación y desarrollo, mientras que un país como Ecuador invirtió 806 millones de dólares (Howmuch, 2020).

Con una población de poco más de 31 millones de personas, Perú tiene el 49% de la población con acceso a Internet, lo que representa poco más de 15 millones de usuarios (Banco Interamericano de Desarrollo, 2020).

En el ámbito nacional existen programas nacionales como StartUp Perú, el cual es una iniciativa del Programa Nacional de Innovación para la Competitividad y Productividad – INNÓVATE PERÚ, del Ministerio de la Producción, que otorga inversiones a startups nacionales. En el año 2019 otorgó aproximadamente $ 13.8 millones de sus inversiones totales casi exclusivamente a nuevas empresas (Mitchell, 2020).

El Perú no cuenta aún con ningún “unicornio tecnológico” y está ubicado en la posición 67 (de 137 puestos) en la promoción de la innovación y el emprendimiento a nivel mundial, según el Global Entrepreneurship Index (BBVA, 2019).

Para los Estados también es importante el desarrollo de las tecnologías para un mejor servicio para a los ciudadanos. En ese sentido, las nuevas tecnologías presentan nuevas oportunidades para un servicio más directo y conveniente a los ciudadanos.

3.3. Gobernanza de internet

Las políticas de Estado definen lineamientos generales que orientan el accionar del Estado en el largo plazo a fin de lograr el bienestar de las personas y el desarrollo sostenible del país. Son el resultado de un consenso alcanzado en el Foro del Acuerdo Nacional en el año 2002 (sociedad civil, Estado y partidos políticos).

El Acuerdo Nacional consiste en 35 Políticas de Estado, las que han sido agrupadas en cuatro ejes temáticos: (i) Democracia y Estado de derecho; (ii) Equidad y justicia social; (iii) Competitividad del país; y (iv) Estado eficiente, transparente y descentralizado. El 24 de Agosto del 2017 se incorporó la Política 35, que hace referencia a una política de sociedad de la información y sociedad del conocimiento.

Lo central del numeral 35, en referencia al gobierno de Internet, es que se establecen los principios nacionales sobre este tema al "impulsar una sociedad de la información hacia una sociedad del conocimiento orientada al desarrollo humano integral y sostenible, en base al ejercicio pleno de las libertades y derechos de las personas"(Acuerdo Nacional, 2017). De igual modo, orienta las políticas nacionales hacia un Internet Libre, Internet Abierto, Internet Neutral e Internet para Todos.

El accionar de la política exterior del Perú se asienta sobre la base de lineamientos fundamentales como el respeto de la soberanía y el principio de no intervención en los asuntos internos de los Estados; la promoción de un mayor crecimiento económico con inclusión social y el desarrollo sostenible en la región; la integración de las zonas fronterizas; el fomento de la paz y la seguridad, necesarias para el desarrollo y la erradicación de la pobreza; el respeto de los derechos humanos, la democracia y el Estado de derecho; la lucha contra las amenazas transnacionales y sus delitos conexos; así como la promoción de la solución pacifica de las controversias entre los Estados.

La emergencia del ciberespacio obliga enfrentar el desafío de gestionar sus riesgos a todo nivel, donde el plano internacional reviste particular importancia, considerando el carácter global y transfronterizo del mismo.

Es necesaria la elaboración de una estrategia que apunte a generar una visión país sobre la gobernanza de internet. Esta visión deberá ser integral y deberá incluir las actuales discusiones en torno a la gobernanza de Internet.

El Ministerio de Relaciones Exteriores deberá coordinar con el resto de los ministerios y agencias de gobierno. De igual modo, debe tener el rol de articulador en la comunidad internacional y coordinador internacional para promover la política nacional.

El Perú está llamado a tener una posición de liderazgo en temas de Gobernanza de Internet en la región latinoamericana. Queda pendiente la discusión de temas como el alcance de la regulación de internet, la articulación público-privada para la inversión en infraestructura digital, la producción de contenidos digitales, la persecución de los delitos que se cometan a través de las redes digitales, entre otros. Finalmente, tales discusiones se realizan en un

contexto de una gran diversidad de actores públicos y privados y en el creciente desarrollo de la Cuarta Revolución Industrial.

CAPÍTULO III: EL MINISTERIO DE RELACIONES EXTERIORES Y LA CIBERDIPLOMACIA

1. Marco institucional del Ministerio de Relaciones Exteriores y la Ciberdiplomacia

El Ministerio de Relaciones Exteriores tiene como misión institucional: “Promover, proteger y defender en el sistema internacional los intereses del Estado peruano y los de sus ciudadanos para la consolidación de su desarrollo sostenible e inclusivo” (PEI, 2019, p. 6). La visión que el Ministerio tiene del Perú hacia el 2021 es: “El Perú es una potencia regional emergente, cuya política exterior, sustentada en los valores democráticos y en el Derecho Internacional, lo ha convertido en un actor influyente de América Latina, con proyección a la región de la Cuenca del Pacífico, en el tratamiento de los principales temas de la Agenda Internacional” (PESEM, 2015, p. 25).

En ese sentido, el objetivo estratégico número Nº 1 del Sector Relaciones Exteriores es: “Posicionar al Perú a nivel regional y global, como potencia regional emergente en los ámbitos bilateral y multilateral” (PESEM, 2015, p. 26) y este objetivo indica que el Perú debe “actuar como un referente clave en el espacio latinoamericano y debe procurar avanzar en el cierre de sus brechas internas pendientes, tales como la brecha social, la escasa cobertura y calidad de la educación pública, el déficit de infraestructura, la baja inversión en investigación científica y tecnológica” (PESEM, 2015, p. 26).

Como se mencionó anteriormente, los desarrollos en el ámbito digital y tecnológico tienen un impacto en las dimensiones políticas, sociales y económicas de las naciones. Por ello, en el contexto de la Cuarta Revolución Industrial, se vuelve prioritaria la defensa y promoción de los intereses nacionales en el ciberespacio y esto responde al objetivo estratégico N°1 que acabamos de mencionar.

Más aún, dada la naturaleza transnacional y multidimensional del ciberespacio diluye la relevancia de las fronteras físicas; la importancia de la acción de la Cancillería en este sentido podría ser desarrollar acciones de política exterior en asuntos concernientes a este fenómeno, en atención a los roles y responsabilidades que le competen en el Reglamento de Organización y Funciones.

A diferencia de los términos “diplomacia digital”, “diplomacia en redes” o “network diplomacy” que han sido utilizados en diversos documentos como comunicados institucionales, temas de charlas, artículos de diplomáticos, y ha sido tema de análisis en

diversos trabajos de investigación de la Academia Diplomática del Perú Javier Pérez de Cuéllar, no se encuentra un documento o artículo que desarrolle el término de “ciberdiplomacia”, como uso de las herramientas diplomáticas para defender y promover los intereses nacionales en el ciberespacio.

A pesar de ello, como se verá en las siguientes páginas, el Ministerio de Relaciones Exteriores realiza acciones vinculadas a la defensa de los intereses nacionales en el ciberespacio en diversos ámbitos, foros y organizaciones.

1.1. El MRE y el Convenio de Budapest

El Ministerio de Relaciones Exteriores tuvo un rol sumamente importante en la decisión y proceso de suscripción del Convenio de Budapest sobre Ciberdelincuencia.

Después de la Decisión No. 14 de la Conferencia 1168 de la Comisión Europea celebrada el 10 de abril de 2013, se estableció la posibilidad de invitar a países no miembros a adherirse al Convenio. La invitación fue válida por cinco años a partir de la fecha de adopción.

El Perú pudo, a través de su embajada en Francia, presentar una carta a la Secretaría General de la Comisión Europea el 8 de septiembre de 2014, que incluye la opción de permitir el acceso y una legislación nacional suficiente para cumplir con los requisitos procesales sustantivos relevantes del Convenio. Posteriormente, a partir de la 1220ª sesión celebrada el 18 de febrero de 2015, el Perú fue invitado formalmente a formar parte del Convenio.

Una vez que se recibió la invitación a unirse al Convenio, se debió iniciar el proceso de mejora interna, en este proceso el Ministerio de Relaciones Exteriores jugó un papel muy importante, tanto como órgano rector de los tratados internacionales como guía para las otras entidades de la administración pública para ejecutar los trámites a seguir de manera efectiva y oportuna.

De acuerdo a lo establecido en 6.2.1 y 6.2.2 de la Directiva No. 002-DGT / RE-2013, el primer paso a dar es solicitar opiniones de sectores e instituciones relacionados con la materia del Convenio, para el perfeccionamiento interno (MRE, 2013, p. 4).

La entidad responsable del cumplimiento de la acción de consulta, coordinación y seguimiento del "Convenio de Budapest sobre Ciberdelincuencia " fue la Dirección de Ciencia y Tecnología, que se encuentra en la Dirección General de Asuntos Económicos del Ministerio de Relaciones Exteriores.

Durante el proceso de adhesión, ya varios países en América Latina formaban parte del Convenio de Budapest y el Ministerio de Relaciones Exteriores informó en el mes de junio del 2017 vía Nota Informativa 339-17, que el Perú estaba muy cerca de convertirse en un Estado miembro del Convenio de Budapest contra la Ciberdelincuencia. En la misma descripción, enfatiza que la integración con el protocolo es importante y necesaria porque ayudará a prevenir actos que comprometan la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos, y el abuso:

> "(…) la próxima adhesión de nuestro país al Convenio resulta importante y necesaria, para ayudar a prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como su abuso; garantizando la tipificación como delito de dichos actos, facilitando su detección, investigación y posterior sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación judicial internacional rápida y fiable. (...)La adhesión permitirá al Perú aplicar a programas técnicos y de capacitación sobre Ciberdelincuencia y temas afines. A su vez, se beneficiará de la cooperación entre los países parte del Convenio. Al incorporarnos, nuestro país será pionero en la región latinoamericana en la lucha frontal contra la Ciberdelincuencia. Con ese objetivo, esta Cancillería ha desplegado sus mejores esfuerzos para que la adhesión al Convenio sea realizada de la forma más expeditiva posible, y así lograr que el Perú, y particularmente su sistema judicial, pueda beneficiar a todos los peruanos a través de las herramientas que pone a nuestra disposición el Convenio de Budapest sobre Ciberdelincuencia" (MRE, 2017).

1.2. El MRE en la Organización de las Naciones Unidas

La primera vez que la Naciones Unidas trató el tema de la seguridad de la información fue en 1998 cuando Rusia presentó un proyecto de resolución en la Primera Comisión de la Asamblea General (AG) titulado “Avances en el campo de la informática y telecomunicaciones en el contexto de la seguridad internacional”, aprobado por consenso por la AG (A/RES/53/70)(Naciones Unidas, 2017). Esta Primera Comisión se encarga de ver Desarme y Seguridad Internacional.

La resolución expresa preocupación ante la posibilidad de que estos medios y tecnologías se utilicen con fines incompatibles al objetivo de garantizar la estabilidad y seguridad internacionales y afecten negativamente a los Estados. Asimismo, invitó a los Estados Miembros a emitir opinión respecto a:

a) Problemas de la seguridad de la información;

b) Determinación de criterios sobre la injerencia no autorizada o la utilización ilícita de los sistemas de información y de telecomunicaciones y de los recursos de información;

c) Conveniencia de elaborar principios internacionales que aumenten la seguridad de los sistemas de información y telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información.

En el marco de la Tercera Comisión de la Asamblea General, la cual se ocupa de los asuntos sociales, humanitarios y culturales, Rusia presentó el 2018 y 2019 el proyecto de resolución “La lucha contra el uso de las tecnologías de la información y comunicación con fines delictivos” (A/C.3/74/L.11), por medio de este proyecto se solicitó al Secretario General que recabe las opiniones de los Estados Miembros sobre los problemas que enfrentan en la lucha contra el uso de las TIC con fines delictivos y que presente un informe para examinarlo en su 74° período de sesiones. El Perú, al igual que otros 32 países, votó en abstención.

El 2019, Rusia presentó un proyecto de resolución bajo el mismo título, para establecer un comité intergubernamental de expertos de composición abierta, con representación de todas las regiones, con miras a elaborar una convención internacional comprehensiva sobre la lucha contra el uso de las tecnologías de la información y comunicación con fines delictivos, teniendo en cuenta los instrumentos internacionales existentes y los esfuerzos a nivel nacional, regional e internacional sobre la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos, en particular el trabajo y los resultados del Grupo de Expertos Intergubernamentales de composición abierta para realizar un estudio exhaustivo sobre el delito cibernético (GEI).

Asimismo, este Comité decidió reunirse en agosto de 2020 en Nueva York, a fin de acordar el esquema y las modalidades para sus futuras actividades y presentarlas en la 75ª sesión de la Asamblea General para su consideración y aprobación” (párrafos operativos 2 y 3). Finalmente esta reunión fue pospuesta por la pandemia del coronavirus.

El proyecto fue aprobado por la AG (A/RES/74/247) el Perú mantuvo votó en abstención junto a otros 33 países, de la región: Argentina, Brasil, Costa Rica, Ecuador, El Salvador, Guatemala, México Y Uruguay. Cabe señalar que Argentina, México y Uruguay forman parte del EEG.

1.3. El MRE y el Llamamiento de Paris

El 12 de noviembre del 2018, durante la reunión del Foro para la Gobernanza de Internet (FGI) en la sede de la UNESCO, el presidente Macron lanzó el Llamamiento de París para la confianza y la seguridad en el ciberespacio.

Aquellos que se suman a esta iniciativa se comprometen a trabajar juntos para fortalecer la capacidad para prevenir y resistir actividades maliciosas en línea; proteger la accesibilidad e integridad de Internet; cooperar para prevenir posibles interferencias con el proceso electoral; combatir conjuntamente las violaciones de propiedad intelectual a través de Internet; prevenir la proliferación de programas y tecnologías maliciosos; mejorar seguridad de todos los usuarios en el uso de los productos y servicios digitales; tomar medidas para combatir los ataques de ciber mercenarios y actores no estatales; fortalecer los estándares internacionales relevantes (France Diplomatie, 2018).

En enero del 2019 el Ministerio de Relaciones Exteriores informó que el Gobierno del Perú se ha sumado a su iniciativa “Llamamiento de París, para la confianza y seguridad en el ciberespacio”, luego que la Embajada del Perú en Francia comunicara formalmente al Ministerio de Europa y Asuntos Exteriores de ese país el apoyo peruano a dicho llamado.

La iniciativa busca que “exista una regulación de las actividades en la web, en la que participen no solo Estados; sino también el sector privado y la sociedad civil, dado que el ciberespacio es un lugar de oportunidades, pero también de nuevas amenazas. La ciber criminalidad y el desarrollo de actividades delictivas pueden poner en peligro a las personas y a infraestructuras estratégicas para la vida de los Estados” (Ministerio de Relaciones Exteriores, 2019).

1.4. Los asuntos del ciberespacio en la OEA

La Organización de los Estados Americanos se ha posicionado como una de las principales organizaciones en la agenda de ciberseguridad a nivel regional y ha permitido que varios países de América Latina desarrollen sus políticas nacionales de ciberseguridad (Sequera, 2018, p. 4)

La OEA ha tenido un rol importante, mediante la emisión de declaraciones, lineamientos y recomendaciones, para cooperar con muchos países de la región en el desarrollo de políticas de ciberseguridad.

A partir de la “Declaración sobre Seguridad de las Américas” del año 2003 se reconoce la necesidad de actualizar el sistema de seguridad para que responda a la nueva realidad mundial. Esta Declaración observa que los nuevos problemas de seguridad son de índole

multidimensional y que los desafíos incluyen el terrorismo, el narcotráfico, el crimen organizado, la degradación del medio ambiente, la pobreza, las migraciones, los ciberataques, entre otros. Con esta aproximación, se empieza a reconocer que las nuevas amenazas trascienden las fronteras y el control de los Estados.

En junio del 2004 la OEA, se desarrolla la ciberseguridad en la región a partir de la Resolución denominada “Estrategia Interamericana de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética”.

A través del Comité Interamericano contra el Terrorismo (CICTE) se empieza a trabajar los temas de seguridad digital, y se desarrolla una red de alerta sobre seguridad digital para las Américas. Por medio de esta red se ofrece información actualizada y asesoría a los Estados miembros frente a vulnerabilidades informáticas.

Cabe mencionar que en el caso peruano el Director de Organismos y Política Multilateral del Ministerio de Relaciones Exteriores es el punto de contacto del CICTE.

En el 2012 y como respuesta a la “Declaración de Fortalecimiento de la Seguridad Cibernética en las Américas”, el CICTE se consolidó como el ente articulador en la región y como catalizador de programas de capacitación en materia de seguridad digital (Sequera, 2018).

A finales de marzo de 2015, el CICTE aprueba la declaración “Protección de infraestructura crítica ante las amenazas emergentes”. Por medio de esta declaración se refuerza el compromiso de fortalecer la cooperación entre los Estados miembros y se busca la colaboración internacional. Igualmente, se reconoce la interdependencia local, regional y global de las infraestructuras críticas nacionales.

Por otra parte, en la declaración del 2015 se le encomienda un nuevo rol a la Secretaría Ejecutiva del CICTE, pues deberá trabajar en el desarrollo de un proyecto de asistencia técnica que le permita elaborar a los Estados un listado de sus infraestructuras críticas junto con su clasificación, de modo que puedan evaluar de manera efectiva las vulnerabilidades, brechas, amenazas, riesgos e interdependencia.

A comienzos de 2016, el CICTE aprobó la declaración “Fortalecimiento de la cooperación y del desarrollo en la seguridad cibernética y la lucha contra el terrorismo en las Américas”. Con esta declaración se reitera y refuerzan los puntos establecidos en las declaraciones precedentes, se introduce el compromiso de los Estados miembros para generar medidas

de fomento de la confianza, se aumenta la cooperación, la transparencia, la previsibilidad y la estabilidad de los Estados en el uso del ciberespacio, y se busca reducir de esta forma los riesgos de conflicto.

Adicionalmente, se ha creado un Grupo de Trabajo de medidas de fomento de la confianza en Ciberseguridad. El Grupo de Trabajo fue establecido en el año 2017, a partir de una propuesta presentada en la OEA por Chile, Colombia, Perú, Costa Rica, Canadá, Guatemala y México.

El mandato del Grupo de Trabajo es elaborar una serie de proyectos de Medidas de Fomento de la Confianza para mejorar la cooperación, la transparencia, la previsibilidad y la estabilidad, y para reducir los riesgos de malinterpretación, escalamiento y conflicto que puedan derivarse del uso de las Tecnologías de información y Comunicación.

1.5. Ciberdiplomacia en APEC

El Foro de Cooperación Económica Asia Pacífico es el principal foro para facilitar el crecimiento económico, la cooperación técnica y económica, la facilitación y liberalización del comercio y las inversiones en la región Asia-Pacífico (APEC, 2020b). A pesar de la competencia entre China y Estados Unidos, que forman parte de este espacio, las áreas de cooperación se han sostenido.

En este Foro se han realizado negociaciones sobre asuntos de la privacidad de los datos temas relacionados a la ciberseguridad. Por medio del APEC Data Privacy Pathfinder, se logra un flujo transfronterizo responsable de información personal dentro de la región de APEC (APEC, 2020a).

En noviembre de 2011, los líderes de APEC emitieron una directiva para implementar el APEC Cross Border Privacy Rules (CBPR) System. Este sistema equilibra el flujo de información y datos a través de las fronteras y, al mismo tiempo, proporciona una protección eficaz a la información personal, esencial para la confianza en el mercado en línea (APEC, 2020a).

En el 2015, por medio del “Marco de Privacidad de APEC”, se abordan las brechas en las políticas y los marcos regulatorios sobre comercio electrónico para garantizar que el libre flujo de información y datos a través de las fronteras, de modo que se pueda proteger de manera efectiva la información personal esencial para la confianza y la confianza en el mercado en línea (APEC, 2020a)

En 2017, los líderes de APEC se comprometieron a trabajar juntos para aprovechar el potencial de Internet y la economía digital y adoptaron la “Hoja de ruta de Internet y

Economía digital de APEC", este instrumento brindará la orientación sobre áreas y acciones clave para facilitar los intercambios tecnológicos y de políticas entre las economías miembros, promueve un crecimiento innovador, inclusivo y sostenible, y busca el cierre de brechas digitales en la región APEC. Se establecen once áreas de trabajo claves:

1. Desarrollo de infraestructura digital

2. Promoción de la interoperabilidad

3. Logro del acceso universal a la banda ancha

4. Desarrollo de marcos de políticas gubernamentales integrales para Internet y la economía digital

5. Promoción de la coherencia y la cooperación de los enfoques normativos que afectan a Internet y la economía digital

6. Promoción de la innovación y la adopción de tecnologías y servicios propicios

7. Aumento de la confianza y la seguridad en el uso de las TIC

8. Facilitar el libre flujo de información y datos para el desarrollo de Internet y la Economía Digital, respetando las leyes y reglamentos nacionales aplicables.

9. Mejora de las medidas de referencia de la economía digital e Internet

10. Mejora de la inclusión de Internet y la economía digital

11. Facilitación del comercio electrónico y promoción de la cooperación en el comercio digital (APEC, 2017).

En este foro el Perú busca que la digitalización y la innovación beneficien a la vasta mayoría de la población y se debe tener una óptica inclusiva para las MYPES y las mujeres.

1.6. Ciberdiplomacia en la Alianza del Pacífico

La Alianza del Pacífico, un mecanismo de articulación política, económica y de cooperación e integración entre Chile, Colombia, México y Perú, cuyos principales objetivos son construir un área de integración que fomente la libre circulación de bienes, servicios capitales, personas y economía (Alianza del Pacífico, 2012).

Por medio de esta alianza estratégica se busca el desarrollo económico de los países miembros, y de esa forma, intentar disminuir la desigualdad socioeconómica de los ciudadanos de los países que la conforman.

En el Acuerdo Marco se establece que busca convertirse en una plataforma de articulación política, integración económica y comercial, y proyección al mundo, con énfasis en la región Asia Pacífico (Alianza del Pacífico, 2012).

Durante la XI Cumbre de la realizada el 1 de julio de 2016 en Puerto Varas, Chile, por mandato presidencial, se conformó el subgrupo de Agenda Digital. Posteriormente, en junio de 2017, el subgrupo de Agenda Digital fue constituido como grupo de trabajo para la implementación de las acciones acordadas en la hoja de ruta de la Agenda Digital (Subgrupo de Agenda Digital, 2016).

Este Grupo de Agenda Digital (GAD) tiene como objetivo promover escenarios de coordinación y convergencia entre los cuatro países con el fin de mejorar las condiciones y el desarrollo de los negocios de la economía digital. Asimismo, se encarga de implementar las acciones establecidas en la hoja de ruta con el fin de propender por la construcción de un mercado digital regional(Subgrupo de Agenda Digital, 2016).

Actualmente el grupo trabaja en el desarrollo de actividades específicas en cuatro pilares o ejes de trabajo: Economía Digital; Conectividad Digital; Gobierno Digital y Ecosistema Digital. Cada uno de estos pilares muestra lo central de los intereses que los países miembros reconocen en la digitalización y por en el ciberespacio (Subgrupo de Agenda Digital, 2016).

Son particularmente interesantes el desarrollo que hace la Hoja de Ruta del 2016 en cuanto a Economía Digital, cuando reconoce que la economía digital tiene una importancia cada vez mayor dentro de la economía tradicional, y se convierte en una fuente de crecimiento y desarrollo económico (Subgrupo de Agenda Digital, 2016).

Más aún, reconoce la urgencia de desarrollar una economía digital en la que las TIC sean protagonistas transversales del emprendimiento, crecimiento económico y desarrollo inclusivo. Para ello, señalan la necesidad de avanzar hacia la creación de un mercado digital regional que permita aprovechar economías de escala y de red para competir en un mundo de plataformas globales.

Por otra parte, es particularmente interesante el desarrollo que la Hoja de Ruta del 2016 realiza sobre el pilar de Ecosistema Digital, pues en ella se evidencian los intereses

comunes en torno a la ciberseguridad y en los temas relacionados al gobierno de Internet como neutralidad de la red, protección de la privacidad en el tratamiento de datos personales. Actualmente, está en debate la posibilidad de crear un Grupo específico responsable por el tema de Economías Digitales.

En cuanto a ciberseguridad, la Hoja de Ruta la denomina “seguridad digital” y menciona que se deberá:

> “Promover políticas de seguridad y privacidad de la información de los consumidores entre los países de la Alianza. Establecer coordinaciones a nivel de la Alianza para la definición de estándares técnicos de seguridad y privacidad de la información, así como de protección de datos personales. En la misma línea, se buscará promover políticas de seguridad de los consumidores entre los países de la Alianza y trabajar en la evaluación y fortalecimiento de las estrategias nacionales de seguridad digital por medio de la cooperación entre los CERT/CIRT respectivos”(SGAD, 2016, p.6).

Por otra parte, en cuanto a protección de la privacidad en el tratamiento de datos personales, tema relacionado con la gobernanza de Internet, se menciona que:

> “la regulación relativa a la protección de datos personales debiera seguir los mejores estándares internacionales alcanzados en la materia. En este sentido, las normativas nacionales debieran propender a considerar estándares de protección de datos que garanticen a los ciudadanos, a los funcionarios públicos, empresas y gobiernos una correcta gestión de estos derechos, permitiendo un equilibrio entre privacidad, recolección, seguridad, tratamiento y gestión de datos para la productividad y resolución de trámites y beneficios para los ciudadanos(SGAD, 2016, p. 6).

1.7. Ciberdiplomacia en la Comunidad Andina

Los temas relacionados al ciberespacio son relativamente recientes en la Comunidad Andina (CAN). En mayo del 2019 el Consejo Presidencial Andino emitió una Declaración Especial en torno al uso de las nuevas tecnologías y el dominio de primer nivel .AMAZON en el que se expresó una profunda preocupación por la reciente decisión de la Junta Directiva ICANN, por la que se viabiliza la delegación del dominio de nivel superior ".Amazon" a la empresa Amazon Inc. en régimen de exclusividad, pese a la oposición de los países miembros de la Organización del Tratado de Cooperación Amazónica (OTCA) y

en contra de la recomendación del propio Comité Consultivo Gubernamental de la ICANN de alcanzar una solución mutuamente aceptable(CAN, 2019).

Más recientemente el 8 de julio del 2020, a través de una reunión virtual, Consejo Presidencial Andino declaró la necesidad de impulsar el comercio entre los Países de la CAN, es necesario desarrollo digital, la innovación y la transformación productiva (CAN, 2020).

De igual modo, expresó la importancia de impulsar una Agenda Digital para la CAN, las actividades relacionadas con la Cuarta Revolución Industrial, las tecnologías de las comunicaciones y la información y las industrias creativas, como herramientas que pueden apalancar la reactivación de los aparatos productivos de la región (CAN, 2020).

Más aún, se busca priorizar a nivel del Comité Andino de Autoridades de Telecomunicaciones (CAATEL) el tratamiento de la gobernanza de internet, especialmente en lo que se refiere a la asignación de los dominios de primer nivel en internet (CAN, 2020).

1.8. El Grupo de Trabajo de la Cuarta Revolución Industrial

En el último tiempo, desde el Ministerio de Relaciones Exteriores se han priorizado los asuntos relacionados con la Cuarta Revolución Industrial. El 7 octubre de 2019, a partir de la Resolución de la Secretaría General RSG 1442-2019, se creó el Grupo de Trabajo de la Cuarta Revolución Industrial (GT-CRI), al cual se le dio la misión de "realizar el seguimiento de los temas concernientes a la problemática de la Cuarta Revolución Industrial, y sentar las bases para la implementación del Observatorio de la Cuarta Revolución Industrial" (Ministerio de Relaciones Exteriores, 2019d). El mandato del Grupo de Trabajo era de un año.

El Grupo de Trabajo está conformado por el(la) señor(a)Viceministro(a), o su representante, quien lo preside; el(la) Director(a) de la Dirección de Estudios y Estrategias de Política Exterior, o su representante, quien actúa como Secretario Técnico; el(la) Director(a) de la Dirección de Negociaciones Económicas Internacionales de la Dirección General para Asuntos Económicos, o su representante; el(la) Director(a) de la Dirección de Cooperación Internacional de la Dirección General para Asuntos Económicos, o su representante; el(la) Director(a) de la Dirección de Ciencia y Tecnología de la Dirección General para Asuntos Económicos, o su representante; el(la) Director(a) de la Dirección de APEC y Foros Especializados de la Dirección General de Asia y Oceanía, o su representante. Después se incorporó también el (la) Director(a) General de la Dirección

General para Asuntos Multilaterales y Globales (Ministerio de Relaciones Exteriores, 2019d).

El día 16 de julio del 2020, durante el discurso de presentación del embajador Mario López Chávarri como nuevo ministro de Relaciones Exteriores, se expusieron los principales lineamientos de política exterior que guiarán su gestión ministerial. En ese discurso el Canciller mencionó que “en el marco de una estrategia multisectorial y multiactor se impulsará el desarrollo de la innovación, la transformación y la inclusión digital y el desarrollo de aplicaciones en el Perú, mediante una estrategia de acercamiento y cooperación con los principales polos tecnológicos del orbe” (López, 2020a).

En este último tiempo el Consulado Peruano en San Francisco, además de realizar acciones consulares, ha cumplido con labores semejantes a la del “consulado tecnológico” uruguayo en San Francisco, creado recientemente. Por medio de ello, se ha permitido el contacto de algunos grupos y empresas nacionales con las principales empresas de Silicon Valley (López, 2020a).

El 18 de setiembre del 2020, el señor Viceministro aprobó el mandato permanente del GT-CRI y la actualización de su agenda sobre la base de los 7 pilares.

i) Gobernanza Digital Global;
ii) Economía Digital y Transformación Digital;
iii) Ciberseguridad;
iv) Cooperación Internacional;
v) Gobierno Digital;
vi) Ciencia, Tecnología e Innovación;
vii) Sociedad Digital.

Esto permitirá fortalecer su apoyo a los esfuerzos nacionales para la inserción en la Cuarta Revolución Industrial a través del desarrollo de acciones concretas para la promoción de la innovación, la transformación digital y la inclusión digital, de acuerdo a lo contenido en el punto 4 del “Plan de Acciones Prioritarias 2020-2021” de Cancillería(López, 2020b).

De igual modo, se podrán construir acciones de Política Exterior mejor informadas, con base en la comunicación, los aportes y el trabajo del GT-CRI, y ejecutarlas a nivel bilateral, y en espacios regionales y multilaterales importantes como la Alianza del Pacífico, la OCDE, APEC y Naciones Unidas, entre otros.

Más aún, se refuerza el involucramiento de la Cancillería con otros sectores del Estado, el empresariado y academia, comprometidos con los esfuerzos nacionales de transformación digital, aprovechando los diversos interlocutores con los que cada Oficina miembro del GT-CRI interactúa como parte regular de sus actividades.

Esta es una excelente iniciativa, en el ámbito nacional se podrá coordinar estrategias y posturas nacionales con los distintos sectores miembros del Sistema Nacional de Transformación Digital y con los demás sectores involucrados en asuntos del ciberespacio, así como con los especialistas y grupos de la sociedad civil que promueven el uso, el respeto de los derechos y libertades en entornos digitales.

Por otra parte, por medio del Grupo de Trabajo se podrán coordinar objetivos y acciones concretas por medio de los Órganos del Servicio Exterior. En ese sentido, por medio de las embajadas se podrán conocer las experiencias exitosas, las tendencias globales, posiciones en torno a la ciberseguridad y la gobernanza de internet y se podrán organizar encuentros, alianzas que permitan defender y promover los intereses nacionales en torno al ciberespacio.

De igual modo, las Representaciones Permanentes ante los Organismos Internacionales se verán fortalecidas con una postura nacional más clara y podrán gestionar los intereses nacionales en torno al ciberespacio de una manera más propia.

2. Necesidad de una Estrategia y Política Exterior para asuntos del ciberespacio

Por lo visto hasta este momento, existen intereses nacionales por los asuntos en el ciberespacio, el cual incluye un desarrollo de la ciberseguridad, el impulso por la innovación, la transformación y la inclusión digital y el desarrollo de aplicaciones, profundizar una gobernanza de internet y el desarrollo de la economía digital. De igual modo, al ser un asunto trasnacional, es indudable el rol y la actuación del Ministerio de Relaciones Exteriores en estos temas. El Ministerio de Relaciones Exteriores no ha sido ajeno a la defensa y promoción de estos intereses. Sin embargo, no existe aún una política integral sobre este tema.

En este último tiempo, la transformación digital se ha convertido en un asunto prioritario para el Perú y por ende debe serlo también para la política exterior. Como se mencionó en el capítulo anterior, la Secretaría de Gobierno Digital de la Presidencia del Consejo de

Ministros, en su calidad de ente rector en materia de gobierno, transformación y confianza digital, se encuentra elaborando la Política Nacional de Transformación Digital y la Estrategia Nacional de Transformación Digital.

El Ministerio de Relaciones Exteriores es uno de los integrantes del Sistema Nacional de Transformación Digital y, como encargado de formular, coordinar y conducir la política exterior del Estado, esta puede ser una oportunidad para complementar estrategia nacional, mediante el desarrollo de una Política Exterior para los asuntos en el ciberespacio.

Por ello, a partir de las prioridades nacionales y en base a las Políticas y Estrategias Nacionales de Transformación Digital, se recomienda complementar estos esfuerzos y articular una Política Exterior y una Estrategia Exterior para Asuntos del Ciberespacio. Por el actual interés en el tema y por el reciente mandato permanente del Grupo de Trabajo de la Cuarta Revolución Industrial parece ser el momento ideal para plantear esta alternativa.

Para hacer esto, la ciberdiplomacia tendrá un rol primordial, por ello se deberán articular objetivos y acciones concretas en torno a la ciberseguridad, la economía digital y la gobernanza de datos, que deberán gestionarse en los ámbitos bilaterales con los países de la región, con los gobiernos de los países que son los mayores focos tecnológicos en el mundo, y una profundización en los espacios multilaterales y regionales en este tema.

A continuación se mostrarán algunos ámbitos que se consideran deberían ser prioritarios en la Política Exterior y en la Estrategia Exterior.

2.1. Determinación de posturas nacionales en la geopolítica del ciberespacio

El Acuerdo Nacional es una guía para la posición que debe tomar el Perú en diversos escenarios. Como se mencionó anteriormente, por medio del numeral 35 se busca “impulsar una sociedad de la información hacia una sociedad del conocimiento orientada al desarrollo humano integral y sostenible, en base al ejercicio pleno de las libertades y derechos de las personas”(Acuerdo Nacional, 2017).

Sin embargo, uno de los retos más grandes en el ciberespacio es la poca capacidad para regularlo, dentro y fuera del país. Esto genera el libre desarrollo de iniciativas de diversos actores, estatales y privados, con intereses legítimos o ilegítimos. Cada una de esas iniciativas merece una permanente evaluación y toma de postura.

En el marco de la competencia entre China y Estados Unidos por la hegemonía, el ciberespacio se ha convertido en un campo de conflicto y existen propuestas y presión internacional de las grandes potencias, para acomodarse a sus intereses.

Por ello, en base a lo explicado en el capítulo anterior, es necesario definir si el programa “Clean Network”, promovido por la administración Trump, responde a los intereses nacionales o no y, del otro lado, es fundamental evaluar si la "Iniciativa Global Sobre Seguridad de Datos" es conveniente para nuestros intereses y objetivos nacionales.

La fuerza gravitacional que generan estos dos países en términos políticos, dadas sus capacidades militares, de cooperación y económicas -entre otros- en el escenario internacional, permite asumir que los países evalúan con cuidado sus posiciones nacionales respecto a iniciativas de cualquiera de estas dos potencias que puedan colisionar con la otra. Esto se aplica también en el ciberespacio.

En ese sentido, si bien la atracción de las tecnologías necesarias para el desarrollo nacional como la 5G, debe realizarse a partir de criterios técnicos, se considera que la presión política de ambas potencias obligará al Perú a tomar una postura a mediano plazo.

Existen también otros ámbitos en donde la postura nacional debe ser más clara, en concreto en cuanto a las empresas de tecnología. Desde temas de impuestos a las empresas que realizan sus operaciones de manera transnacional, el uso de los datos privados, la privacidad de la información, la neutralidad en la red, los contenidos libres y las excepciones al derecho de autor, así como las reglas que promueven la innovación tecnológica necesitan ser evaluados.

Más allá del poder económico y monopólico de este tipo de empresas, la naturaleza del negocio vinculado a acumulación y procesamiento de información de los usuarios y su influencia social, cultural y política les da a estas empresas un enorme poder y por ello se convierten en un riesgo potencial, y el Perú debe tener la capacidad de sustentar y promover su posición en la comunidad internacional.

En el ámbito nacional se podrá coordinar estrategias y posturas nacionales con los distintos sectores miembros del Sistema Nacional de Transformación Digital y con los demás sectores involucrados en asuntos del ciberespacio, así como con los especialistas y grupos de la sociedad civil que promueven el uso, el respeto de los derechos y libertades en entornos digitales.

Por otra parte, por medio del Grupo de Trabajo de la Cuarta Revolución Industrial se podrán coordinar objetivos y acciones concretas por medio de los Órganos del Servicio Exterior. En ese sentido, por medio de las misiones en el exterior se podrán conocer las experiencias exitosas, las tendencias globales, posiciones en torno a la ciberseguridad y la gobernanza

de internet y se podrán organizar encuentros, alianzas que permitan defender y promover los intereses nacionales en torno al ciberespacio.

De igual modo, las Representaciones Permanentes ante los Organismos Internacionales se verán fortalecidas con una postura nacional más clara y podrán gestionar los intereses nacionales en torno al ciberespacio de una manera más propia.

2.2. El Acuerdo de Economía Digital (DEPA)

Como se mencionó en el capítulo anterior, el 11 de junio del 2020, Nueva Zelandia, Chile y Singapur, firmaron de forma remota y mediante la utilización de la firma digital, el primer Acuerdo de Asociación de Economía Digital (DEPA, por sus siglas en inglés) en el mundo. El Acuerdo está abierto para la adhesión de nuevos miembros una vez que entre en vigor.

El acuerdo representa un hito en la política de negociación comercial y la elaboración de normas globales en la nueva era digital y es pionero porque promueve una economía digital global integrada y señala el camino para la formulación de normas en el futuro.

Por ello será necesario evaluar la pertinencia de adherirse a un acuerdo como ese y, promover este tipo de negociaciones en el futuro.

2.3. La Alianza del Pacífico como espacio prioritario en la Estrategia Política Exterior en asuntos del ciberespacio

La visión 2030 de la Alianza del Pacífico, presentada en julio del 2018, presenta una perspectiva de futuro sumamente interesante ya que, busca generar un área de integración profunda, mediante un mayor crecimiento, desarrollo y competitividad. Por ello, enfoca sus trabajos para alcanzar a ser un área: Más integrada, más global, más conectada y más ciudadana.

En esta visión de futuro la tecnología tiene un rol central, ya que es transversal a los objetivos de la visión 2030. Es por ello que se propone elevar los temas de vinculados a la ciencia y tecnología a un trabajo e bloque en los principales focos tecnológicos del mundo.

Existen cuatro ventajas para gestionar estos temas en bloque y a partir de la Alianza del Pacífico. En primer lugar, la visión al 2030 propone un camino en el que la tecnología tiene un rol central y es transversal a los objetivos para profundizar en el área de integración.

En segundo lugar ya existen las instancias apropiadas para dialogar y proponer acciones coherentes que permitan promover la inserción tecnológica de estos países. En ese sentido, el Grupo de Agenda Digital (GAD) tiene como objetivo promover escenarios de coordinación y convergencia entre los cuatro países con el fin de mejorar las condiciones

y el desarrollo de los negocios de la economía digital. Asimismo, se encargara de implementar las acciones establecidas en la hoja de ruta con el fin de propender por la construcción de un mercado digital regional y grupo trabaja en el desarrollo de actividades específicas en cuatro pilares o ejes de trabajo: Economía Digital; Conectividad Digital; Gobierno Digital y Ecosistema Digital.

En tercer lugar, sin que sea una política exterior común, por medio de la Declaración de Cali del año 2013, se abrió la posibilidad de compartir las sedes diplomáticas, consulares y de promoción comercial. Por ello, a partir de un Plan de Trabajo integral, se podría tener una presencia en todos los focos tecnológicos mundiales y reducir costos.

Se considera que la operación conjunta de sedes diplomáticas no sólo cumple con el propósito de hacer más fuerte la presencia de los países de la Alianza del Pacífico alrededor del mundo, sino que también permite reducir los costos de funcionamiento de estas sedes.

Finalmente, dada la coyuntura mundial en el que los temas de ciencia y tecnología se han vuelto prioritarios, este puede ser un tema que permita nutrir y dinamizar la Alianza del Pacifico.

2.4. Los Agregados de Ciencia, Tecnología e Innovación

Un agregado es normalmente un funcionario, que se desempeña como diplomático o como miembro del personal de apoyo, bajo la autoridad de un embajador u otro jefe de una misión diplomática y se encargan de gestionar los temas relacionados con su área de especialidad e incluso pueden tener responsabilidades especiales incluye a los agregados culturales, militares, policiales, comerciales, marítimos o científico o tecnológico (Ishmael, 2012).

Un agregado científico o tecnológico forma parte de una misión diplomática, y tradicionalmente tiene tres funciones principales: asesorar al embajador en asuntos científicos y técnicos, informar sobre eventos tecnológicos y representar a su país en asuntos tecnológico y técnicos ante el gobierno, las academias extranjeras, la industria, entre otros (Loftness, 1955).

Para S4D4C (“Using Science for/in Diplomacy for addressing global Challenges”), un proyecto de la Unión Europea para el fomento de la diplomacia científica, un agregado científico o tecnológico tiene la responsabilidad de actuar de enlace en temas de ciencia, investigación, tecnología e innovación con el Estado receptor, así como con la comunidad científica, la academia y la industria tecnológica local (S4D4C, 2020).

En el Perú, según la Resolución Ministerial N° 1072-RE, 13/11/2015 en la que se aprueba el Manual de Clasificación de Cargos del Ministerio de Relaciones Exteriores, presentado por la Oficina General de Planeamiento y Presupuesto, existen tres tipos de agregados: el Agregado Económico Comercial, el Agregado Cultural y el Agregado, a cada uno de ellos se les especifica la naturaleza del cargo, sus actividades principales y los requisitos necesarios para el cargo.

Sin embargo, a pesar de la actual premura e importancia de una mayor vinculación a los desarrollos tecnológicos, no existe ordenamiento o desarrollo alguno sobre los cargos de un “Agregado de Ciencia, Tecnología e Innovación”.

Lo fundamental de este cargo consiste en la posibilidad de incorporar a las misiones diplomáticas a especialistas en temas vinculados al ciberespacio, las nuevas tecnologías, innovación, regulación internacional sobre la materia, etc., como sucede en las representaciones de otros países. De este modo, la misión diplomática se verá fortalecida en los conocimientos y capacidades de estos especialistas.

El desarrollo de este puesto podría ser una clave para que, a partir de un especialista en la materia, la apropiada capacitación, el desarrollo de objetivos claros y acciones estratégicas medibles, desde el Ministerio de Relaciones Exteriores se pueda realizar la necesaria vinculación, atracción, análisis y desarrollo de los avances tecnológicos que necesita el país. Por lo que se propone desarrollar y promover ese rol.

En el anexo se muestra una propuesta de desarrollo para este tipo de agregado.

2.5. Capacitación permanente del personal diplomático

Se considera indispensable que el personal diplomático que reciba preparación permanente en temas relacionados a “diplomacia tecnológica”, “ciberdiplomacia” y “diplomacia científica”, así como capacitación en herramientas de gestión para la vinculación. En particular, en cómo reconocer el impacto que las nuevas tecnologías puedan tener en la sociedad y en cómo generar vínculos con la tecnología local.

Más aún la capacitación no solo debe ser desde una perspectiva de Ciencia y Tecnología, sino también desde una perspectiva que demuestre la incidencia del ciberespacio y las nuevas tecnologías en el ejercicio de la labor diplomática en un mundo cada vez más digital, así como en la implicancia geopolítica de este ámbito en las Relaciones Internacionales.

Finalmente, se considera importante evaluar la pertinencia de tener a funcionarios con un mayor grado de especialidad en estos asuntos.

2.6. Reconocimiento y vinculación con las grandes empresas tecnológicas

A partir del reconocimiento de la influencia que las grandes empresas tecnológicas tienen en el ciberespacio, expuestas en capítulos anteriores, se propone como parte de la Estrategia de Política Exterior para los asuntos en el ciberespacio un mayor relacionamiento con las grandes empresas tecnológicas, como un agente privilegiado en los asuntos del ciberespacio.

Más aún, se requiere establecer una serie de posturas en torno a estos actores. Por un lado, pueden ser extraordinarios aliados para la transformación digital que requiere el país, así como agentes privilegiados de cooperación e inversión. Por otro lado, al ser actores con mucho poder e influencia, son un elemento de riesgo para nuestra sociedad, política y economía.

Por otro lado, al considerar las diversas posiciones de las principales potencias tecnológicas hacia estas empresas, será necesario una constante evaluación individual y conjunta de estos actores, con la finalidad de promover la regulación nacional e internacional que responda a nuestros intereses.

2.7. Defensa y promoción de las empresas tecnológicas nacionales

Como se ha visto a lo largo del presente trabajo, los Estados tienen el interés por promover y defender los intereses de sus empresas tecnológicas nacionales. Esto se debe a que son una vía de generación de riqueza y prosperidad y son consideradas, en gran medida, aliadas estratégicas de los intereses de los gobiernos.

Como parte de las prioridades nacionales en el ámbito del ciberespacio, se vuelve fundamental la promoción de estas empresas en los espacios nacionales y la mayor vinculación en la economía digital global. El desarrollo, la innovación y la vinculación de este tipo de empresas es un elemento clave para la atracción y transformación de tecnologías que necesita el Perú.

Por ello, se considera necesario estudiar el tipo de regulación en el ámbito del ciberespacio que beneficie a las empresas nacionales, les permita competir en un sector sumamente competitivo y monopólico y, permita compartir beneficios políticos, sociales y económicos a la ciudadanía, el gobierno y la Academia.

Como se comentó en capítulos anteriores, el Perú no cuenta aún con ningún “unicornio tecnológico” y está ubicado en la posición 67 (de 137 puestos) en la promoción de la innovación y el emprendimiento a nivel mundial, según el (GIobal Innovation Index, 2019).

Si bien existen algunas iniciativas nacionales respecto a la promoción de este tipo de empresas; al considerar que los principales focos tecnológicos se encuentran en el exterior, los grandes inversionistas son extranjeros, las actuales tecnologías están aún distantes y que la regulación al respecto no se negocia en los ámbitos nacionales, es necesario articular estrategias que contemplen el beneficio de estas empresas.

Cabe mencionar que la importancia del crecimiento de este tipo de empresas no tiene solo consecuencias de beneficio económico, es también una variable importante para los intereses nacionales en temas de ciberseguridad, y gobernanza digital.

3. Estrategia de relacionamiento con las grandes empresas tecnológicas de Silicon Valley

El Perú tiene intereses sumamente relevantes con las grandes empresas tecnológicas más allá de lo relacionado a los temas económicos. Por un lado, lo relacionado a la ciberseguridad tiene una vital importancia, en este ámbito no solo son fundamentales las cuestiones técnicas sobre cómo evitar las penetraciones cibernéticas, sino principalmente políticas sobre las motivaciones de los responsables y cómo limitar esas acciones (Riordan, S. 2019, p. 9). Esto es aplicable a las nuevas tecnologías que usan estas grandes empresas.

Por otra parte, el Perú tiene intereses en el gobierno de Internet, en donde se incluyen temas que como la neutralidad de la red, reglas antimonopolios, contenidos libres, privacidad, libertad de internet, etc. Las grandes empresas tecnológicas, como se ha visto en capítulos anteriores, han empezado a ocupar un rol determinante en estos aspectos.

Como parte del relacionamiento con las grandes empresas tecnológicas, se recomienda priorizar la región de Silicon Valley, localizada en la zona sur del Área de la Bahía de San Francisco, en el norte de California, Estados Unidos. Esta región es considerada la zona más innovadora y es el mayor foco tecnológico del mundo. Además en esta zona están localizadas muchas de las mayores corporaciones de tecnología del mundo.

Si bien existen grandes empresas tecnológicas en diversas regiones del mundo, en la actualidad, San Francisco es la sede principal de las empresas tecnológicas más grandes, entre ellas destaca Adobe Systems, Alphabet Inc. (Google), Apple Inc., Cisco Systems,

Facebook, HP Inc., Intel, Netflix, Nvidia, Oracle Corporation y Tesla Motors. Además, el entorno innovador de esa región es de los más dinámicos del mundo, por lo que se puede suponer que en este lugar sucederán los nuevos emprendimientos disruptivos del futuro.

Finalmente, la mayoría de las herramientas tecnológicas usadas por la población y empresas nacionales son aún de origen norteamericano.

No se debe descartar una vinculación semejante en otros polos tecnológicos en el mundo como Seúl (Corea del Sur), Singapur, Tokio (Japón), Hong Kong (China), Shanghái (China), San Francisco (Estados Unidos), Tallin (Estonia), Nueva York (Estados Unidos), Pekín (China), Tel Aviv (Israel).

Por ello, a partir de la experiencia danesa, explicada anteriormente, se considera necesaria una relación más directa y completa con las grandes empresas tecnológicas, como se realizaría en una "embajada tradicional". Se considera que es una oportunidad para concertar posiciones de interés nacional.

La principal característica de esta alternativa es el modelo danés de "oficina tecnológica" que permitiría gestionar de manera integral los intereses y prioridades del Estado con las grandes empresas tecnológicas.

A pesar de las diferencias evidentes entre una relación diplomática entre Estados, la experiencia danesa y el testimonio de sus representantes es que la gestión de intereses ante las grandes empresas tecnológicas no es muy distinta a la de una representación tradicional, práctica y *know-how* de incalculable valor del Ministerio de Relaciones Exteriores.

Esta alternativa sería legalmente factible para el Perú ya que, según la normativa de la Secretaría de Estado de los Estados Unidos se permite crear Oficinas Anexas de la Embajada y los consulados en otras regiones. Una Oficina Comercial es un ejemplo de una Oficina Anexa, pero no es la única posibilidad.

Acogidos a esta legislación se propone a mediano plazo establecer una Oficina Anexa de la embajada peruana en Washington y del consulado localizada en San Francisco.

Más aún, al considerar el bajo nivel de desarrollo digital actual peruano, el incipiente mercado digital nacional y el bajo peso relativo nacional en temas de ciberseguridad y gobierno de Internet, se propone realizar una representación compartida por medio de la Alianza del Pacífico, como ya se realizan en la actualidad por medio de las embajadas compartidas, basándose en la Declaración de Cali del año 2013.

La iniciativa mencionada se relaciona con la importancia de profundizar los vínculos en los intereses digitales y del ciberespacio mencionados anteriormente.

Los cuatro países miembros de la Alianza del Pacífico, México, Colombia, Perú y Chile, con una población conjunta de más de 225 millones de personas, un PBI nominal 2 228 471 millones de dólares, los cuatro países en conjunto conformarían la octava economía mundial; representan el 40% del PBI en América Latina y el Caribe y el 41% del total de la IED; son de las economías más competitivas de la región (Ernst & Young, 2018, p. 7). Además, es una zona con una importante evolución digital, se convierten en un interlocutor interesante para los temas más significativos para las grandes empresas tecnológicas.

Finalmente se considera que la operación conjunta de esta sede no sólo cumpliría con el propósito de hacer más fuerte la presencia de los países de la Alianza del Pacífico alrededor del mundo, sino que también permite reducir los costos de funcionamiento.

En las siguientes páginas se mostrará una posible sucesión de acciones que permitirán articular esta propuesta.

3.1. Primeros pasos: un nuevo funcionario en Consulado General del Perú en San Francisco

A mediano plazo se recomienda nombrar a un funcionario diplomático, y que este sea enviado a servir en Consulado General del Perú en San Francisco, pero que sirva de manera funcional y jerárquica a la embajada peruana en los Estados Unidos. Por lo que, reportará al embajador peruano en Washington.

La primera labor de este diplomático será buscar participar de reuniones con grupos, universidades, inversionistas, empresas tecnológicas, y representaciones de otros países con la finalidad de informar y buscar articular en el campo una estrategia más sólida. La función de este diplomático permitiría complementar la labor que está desarrollando el Consulado General del Perú en San Francisco, sin interferir en la gestión consular.

En paralelo se considera importante articular un equipo de trabajo y un staff o comité de asesores digital compuesto por representantes de otros sectores nacionales vinculados a los intereses prioritarios y especialistas, que puedan trabajar desde sus especialidades en Lima y aconsejar.

Según el artículo 142° del ROF, el Ministerio de Relaciones Exteriores mantiene relaciones de coordinación permanentes con los diferentes sectores nacionales públicos y privados (y la academia), con la finalidad de asegurar la compatibilidad entre los intereses y acciones

de dichos sectores con los objetivos de la política exterior del Estado peruano. (ROF, 2010, p.58).

Este grupo de asesores puede estar conformado por la Secretaría de Gobierno Digital-PCM, el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica-CONCYTEC, el Ministerio de Educación, el Ministerio de Producción y los demás miembros relevantes del Sistema Nacional de Transformación Digital y se considera oportuno que el Grupo de Trabajo de la Cuarta Revolución Industrial, por medio de su mandato permanente podría ser el interlocutor de Cancillería ante este Equipo de asesores digitales.

Además, podrá informar de manera directa de las principales implicaciones de las nuevas tecnologías y de las decisiones que toman las grandes empresas tecnológicas a su jefe funcional, el embajador peruano en Washington, a la Cancillería en Lima, así como en las representaciones permanentes de las Naciones Unidad en donde se ven temas de ciberseguridad y gobierno de internet como en Nueva York, Viena y Ginebra.

3.2. Trabajo desde la Alianza del Pacífico con las grandes empresas tecnológicas en Silicon Valley

En paralelo a las gestiones mencionadas, se debe ir articulando con los demás miembros de la Alianza del Pacífico, iniciativas para privilegiar una mayor relación con las empresas tecnológicas de Silicon Valley.

Como parte del trabajo concreto, se recomienda un viaje y gira de una Comisión de Alto Nivel de la Alianza del Pacífico a las oficinas de un grupo de empresas tecnológicas. De igual modo, se recomienda invitar a representantes de las principales empresas tecnológicas a Cumbres y reuniones especiales en el marco de este foro.

En el plazo de un periodo prudente se deberá buscar establecer una representación compartida, como anexos de sus respectivas embajadas y consulados en la región de San Francisco y, que desde un trabajo como el de una “embajada tradicional”, busque articular temas de interés con las empresas tecnológicas. A semejanza de la “Oficina del Embajador Tecnológico” de los daneses explicada en el capítulo anterior.

Después de consultar a especialistas, se ha confirmado que la Secretaría de Estado de los Estados Unidos de América permite dos tipos de oficinas localizadas en lugares distintos a la misión diplomática o consular: las “Oficinas Anexas” y las “Oficinas Misceláneas”.

Por un lado están las “Oficinas Anexas” que forman parte de la misión diplomática o consular pero se localizan en un espacio geográfico distinto, y sus funcionarios al desempeñar sus cargos gozan de estatus diplomático. Un ejemplo de una “Oficina Anexa”

sería una Oficina Comercial, pero se podría diseñar una oficina con distintas características.

Por otro lado, se encuentran las "Miscellaneous Foreign Government Offices" u Oficinas Misceláneas, que son oficinas que no forman parte de las embajadas o consulados y que realizan funciones no comerciales (US Department of State, 2018, p. 32). Estas oficinas no se rigen por la Convención de Viena sobre Relaciones Diplomáticas o la Convención de Viena sobre Relaciones Consulares. Sin embargo, si son solicitados, pueden tener derecho a ciertos privilegios limitados, en base a la reciprocidad.

En el caso de las oficinas anexas no se requiere contar con una autorización que acredite a los funcionarios diplomáticos, ya que estos dependen directamente de la Embajada o del Consulado correspondiente. La única obligación es la de notificar y registrar formalmente la llegada y el término de funciones de todos los empleados.

Si se contrataran “empleados locales”, estos se regirán bajo la legislación local sobre esta materia. La supervisión de las tareas y la responsabilidad en última instancia en caso de surgir alguna controversia de índole laboral o civil recaería en la Embajada o el Consulado, según sea el caso.

Para cualquiera de las dos opciones se debe solicitar la autorización para la apertura y establecimiento de la oficina y la Embajada es quien debe solicitar al Departamento de Estado, mediante una Nota Diplomática, la autorización para instalar la Oficina Anexa o la Oficina Miscelánea (US Department of State, 2018).

Las oficinas descritas no son novedad para el Perú. En la actualidad, en Estados Unidos existen cuatro Oficinas Comerciales-OCEX en Los Ángeles, Nueva York, Miami y Houston que son gestionadas por funcionarios del Ministerio de Comercio Exterior y Turismo. Sin embargo, para la Secretaría de Estado de Estados Unidos, estas oficinas son anexos de los consulados y representan simultáneamente a la embajada peruana.

Al observar que según el artículo 74 del Reglamento de Organización y Funciones del Ministerio de Comercio Exterior y Turismo estas oficinas desempeñan funciones de identificación de mercados y de promoción de exportaciones, turismo, imagen país e inversión (MINCETUR, 2015), se considera que dada la pluralidad de intereses y temas a tratar con las empresas tecnológicas, este tipo de representación no sería el adecuado.

Más aún, si se hace un análisis de la experiencia danesa, este país tiene Oficinas Comerciales[1] en diversas partes del mundo, pero han preferido establecer la “Oficina del Embajador Tecnológico” justamente porque las funciones de esta oficina son otras.

Por los criterios y condiciones mencionadas, se recomienda solicitar que la representación sea una Oficina Anexa compartida en el marco de la Alianza del Pacífico, que se denominen “Oficinas Tecnológicas” y que funcionen a semejanza de la “Oficina del Embajador Tecnológico”.

Finalmente se considera que la operación conjunta de esta sede no sólo cumpliría con el propósito de hacer más fuerte la presencia de los países de la Alianza del Pacífico alrededor del mundo, sino que también permite reducir los costos de funcionamiento.

3.3. Centros de Innovación de la Alianza del Pacífico

A partir de la experiencia de los países nórdicos con el proyecto de “Nordic Innovation Houses”, mostrada en el capítulo anterior y, a partir de los intereses en una transformación digital vinculado a la economía digital y tecnológica, se propone para un mediano plazo, la creación centro de innovación en el marco de la Alianza del Pacífico para la región de San Francisco.

Asociado a la representación compartida, se recomienda articular unas oficinas destinadas a colaborar con startups y empresas tecnológicas de los países miembros de la Alianza del Pacífico mediante acciones que alientan la incubación de proyectos innovadores, espacios de co-working, la construcción comunitaria y las actividades o eventos de networking, promoción comercial con las grandes empresas tecnológicas.

De igual modo, a partir de relacionamientos con diversas organizaciones tecnológicas, se podrán gestionar intercambios, proyectos de inversión, becas cooperación que promueva la transformación digital nacional.

Se considera que por el tipo de funciones que ejercería este centro compartido , se debería solicitar al Departamento de Estado la apertura de una Oficina Miscelánea y se debería contratar a personal local capacitado en tecnología e innovación y coordinar con los sectores nacionales.

[1] Estas oficinas son denominadas “Delegaciones Comerciales” y cumplen con funciones semejantes.

CONCLUSIONES

El ciberespacio, en el contexto de la Cuarta Revolución Industrial, representa un nuevo espacio de desarrollo para las naciones y al mismo tiempo constituye una amenaza a su seguridad. En este ámbito se pueden realizar las actividades que siempre se realizaron en la realidad física y se ha convertido en un ámbito fundamental en donde los intereses de los Estados convergen o divergen.

Varios Estados han desarrollado políticas nacionales y exteriores con la finalidad de preservar sus intereses en el ciberespacio y el ejercicio de la diplomacia en este ámbito ha sido recurrente. Al uso de la diplomacia en el ámbito del ciberespacio se le denomina "ciberdiplomacia" y ha sido prioritariamente empleada en temas relacionados a ciberseguridad, economía digital y tecnológica y gobernanza de internet.

En estos escenarios, las grandes empresas tecnológicas han conseguido posicionarse y obtener una enorme influencia global, incluso el modo de relacionarse con los Estados es sumamente novedoso. Las empresas tecnológicas también tienen intereses relacionados a la ciberseguridad, la economía digital y tecnológica y la gobernanza de internet y, dependiendo del tema, pueden converger o divergir.

Las Políticas Nacionales y Exteriores hacia los asuntos del ciberespacio de las principales potencias mundiales demuestran que éste se ha vuelto un espacio de competencia y conflicto en donde ejercer poder. De igual modo, en estas políticas se reconoce la importancia y el rol de las grandes empresas tecnológicas como un actor a contener o impulsar, según sea la temática.

En un escenario geopolítico complejo, algunas potencias han alcanzado cierto liderazgo en asuntos relacionados al ciberespacio y han logrado posicionarse adecuadamente. Más aún, resaltan los casos de Dinamarca y Estonia que, siendo países relativamente pequeños, han alcanzado un elevado nivel de desarrollo en los temas prioritarios relacionados con el ciberespacio. En particular, por su creatividad para relacionarse con las grandes empresas tecnológicas se han convertido en líderes y modelos mundiales.

A pesar de que la posición y desarrollo peruano en los asuntos del ciberespacio es aún muy débil, la reciente iniciativa del Sistema Nacional de Transformación Digital y el anuncio de la Política Nacional de Transformación Digital y de la Estrategia Nacional de Transformación Digital son ocasiones privilegiadas para que Ministerio de Relaciones Exteriores, como encargado de formular, coordinar y conducir la política exterior del Estado pueda promover una Política y Estrategia Exterior para Asuntos del ciberespacio.

En ese sentido, será necesario determinar algunas posturas nacionales en torno a la regulación en el ciberespacio, y sobre la posición de Perú en referencia a las grandes potencias mundiales. De igual modo, al considerar el poder *de facto* de las grandes empresas tecnológicas, es importante establecer una relación más directa con estos actores y promover el tipo de regulación que proteja y promueva nuestros intereses.

De igual modo, es fundamental que todo el personal diplomático conozca de los intereses nacionales en el ciberespacio para que estos puedan ser promovidos y defendidos, por ello se considera necesario que reciban directivas y capacitación permanente al respecto. Más aún, se considera importante que en los focos tecnológicos del mundo exista un perfil de diplomático más especializado en estos temas.

La Alianza del Pacífico pareciera ser la plataforma idónea para potenciar la posición nacional para asuntos del ciberespacio. Este bloque tiene la visión común, las instancias de gestión adecuadas y las posibilidades de compartir espacios físicos, que permitirían potenciar las actividades y las posturas nacionales.

Al considerar que el actual centro tecnológico del mundo se encuentra en San Francisco - California (Estados Unidos) y que las grandes empresas tecnológicas ahí ubicadas siguen siendo las más influyentes para nuestro país, se recomienda priorizar una mayor presencia nacional en esa zona, como opción de promoción y defensa de los intereses nacionales en el ciberespacio.

BIBLIOGRAFÍA

Acosta, M., Yagual Velastegui, A., & Coronel Pérez, V. (2018). Perspectivas De La Economía Digital En Latinoamérica: Caso Ecuador. *3C Empresa : Investigación y Pensamiento Crítico*, *7*(3), 28–43. https://doi.org/10.17993/3cemp.2018.070335.28-43/

Acuerdo Nacional. (2017). *Sociedad de la información y sociedad del conocimiento*. https://www.acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/politicas-de-estado/politicas-de-estado-castellano/iv-estado-eficiente-transparente-y-descentralizado/35-sociedad-de-la-informacion-y-sociedad-del-conocimiento/

Aguirre, R. (2001). *Ciberspacio y comunicacion:nuevas formas de vertebracion social en el sigo XXI*. http://www.biblioteca.org.ar/libros/150717.pdf

Alandete, D. (1 de junio de 2012). Obama ordenó un ataque cibernético contra Irán del que perdió el control. *El País*. Recuperado de: https://elpais.com/internacional/2012/06/01/actualidad/1338572841_317814.html

Alcalde, J. (2009). *La Pugna por un Nuevo Orden Internacional*. 1–68.

Alianza del Pacífico (2012). *Acuerdo Marco de la Alianza del Pacífico*

Álvarez, R. (23 de noviembre de 2018). *El gobierno de EEUU arremete contra Huawei y "aconseja" a los países aliados que no usen sus productos*. Xataka. Recuperado de: https://www.xataka.com/legislacion-y-derechos/gobierno-eeuu-arremete-huawei-aconseja-a-paises-aliados-que-no-usen-sus-productos

APEC. (2017). *APEC Internet and Digital Economy Roadmap*. *November*.

APEC. (2020a). *Digital Economy Steering Group*. APEC. https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group

APEC. (2020b). *Mission Statement*. APEC. https://www.apec.org/About-Us/About-APEC/Mission-Statement

Arcos, E. (18 de enero de 2012). *¿Qué es y cómo funciona la Ley SOPA?, en términos simples y sencillos*. Hipertextual. Recuperado de: https://hipertextual.com/2012/01/que-es-y-como-funciona-la-ley-sopa-en-terminos-simples-y-sencillos

Arteaga, F. (2019). *Capacidades ofensivas, disuasión y ciberdefensa*. Real Instituto Elcano. http://www.realinstitutoelcano.org/wps/portal/riel

Ballesteros, A. (27 de junio de 2020). *Estonia, el nuevo paraíso para startups (Incluso más que Delaware)*. Emprendedores. Recuperado de: https://www.emprendedores.es/casos-de-exito/estonia-el-nuevo-paraiso-para-startups-incluso-mas-que-delaware/

Banco Interamericano de Desarrollo. (2020). *CIBERSEGURIDAD, Riesgos, Avances y el camino a seguir en America Latina y El Caribe.*

Barrinha, A. (2018). Virtual neighbors: Russia and the EU in cyberspace. *Insight Turkey*, *20*(3), 29–41. https://doi.org/10.25253/99.2018203.02

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Barrios, G. (2015). The Ethics of Cyberspace. *Revista de Ciencias Sociales y Humanidades*, *79*, 173–178.

Barrios, M. (2017). *Las disputas geopolíticas de la seguridad en el ciberespacio*. https://rebelion.org/las-disputas-geopoliticas-de-la-seguridad-en-el-ciberespacio/

Bavaresco, A. (2003). La crisis del estado-nación y la teoría de la soberanía en Hegel. *Revista de Pensament i Anàlisi*, 55–80.

BBC. (31 de octubre de 2013). Cómo espía EE.UU., según Snowden. *BBC*. Recuperado de: https://www.bbc.com/mundo/noticias/2013/10/131031_eeuu_nsa_espionaje_tecnicas_az

BBC. (20 de mayo de 2014). El golpe de EE.UU. al espionaje chino: el "robo del siglo XXI." *BBC Mundo*. Recuperado de: https://www.bbc.com/mundo/noticias/2014/05/140519_econonomia_hackers_china_eeuu_lav

BBC. (20 de marzo de 2018). *5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día*. BBC. Recuperado de: https://www.bbc.com/mundo/noticias-43472797

BBC. (18 de julio de 2018). *Multa récord a Google: por qué Europa sancionó al gigante tecnológico con US$5.000 millones*. BBC. Recuperado de: https://www.bbc.com/mundo/noticias-44872301

BBC. (16 de mayo de 2019). *Huawei: así respondió la tecnológica china a la decisión de Donald Trump de cerrarle la puerta del mercado de telecomunicaciones en EE.UU.* BBC. Recuperado de: https://www.bbc.com/mundo/noticias-internacional-48295727

BBC. (29 de julio de 2020). *Amazon, Apple, Facebook y Google: las duras críticas del Congreso de EE.UU. ante el creciente poder de las cuatro mayores empresas tecnológicas*. BBC. Recuperado de: https://www.bbc.com/mundo/noticias-internacional-53562696

BBVA. (4 de enero de 2019). *El "boom" peruano de las "startups."* BBVA. Recuperado de: https://www.bbva.com/es/el-boom-peruano-de-las-startups/

Borda, S. (2013). Estados Unidos o el último Estado hegemónico El poder en la era del ascenso y la consolidación del resto del mundo. *Revista Nueva Sociedad*, *67*(246), 64–77. www.thedailybeast.com/newsweek/2012/04/29/myth-of-decline-u-s-is-stronger-and-

Bozhkov, N. (2020). China ' s Cyber Diplomacy: A Primer. *Digital Dialogue*, *EU Cyber Direct*.

Bulls, H. (2000). The Anarchical Society: A Study of Order in World Politics. In *Internasjonal Politikk* (3rd ed., Vol. 58, Issue 2). palgrave. https://doi.org/10.11375/kokusaiseiji1957.126_199

Buzai, G. (2013). Fronteras en el ciberespacio. El nuevo mapa mundial visto desde Buenos Aires (Argentina). *Cuadernos de Geografía: Revista Colombiana de Geografía*, *23*(2), 85–92. https://doi.org/10.15446/rcdg.v23n2.38088

CAN. (2019). *Declaración especial del Consejo Presidencial Andino sobre uso de nuevas tecnologías y el dominio de primer nivel .Amazon*.

CAN. (2020). *Declaración del Consejo Presidencial Andino*.

Castillo, L. (4 de julio de 2017). *¿Qué es un Unicornio Tecnológico?* Colaborativo. Recuperado de: https://colaborativo.net/todo/ciencia-y-tecnologia/empresa-unicornio/

Champetier de Ribes, V. (2018). *The Full Digital Nation*. Cent Mille Milliards.

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: causes, challenges,

prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5). https://doi.org/10.1002/widm.1211

CMSI. (2008). *¿Por qué una Cumbre sobre la Sociedad de la Información?*

Comisión Económica para a América Latina (CEPAL). (2016). *Horizontes 2030. La igualdad en el centro del desarrollo sostenible. Trigésimo sexto período de sesiones de la CEPAL.* https://doi.org/10.1017/CBO9781107415324.004

Comité Interministerial sobre Ciberseguridad. (2018). *Política Nacional de Ciberseguridad*.

CONCYTEC. (2006). *Plan Nacional Estratégico De Ciencia, Tecnología e Innovaciónpara la Competitividad y el Desarrollo Humano PNCTI 2006-2021*.

Constanza, C. (4 de noviembre de 2017). *ARE THE BATX (BAIDU, ALIBABA, TENCENT AND XIAOMI) THE NEW GAFA?* Innovation Is Everywhere. Recuperado de : https://www.innovationiseverywhere.com/webinar-batx-english/

Cuihong, C. (2018). Global cyber governance: China's contribution and approach. *China Quarterly of International Strategic Studies*, *4*(1), 55–76. https://doi.org/10.1142/S2377740018500069

Danca, D. (2015). Cyber Diplomacy – A New Component of Foreign Policy. *Journal of Law and Administrative Sciences*, *3*.

Dellinger, A. (2019). *How The Biggest Tech Companies Spent Half A Billion Dollars Lobbying Congress*. Forbes.

Deutsche Welle. (11 de julio de 2020). *Francia sigue adelante con "tasa Google", pese a sanciones de EE.UU.* Recuperado de: https://www.dw.com/es/francia-sigue-adelante-con-tasa-google-pese-a-sanciones-de-eeuu/a-54139040

Dobrygowski, D. (11 de setiembre de 2019). *Why Companies Are Forming Cybersecurity Alliances*. Harvard Business Review. Recuperado de: https://hbr.org/2019/09/why-companies-are-forming-cybersecurity-alliances

Easley, R. F., Guo, H., & Krämer, J. (2018). From net neutrality to data neutrality: A techno-economic framework and research agenda. *Information Systems Research*, *29*(2), 253–272. https://doi.org/10.1287/isre.2017.0740

Eissa, G. S., Gastaldi, S., Poczynok, I., & Zacarias Di Tullio, M. E. (2014). *El ciberespacio y sus implicancias en la defensa nacional*. *25*, 181–197. http://sedici.unlp.edu.ar/handle/10915/40210

El Peruano. (22 de octubre de 2020). *Gobierno presenta política nacional de transformación digital.* Recuparado de: https://elperuano.pe/noticia/105772-gobierno-presenta-politica-nacional-de-transformacion-digital

Ernst & Young. (2018). *Guía de Negocios e Inversión de la Alianza del Pacífico*.

Fedele, L., & Fedele, L. (2011). From Basic Maintenance to Advanced Maintenance. *Methodologies and Techniques for Advanced Maintenance*, 63–112. https://doi.org/10.1007/978-0-85729-103-5_5

FMPRC. (1 de marzo de 2017). *International Strategy of Cooperation on Cyberspace*. Recuperado de: http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

FMPRC. (8 de setiembre de 2020). *China Propone "Iniciativa Global Sobre Seguridad de Datos."* FMPRC. Recuperado de: https://www.fmprc.gov.cn/esp/zxxx/t1813441.shtml

Forbes. (11 de febrero de 2019). *Las 10 marcas más valiosas del mundo en 2019*. Forbes2.Recuperado de: https://www.forbes.com.mx/las-10-marcas-mas-valiosas-

del-mundo-en-2019/

France Diplomatie. (2018). *Paris Call for Trust and Security in Cyber-space - Ministry for Europe and Foreign Affairs*. *November*. https://www.diplomatie.gouv.fr/en/french-foreign-policy/united-nations/alliance-for-multilateralism-63158/article/paris-call-for-trust-and-security-in-cyberspace

Francia Diplomacia. (2018). *Francia y la ciberseguridad*. Francia Diplomacia. https://www.diplomatie.gouv.fr/es/politica-exterior/defensa-y-seguridad/ciberseguridad/

García, P. (19 de agosto de 2020). *El Acuerdo de Asociación de Economía Digital, un hito en las negociaciones comerciales*. Más Allá de Las Fronteras. Recuperado de: https://blogs.iadb.org/integracion-comercio/es/el-acuerdo-de-asociacion-de-economia-digital-un-hito-en-las-negociaciones-comerciales/#:~:text=Promoción de Exportaciones-,El Acuerdo de Asociación de Economía Digital,hito en las negociaciones comerciales&te

Garcia Serrano, A. (2017). *Inteligencia Artificial Fundamentos* (2nd ed.). Alfaomega Grupo Editor.

Global Innovation Index. (2019). *Global Innovation Index 2019*. Recuperado de https://www.globalinnovationindex.org/gii-2016-report#

Gispert, B. (3 de agosto de 2020). *El momento de las 'big tech.'* La Vanguardia. Recuperado de: https://www.lavanguardia.com/economia/20200803/482640904680/tecnologicas-big-tech-google-alphabet-apple-facebook-amazon.html

González, M. (20 de diciembre de 2017). *La UE da la razón a los taxistas y dice que Uber es un servicio de transporte*. Xataka. Recuperado de: https://www.xataka.com/legislacion-y-derechos/la-ue-da-la-razon-a-los-taxistas-y-dice-uber-es-un-servicio-de-transporte

Hernández-Leal, E. J., Duque-Méndez, N. D., & Moreno-Cadavid, J. (2017). Big Data: una exploración de investigaciones, tecnologías y casos de aplicación. *TecnoLógicas*, *20*(39), 15–38. https://doi.org/10.22430/22565337.685

Hidalgo, F. (19 de setiembre de 2019). *Un embajador danés para Silicon Valley*. Innovacion.Cl. Recuperado de: http://www.innovacion.cl/2019/09/un-embajador-danes-para-silicon-valley/

Howmuch. (16 de julio de 2020). *Find Out How Much Your Country Spends on Research & Development*. Howmuch.Net.Recuperado de: https://howmuch.net/articles/research-development-spending-by-country

Iglesias, J. P. (9 de agosto de 2020). *Chile en medio de la guerra por el 5G*. La Tercera. Recuperado de: https://www.latercera.com/mundo/noticia/chile-en-medio-de-la-guerra-por-el-5g/35AUIOFX3VBKLNSWWQZBJ355HU/

Innovation, N. (2013). *Nordic Innovation Annual Report 2011*. https://www.diva-portal.org/smash/get/diva2:707229/FULLTEXT01.pdf

Ishmael, O. (2012). *The role of diplimatic attachés*. Notes on Diplomatic Practice. https://odeenishmaeldiplomacy.wordpress.com/2012/10/20/the-role-of-diplomatic-attaches/

ITU. (2017). Abrir Sendas hacia 5G. *ITU News MAGAZINE*, *1020‑4164*, 36. https://www.itu.int/en/itunews/Documents/2017/2017-02/2017_ITUNews02-es.pdf

ITU. (2019). Global Cybersecurity Index 2018. In *Measuring the Digital Transformation*.

Jorge-Ricart, R. (2020). *Empresas tecnológicas y Estados : ¿ policy o política ?* 2–4.

Keen, A. (2018). *advanced e-government? Estonia.* TED. https://ideas.ted.com/where-in-the-world-will-you-find-the-most-advanced-e-government-estonia/

Kissinger, H. (2014). *Orden Mundial* (3 Edición). DEBATE. http://red.pucp.edu.pe/ridei/wp-content/uploads/biblioteca/090705.pdf

Kleinman Ruiz, I. (2019). *“ Computación cuántica : Aplicaciones prácticas que la computación clásica no puede solucionar ” Ignacio Kleinman Ruiz*. *December*, 1–75.

Klynge, C. (22 de enero de 2019). *Why Silicon Valley Demands Diplomats*. Techonomy Exclusive. recuperado de: https://techonomy.com/2019/01/silicon-valley-demands-diplomats/

Kuehl, D. T. (2011). From cyberspace to cyberpower: Defining the problem. *Cyberpower and National Security*, 24–42.

Kurbalija, J. (2016). *Introducción a la Gobernanza de Internet* (DiploFound). http://www.diplomacy.edu

Kurowska, X. (2019). *What does Russia want in cyber diplomacy ? A primer*. *December*. https://eucyberdirect.eu/wp-content/uploads/2019/12/13-kurowska_rif-final.pdf

Larrañaga, P. (14 de febrero de 2019). *Por qué un Ministerio de Inteligencia Artificial no es una idea descabellada*. The Conversation. Recuperado de: https://theconversation.com/por-que-un-ministerio-de-inteligencia-artificial-no-es-una-idea-descabellada-109741

Laureano, J. (2020). *Usuarios de Internet 2020, tecnologías y tendencias: Decisiones en torno a Covid-19*. Asociación de Usuarios de Internet Del Perú. http://www.aui.org.pe/usuarios-de-internet-2020-tecnologias-y-tendencias-decisiones-en-torno-a-covid-19/

Lazar, A. (2013). *Cyberpower, a view into future powers*. Cibersecurity Trends. https://cybersecuritytrends.uk/2017/10/31/cyberpower-a-view-into-future-powers/

Lederman, D. (2014). El emprendimiento en América Latina. In *Banco Mundial* (Vol. 22, Issue 1). https://doi.org/10.7770/cuhso-v22n1-art358

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingenieria de Software*, *3*(4), 161. https://doi.org/10.18294/relais.2015.161-176

Lessig, L. (2002). Las leyes del ciberespacio. *THEMIS: Revista de Derecho*, *44*, 171–179.

Lewis, J. (2016). Experiencias avanzadas en políticas y prácticas de ciberseguridad: Panorama general de Estonia, Israel, República de Corea y Estados Unidos. In *BID*. https://doi.org/http://dx.doi.org/10.18235/0000420#sthash.FZeIoDW6.dpuf

Loftness, R. (1955). Why Science Attachés? *The Science Monthly*, *80*.

López, M. (2020a). *Ceremonia de presentación del embajador Mario López Chávarri como Ministro de Relaciones Exteriores*. MRE. Recuperado de: https://www.youtube.com/watch?v=2BGPF9sLjgw&t=1314s

López, M. (2020b). *Prioridades del Ministerio de Relaciones Exteriores y Acción Diplomática Pos-COVID-19*.Recuperado de: https://www.youtube.com/watch?v=9TPGGO8qLjgw&t=1314s

Lynn, W. J. (2010). Defending a new domain. *Foreign Affairs*, *89*(5), 97–108.

Mateos, J. M. M. (2015). *Aproximación jurídica al Ciberespacio*. *57*, 20.

Mayer-Schonberger, V., & Ramge, T. (2018). A Big Choice for Big Tech. *Foreign Affairs*,

97(5), 48–54.

MINCETUR (2015). *Reglamento de Organización y Funciones del Ministerio de Comercio Exterior y Turismo*

Ministerio de Economía y Finanzas. (2019). *Plan Nacional de la Competitividad y Productividad 2019-2030*. https://www.mef.gob.pe/contenidos/inv_privada/planes/PNIC_2019.pdf

Ministerio de Relaciones Exteriores. (29 de enero de 2019). *Perú se suma al "Llamamiento de París por la confianza y seguridad en el ciberespacio."* Nota Informativa. Recuperado de: https://www.gob.pe/institucion/rree/noticias/24992-peru-se-suma-al-llamamiento-de-paris-por-la-confianza-y-seguridad-en-el-ciberespacio

Ministerio de Relaciones Exteriores. (2020a). *Dirección de Energía, Ciencia y Tecnología e Innovación (DECYTI)*. https://minrel.gob.cl/minrel/site/edic/base/port/tecnologias.html

Ministerio de Relaciones Exteriores. (17 de febrero 2020b). *Inauguración del Consulado General del Uruguay en San Francisco*. Recuperado de: https://www.gub.uy/ministerio-relaciones-exteriores/comunicacion/comunicados/1120-inauguracion-del-consulado-general-del-uruguay-san-francisco

Ministerio de Relaciones Exteriores. (2020c). *Plan estratégico 2015-2020 bases para la política exterior del uruguay presentación*. https://www.gub.uy/ministerio-relaciones-exteriores/sites/ministerio-relaciones-exteriores/files/2018-10/bases%2Bpara%2Bla%2Bpolitica%2Bexterior%2Bdel%2Buruguay.pdf

Ministerio de Relaciones Exteriores. (2020c). RSG N° 1442/RE del 7-10-2019 Creación del Grupo de Trabajo "Grupo de Trabajo de la Cuarta Revolución Industrial"

Ministerio de Relaciones Exteriores de Chile. (2018). *Política Exterior de Chile 2030*. 123.

Ministry of Finance. (2018). *Danish Cyber and Information Security Strategy*. *May*, 53. https://uk.fm.dk/publications/2018/danish-cyber-and-information-security-strategy

Ministryof Foreign Affairs. (2019). *The Global Epicentre for Entrepreneurship and Technology*. Ministry of Foreign Affairs of Denmark. https://thetradecouncil.dk/en/services/innovation/innovation-centre-denmark-silicon-valley

Miranzo, M. (2014). La protección de infraestructuras críticas. *UNISCI Discussion Papers*, *35*(May), 339–352.

Mitchell, G. (12 de febrero de2020). *Peru's startup scene is ready for more*. Techcrunch. Recuperado de: https://techcrunch-com.cdn.ampproject.org/c/s/techcrunch.com/2020/02/12/perus-startup-scene-is-ready-for-more/amp/

Molina, T. (2020). *Techplomacy: El ejemplo danés*. Centro de Estudios Internacionales de la Universidad de Belgrano.

Monasterio, F. (2 de agosto de 2020). *Cómo un aviso en el Diario Oficial abre por fin la puerta al 5G en Chile*. Pauta. Recuperado de: https://www.pauta.cl/ciencia-y-tecnologia/anuncian-una-licitacion-que-incorporara-la-tecnologia-5g-en-chile

Mugica, A. S. (2018). The world order and hegemonic reconfiguration in the 21st century. *Revista Mexicana de Ciencias Politicas y Sociales*, *63*(233), 365–388. https://doi.org/10.22201/fcpys.2448492xe.2018.233.56138

Naciones Unidas. (2017). *Los avances en la informatización y las telecomunicaciones en*

el contexto de la seguridad internacional. Oficina de Asuntos de Desarme. Recuperado de: https://www.un.org/disarmament/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/

Nishiyama, A. (17 de mayo de 2019). *Así era la primera cabina de Internet del Perú*. RPP. Recuperado de: https://rpp.pe/tecnologia/mas-tecnologia/asi-era-la-primera-cabina-de-internet-del-peru-noticia-1051281

Nordic Innovation. (2020a). *About Nordic Innovation*. Recuperado de: https://www.nordicinnovation.org/about-us

Nordic Innovation. (2020b). *Nordic Innovation House*. Recuperado de: https://www.nordicinnovation.org/programs/nordic-innovation-house

Nye, J. (2010). Cyber power. *Belfer Center for Science and International Affairs*, *May*, 182–198. https://doi.org/10.4324/9781315536934

Ontiveros, E., & López, V. (2017). *Economía de los Datos Riqueza 4.0*. www.fundaciontelefonica.com/publicaciones

Pearson, F. (2000). *Relaciones Internacionales: Situación global en el siglo XXI* (4th ed.).

PEI. (2019). Plan Estratégico Institucional 2020-2022. Minsiterio de Relaciones Exteriores. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/351057/PEI_2020-2022_RM__0536-RE-2019.pdf

Pérez de Cuellar, J. (1997). *Manual de Derecho Diplomático* (1st ed.). México D.F., México: Fondo de Cultura Económica.

PESEM. (2015). Plan Estratégico Sectorial Multianual Sector Relaciones Exteriores 2015 – 2021. Ministerio de Relaciones Exteriores. Recuperado de: http://transparencia.rree.gob.pe/index.php/2-planeamiento-y-organizacion/22-planes-y-politicas/222-documentos-de-planificacion/plan-estrategico-sectorialmultianual-pesem/ano-2016/8105-plan-estrategico-sectorial-multianual-delsector-relaciones-exteriores-pesem-2015-2021/file

Picron, A. (2018). L ’ E-stonie : modèle d ’ un état plateforme. In *Institut Sapiens*.

Piketty, T. (2 de noviembre de 2014). La desigualdad asesina la democracia. *El País*. Recuperado de: https://elpais.com/economia/2014/10/31/actualidad/1414757399_744768.html

Plantera, F. (11 de octubre de 2019). *Estonia takes on a major role in cyber diplomacy with a new department for international cooperation*. 1–5. Recuperado de https://e-estonia.com/estonia-cyber-diplomacy-international-cooperation/

Portafolio. (7 de mayo de 2019). *Duque, de gira en Silicon Valley*. Portafolio. Recuperado de: https://www.portafolio.co/economia/gobierno/duque-de-visita-en-silicon-valley-529304

Prado, B. (2018). GEOPOLÍTICA DEL CIBERESPACIO : HACIA EL HEARTLAND. *Geografía y Sistemas de Información Geográfica (GEOSIG)*, *10*, 1–13. http://www.revistageosig.wixsite.com/geosig

Presidencia de Rusia. (2010). *Doctrina militar de la Federación de Rusia*. http://kremlin.ru/supplement/461

Presidencia del Consejo de Ministros. (2011a). *La Agenda Digital 2.0.*

Presidencia del Consejo de Ministros. (2011b). *Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0.*

Presidencia del Consejo de Ministros. (2018a). *Aprueban la definición de Seguridad Digital*

Decreto Supremo que crea el Portal de disposiciones adicionales sobre el software. El Peruano. Recuperado de: https://busquedas.elperuano.pe/normaslegales/aprueban-la-definicion-de-seguridad-digital-en-el-ambito-nac-decreto-supremo-n-050-2018-pcm-1647865-1/

Presidencia del Consejo de Ministros. (2018b). *Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital* (pp. 4–8).

Proyecto de Ley (04237/2018-CR) – *Ley que promueve la Seguridad Informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad* (2019). Recuperado de: https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL0423720190417..pdf

Puente, M. L. (1 de abril de 2018). *Guía para entender la nueva geopolítica del ciberespacio*. Perfil. Recuperado de: https://www.perfil.com/noticias/elobservador/guia-para-entender-la-nueva-geopolitica-del-ciberespacio.phtml

Redondo, B. (1 de febrero de 2019). *Protección de Datos en Estados Unidos: ¿Cómo afecta a tu negocio?* Mailjet. Recuperado de: https://es.mailjet.com/blog/news/noticiasproteccion-de-datos-eeuu/

Reguera Sánchez, J. (2015). Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario | GESI. *Grupo de Estudios En Seguridad Internacional GESI*, 30. http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

Reuters. (23 de julio de 2020). *China iniciará nueva campaña de control de noticias en redes sociales*. Reuters. Recuperado de: https://lta.reuters.com/article/idLTAKCN24O1M3-OUSLT

RICTY. (2018). *El Estado de la Ciencia. Principales Indicadores de Ciencia y Tecnología Iberoamericanos / Interamericanos*. 166.

Rincón, H. (2007). ECONOMÍA DIGITAL : ¿ SE REQUIEREN NUEVOS FUNDAMENTOS TEÓRICOS QUE LA DEFINAN ? *Revista de Administração e Contabilidade Da Unisinos*, *4*(2), 182–191.

Riordan, S. (2019a). *Cyberdiplomacy: Managing Security and Governance Online* (Polity; 1s).

Riordan, S. (2019b). *The Geopolitics of Cyberspace A Diplomatic Perspective* (Brill Rese).

Robayo Acuña, P. V. (2016). La innovación como proceso y su gestión en la organización: una aplicación para el sector gráfico colombiano. *Suma de Negocios*, *7*(16), 125–140. https://doi.org/10.1016/j.sumneg.2016.02.007

Rodriguez, D. (6 de agosto de 2020). *Marushka Chocobar: "El proceso de transformación digital del país se centra en la construcción de una ciudadanía digital para todos los peruanos."* Stakeholders. Recuperado de: https://stakeholders.com.pe/digital/el-proceso-de-transformacion-digital-del-pais-se-centra-en-la-construccion-de-una-ciudadania-digital-para-todos-los-peruanos/

ROF. (2010). Reglamento de Organización y Funciones del Ministerio de Relaciones Exteriores. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/581569/ROF_-_del_Ministerio_de_Relaciones_Exteriores.pdf

Romero, J. J., Dafonte, C., Gòmez, Á., & Penousal, F. J. (2007). Inteligencia Artificial Y

Computación Avanzada. In *Inteligencia Artificial* …. http://fmachado.dei.uc.pt/wp-content/papercite-data/pdf/ms07.pdf#page=9

Romm, T. (10 de noviembre de2016). *Tech companies launch new AI coalition*. Politico. Recuperado de: https://www.politico.com/story/2016/10/tech-companies-launch-new-ai-coalition-229600

Roth, A. (28 de abril de 2019). *Russia's great firewall: is it meant to keep information in – or out?* The Guardian. Recuperado de: https://www.theguardian.com/technology/2019/apr/28/russia-great-firewall-sovereign-internet-bill-keeping-information-in-or-out

Ruppel, E. (2020). *La dura realidad del emprendimiento en una economía global*. OpenMind BBVA. Recuperado de: https://www.bbvaopenmind.com/articulos/dura-realidad-del-emprendimiento-en-economia-global/

S4D4C. (2020). *Scientists working in embassies*. S4D4C. Recuperado de: https://www.s4d4c.eu/topic/2-3-3-science-counsellors-attaches-advisers-and-envoys-in-embassies/

Sandoval, D. (2019). La Cuarta Revolución Industrial en el marco de la competencia entre China y Estados Unidos por la hegemonía. Una propuesta para la Política Exterior del Perú. In *Academia Diplomática del Perú Javier Pérez de Cuéllar* (Vol. 53). https://doi.org/10.1017/CBO9781107415324.004

Satariano, A. (5 de setiembre de 2019). *El primer embajador del mundo para la industria tecnológica*. The New York Times. Recuperado de: https://www.nytimes.com/es/2019/09/05/espanol/ciencia-y-tecnologia/dinamarca-embajador-industria-tecnologica.html

Schwab, K. (2016). *La Cuarta Revolución Industrial* (FEM). DEBATE.

Scitech Diplohub. (2015). *What is Science Diplomacy?* Scitech Diplohub. Recuperado de: http://www.scitechdiplohub.org/what-is-science-diplomacy/

SCRF. (2013). *Fundamentos de la política estatal de la Federación de Rusia en el campo de la seguridad de la información internacional para el período hasta 2020*. http://www.scrf.gov.ru/security/information/document114/

Secretaría General Consejo de la Unión Europea. (2015). Conclusiones del Consejo sobre la ciberdiplomacia. In *Unión Europea*. https://doi.org/10.1017/CBO9781107415324.004

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Public Affairs.

Segal, A. (2020a). China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. *The National Bureau of Asian Research*, *87*, 119–128.

Segal, A. (2020b). *The Geopolitics of Cyberspace*. Council on Foreign Relations. https://www.cfr.org/project/geopolitics-cyberspace

Sepúlveda, G. (20 de marzo de 2019). *Riesgos y amenazas del IoT: ¿A qué nos exponemos?* Blog Nivel 4. Recuperado de: https://blog.nivel4.com/noticias/riesgos-y-amenazas-del-iot-a-que-nos-exponemos/

Sequera, M. (2018). *Derechos Humanos y Seguridad Digital: Una Pareja Perfecta*. Privacy International.

Shalal, A. (4 de julio de 2017). *Germany big target of cyber espionage and attacks: government report*. Reuters. Recuperado de: https://www.reuters.com/article/us-germany-espionage-idUSKBN19P0UC

Sitaraman, G. (2020). Too Big To Prevail. *Foreign Affairs*, *99*(2), 116–126. https://doi.org/10.1108/03074801211245156

STIC. (2019). *Informe Primer Año de Trabajo*. Recuperado de: https://www.ecosisteam.cl/wp-content/uploads/2019/10/Informe-del-Consejo-CTI-Chile-Estados-Unidos-2019.pdf

Suárez, T. (11 de mayo de 2019). *Macron y Zuckerberg abordaron el control sobre los contenidos de odio en redes sociales*. France24. Recuperado de: https://www.france24.com/es/20190511-macron-zuckerberg-estrategias-odio-redes-sociales

Subgrupo de Agenda Digital (SGAD). (2016). *Hoja de ruta Subgrupo Agenda Digital*. Alianza del Pacífico. Recuperado de: https://alianzapacifico.net/?wpdmdl=8783

Subsecretaría de Relaciones Económicas Internacionales. (2020). *¿Qué es el Acuerdo de Asociación de Economía Digital?* Recuperado de: https://www.subrei.gob.cl/landings/depa

The New York Times. (29 de junio de 2020). *All the Companies Quitting Facebook*. The New York Times. Recuperado de: https://www.nytimes.com/2020/06/29/business/dealbook/facebook-boycott-ads.html

TVPerú Noticias. (221 de octubre de 2020). *Presidente participa en la presentación del Diseño de la Política Nacional de Transformación Digital.* Recuperado de: https://www.youtube.com/watch?v=vdhuzi6wSvI&ab_channel=TVPer%C3%BANoticias

UDENRIGSMINISTERIET. (2019). *TechPlomacy (technological-diplomacy)*. Recuperado de: https://techamb.um.dk/en/techplomacy/abouttechplomacy/

US Department of State. (2018). *Accreditation Policy Handbook*. Recuperado de: https://www.state.gov/wp-content/uploads/2019/05/Accreditatio-Handbook.pdf

US Department of State. (2020). *The Clean Network*. Recuperado de: https://www.state.gov/the-clean-network/

Van Raemdonck, N. (2020). *Cyber Diplomacy in Latin America* (Issue EU Cyber Direct). Digital Dialogue.

Vanguardia, L. (28 de abril de 2019). *Sebastián Piñera aterriza en Corea del Sur para visita de Estado de dos días*. La Vanguardia. Recuperado de: https://www.lavanguardia.com/politica/20190428/461915527354/sebastian-pinera-aterriza-en-corea-del-sur-para-visita-de-estado-de-dos-dias.html

von der Leyen, U. (2020). Speech by President von der Leyen at the European Parliament Plenary on. *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/speech_20_941

Watts, S., & Richard, T. (2018). Baseline territorial sovereignty and cyberspace. *Lewis & Clark Law Review*, *22*(3), 803–872.

WEF. (2020). *Centro para la Cuarta Revolución Industrial*. WEF. https://es.weforum.org/focus/centro-para-la-cuarta-revolucion-industrial

WGIG. (2005). *Informe del Grupo de Trabajo sobre el Gobierno de Internet*.

White House. (2011). *International Strategy for Cyberspace*.

Xia, L. (28 de febrero de 2019). *China has 829 mln online users: report*. Xinhuanet. Recuperado de: http://www.xinhuanet.com/english/2019-02/28/c_137857753.htm

Zakrzewska-Bielawska, A. (2010). High Technology Company: Concept, Nature, Characteristics. *Recent Advances in Management, Marketing and Finances*, *1*(1), 93–

98.

Ziolkowski, K. (2013). *Peacetime Regime for State Activities in Cyberspace*. NATO Cooperative Cyber Defence Centre of Excellence.

Zuckerman, M. (1998). Un segundo siglo americano. *Política Exterior*, *12*(65), 145–152. https://doi.org/https://www.jstor.org/stable/20644374

ANEXO

CARGO	AGREGADO E N CIENCIA, TECNOLOGÍA E INNOVACIÓN	CLASIFICACIÓN	EC/SP-ES
NATURALEZA DEL CARGO: Ejecución de actividades especializadas en materia tecnológica en el exterior.			
ACTIVIDADES PRINCIPALES: a) Desarrollar actividades orientadas a promover la cooperación bilateral en el campo de la tecnología en el exterior propiciando la realización de acuerdos bilaterales de intercambio tecnológico. b) Coordinar la implementación de acciones orientadas a incrementar la relación del Perú con el gobierno, las empresas tecnológicas y las universidades. c) Informar y replicar las buenas prácticas sobre vinculación tecnológica de las otras misiones acreditadas en el mismo lugar donde labore. d) Apoyar la realización de encuentros de promoción tecnológica, así como la participación en ferias, reuniones y ponencias especializadas, con la finalidad de conseguir cooperación científica y tecnológica. e) Representar, en coordinación con el Jefe de Misión, al Estado Peruano ante el gobierno, las empresas tecnológicas y las universidades. f) Aconsejar e informar al Jefe de Misión sobre asuntos relacionados a la ciberseguridad y la gobernanza de internet. g) Realizar acciones que busquen vincular las nuevas tecnologías con la industria y las startups nacionales, en coordinación con los demás sectores. h) Promover intercambios, becas y cooperación en temas tecnológicos. i) Promover la atracción y vinculación de la inversión extranjera a los desarrollos tecnológicos nacionales. j) Coordinar con la Dirección de Ciencia y Tecnología de la Dirección General para Asuntos Económicos. k) Capacitación permanente en asuntos de ciencia, tecnología e innovación.			
REQUISITOS: Ser peruano de nacimiento. Destacar en algún conocimiento tecnológico. Obligatorio, título profesional universitario en estudios relacionados a ingenierías, ciencia, tecnología o informática.			