¿ES LA INTERNET UNA HERRAMIENTA USADA POR LOS ACTORES ESTATALES Y NO ESTATALES PARA ALCANZAR SUS INTERESES? LOS CASOS DE COREA DEL NORTE, CHINA, RUSIA E IRÁN

LUIS CARLOS GARCÍA FLÓREZ

CRISTIAN JHOVANY QUITIÁN CASTRILLÓN

INSTITUTO DE ALTOS ESTUDIOS PARA EL DESARROLLO

UNIVERSIDAD EXTERNADO DE COLOMBIA

BOGOTÁ, D.C. 2021

¿Es la Internet una herramienta usada por los actores estatales y no estatales para alcanzar sus intereses? Los casos de Corea del Norte, China, Rusia e Irán

Trabajo de Grado

Presentado como requisito para optar al título de

Magíster

en Análisis de Problemas Políticos, Económicos e Internacionales Contemporáneos

Presentado por:

Luis Carlos García Flórez

Cristian Jhovany Quitián Castrillón

Dirigido por:

Alfonso Soria Mendoza

2021

TABLA DE CONTENIDO

- Introducción……. 4
- Capítulo I: **El ciberespacio ¿Por qué se convierte en un escenario de conflicto para los actores estatales?**..... 17
- **1.1 Ciberataques y Ciberconflictos**…….. 21
- 1.2 Casos de ciberataque……. 24
- 1.2.1 Corea del Norte……...24
- 1.2.2 China……...30
- 1.2.3 Rusia……... 38
- 1.2.4 Irán, Estados Unidos e Israel…….. 45

- Capítulo II: **Actores no estatales en el ciberespacio ¿Cuáles son sus intereses?**..... 52
- **2.1 Noticias falsas**……. 60
- 2.1.1 Noticias falsas sobre Corea del Norte…… 65
- 2.1.2 China y las *fake news*……..72
- 2.1.3 Rusia y la desinformación……. 80
- 2.1.4 Irán, creador y víctima de las noticias falsas…….. 85
- **2.2 Ciberactivismo**……. 91
- 2.2.1 Desafiando al régimen norcoreano……. 94
- 2.2.2 Derechos humanos y democracia en China…… 99
- 2.2.3 Lucha social y política en Rusia……. 104
- 2.2.4 Más libertades en Irán……. 109
- Conclusiones…….116
- Referencias……119

Introducción

El desarrollo de la Internet y los constantes avances tecnológicos de la red, han hecho de esta un espacio en el que todas las personas pueden subir y buscar información a un solo clic. Sin embargo, Internet es más que ello; y para entenderla se debe empezar por conocerla en su sentido más básico; desde su definición misma. La Real Academia Española (RAE), define la palabra Internet, como una "red informática mundial, descentralizada, formada por la conexión directa entre computadores mediante un protocolo especial de comunicación". Otras definiciones del término sugieren que:

> Internet es una gran red internacional de ordenadores (…) una red de redes. Permite, como todas las redes, compartir recursos. Es decir: mediante el ordenador, establecer una comunicación inmediata con cualquier parte del mundo para obtener información sobre un tema que nos interesa, ver los fondos de la Biblioteca del Congreso de los Estados Unidos, o conseguir un programa o un juego determinado para nuestro ordenador. En definitiva: establecer vínculos comunicativos con millones de personas de todo el mundo, bien sea para fines académicos o de investigación, o personales" (De la Cuadra, 1996, p. 35).

Ahora bien, el referirnos a la Internet como una "herramienta" nos lleva a preguntarnos por el significado de ese segundo componente del título. En el sitio web *Lexico* desarrollado por la Universidad de Oxford se define como el "mecanismo o técnica necesarios para desarrollar un trabajo de manera satisfactoria". El vocablo "herramienta" proviene del latín "ferramenta", y también es definido como un "instrumento, simple o complejo que permite la realización de un trabajo" (Definicion.co, 2015).

En el presente escrito al referirnos a la Internet como "herramienta", haremos referencia a la forma en la que la Internet es usada por los actores del sistema internacional como mecanismo o instrumento para atacar a otros y de esa forma conseguir réditos políticos o económicos. Puede ser en política interna para desestabilizar gobiernos o en política externa, cuando ese actor consigue acumular más poder y hacerse más fuerte en la escena internacional.

Por otra parte, cuando mencionamos a los actores estatales y no estatales, debemos empezar por analizar qué es considerado un actor internacional. Si bien las diferentes teorías de relaciones internacionales divergen sobre el tema, pues por ejemplo, desde la perspectiva realista y para autores como Morgenthau (1948), el Estado es el único actor digno para ser considerado dentro del sistema internacional, para efectos del presente escrito se entenderá al actor internacional desde una perspectiva más contemporánea, entendiendo al actor internacional, en palabras de Barbé (2007) como "aquella unidad del sistema internacional (entidad, grupo, individuo) que goza de habilidad para movilizar recursos que le permitan alcanzar sus objetivos, que tiene capacidad para ejercer influencia sobre otros actores del sistema y que goza de cierta autonomía".

Así las cosas, al hablar de actores estatales, nos referiremos al Estado-nación y cuando hablamos de actores no estatales, estaremos refiriéndonos a actores como: 1) las Organizaciones Intergubernamentales, 2) las empresas transnacionales, 3) organizaciones no gubernamentales, 4) los individuos e incluso 5) actores ilegales. No obstante, se hace necesaria una aproximación teórica más profunda que nos permita entender a estos actores, pues entenderlos será de suma importancia para el desarrollo del presente trabajo.

Dicho lo anterior, abordaremos en primer lugar, los actores estatales. En el párrafo anterior se mencionaba incluso que, desde las teorías realistas de las Relaciones Internacionales y en palabras de Morgenthau, este es el único actor "digno" dentro del sistema internacional; lo cual, si bien no será esta la noción sobre la cual se abordarán a los actores internacionales en el presente trabajo, si permite llegar a una conclusión y es que el Estado parece ser el actor internacional más preponderante dentro del Sistema Internacional; tal como lo plantea Calduch (1991):

> La consideración del carácter primario de los estados se debe a dos razones fundamentales. En primer lugar, porque el estado ocupa una posición central, privilegiada e insustituible en relación con los demás grupos sociales, al institucionalizar el poder interior y dominar las relaciones de poder en el contexto internacional. En segundo término, y como consecuencia de lo anterior, los

> estados se convierten en mediadores del protagonismo internacional de todos aquellos grupos sociales que nacen y se desarrollan al amparo del marco jurídico, político, económico y territorial de los estados. En otras palabras, si los estados son los grupos más poderosos, interna e internacionalmente, las demás colectividades sólo podrán actuar de modo significativo en el contexto internacional en la medida en que lo permitan los actores estatales, y dentro de los cauces establecidos por ellos (Calduch, 1991, p.3).

Así las cosas, el Estado, como lo plantea Calduch (1991) es considerado como el actor internacional más importante. Sin embargo, para intentar entenderlo a mayor profundidad también debemos considerar que no todos los Estados son iguales. Barbé (1993) toma de Russett y Starr (1989) que "dada la diferencia existente entre los estados en términos de recursos, capacidades, posibilidades y capacidad para explotar y escoger entre todas esas posibilidades, es inapropiado llamar a todas esas unidades estados". De esta manera, partiendo de la premisa que no todos los Estados cuentan con los mismos recursos, ni cuentan con un mismo poder estructural, el cual, en palabras de Lukes (1985) es la capacidad para establecer y reescribir las reglas que dan forma a la estructura según la propia conveniencia; valdría la pena incluso pensar en que este actor internacional podrá a su vez subdividirse según sus diferentes características.

Barbé (1993) en su artículo *"El Estado como actor internacional: Crisis y consolidación del sistema de Estados"* establece que si bien jurídicamente existe el principio de la igualdad entre los Estados, el cual se refleja en la composición de la Asamblea General de Naciones Unidas; de los Estados se pueden dividir ciertas características que explica a lo largo de su artículo, como lo son: edad, territorio, población, tamaño económico y tamaño militar. Barbé establece que, desde estas características, las diferencias son más que notables, pues tenemos Estados tan grandes como Rusia, pero tan pequeños como el Vaticano, tan ricos como Estados Unidos y tan pobres como muchos Estados africanos. Por lo tanto, es difícil hablar del actor estatal como un igual, ya que son sumamente diferentes y con posibilidades distintas. No obstante, en el presente trabajo se analizará cómo los actores estatales, aun siendo tan diferentes, pueden hacer uso de la Internet para alcanzar sus intereses.

Por otra parte, y como consecuencia de lo anterior, es importante hablar también de los actores no estatales. Basados en el artículo de Trejos (2016), titulado *"Los actores estatales en la sociedad internacional: una aproximación a la diplomacia ciudadana en Colombia"* en donde recoge las definiciones de diferentes autores como Barbé (2008), Jouve (1992) y Merle (1991), se puede entender que, los actores no estatales son aquellas unidades que tienen la posibilidad de movilizar recursos, influenciar otros actores del sistema internacional y que pueden cumplir una función relevante en el escenario internacional. De esta manera, se podría clasificar entre estos a las corporaciones, organizaciones gubernamentales y no gubernamentales, grupos e individuos y entre otros.

> La definición de Barbé (2008) retoma elementos de los franceses Jouve (1992), quien reconoce en el escenario internacional la presencia de actores supraestatales (empresas multinacionales, organizaciones gubernamentales y no gubernamentales internacionales) e infraestatales (Grupos e individuos) y Merle (1991), quien define como actor a toda autoridad, organismo, grupo e inclusive a toda persona con la capacidad de cumplir una función de cierta relevancia en el escenario internacional (Trejos, 2016, p.82).

Ahora bien, también es importante entender, tal como establece Vargas (2014), que los actores no estatales no son nuevos, de hecho, se señalan actores como la Cruz Roja, el cual aparece hacia finales del Siglo XIX. Por otra parte, el mismo autor, recoge las ideas de Badie (2008), Riordan (2005) y Rosenau (1992), para establecer que "desde finales del siglo XX se acaba el monopolio del Estado en las relaciones internacionales y se asiste a un mundo con múltiples centros que crea una proliferación de actores no estatales y una gobernanza por encima de los propios Estados". Por otra parte, Verdes-Montenegro (s.f) señala que los actores no estatales han ganado terreno en la escena internacional y que incluso, estos han ido desplazando a los Estados, pues no siempre estos últimos son los actores principales, ni los únicos en la estructura de poder.

En este orden de ideas, se puede establecer que los actores no estatales, juegan también un rol preponderante en la escena internacional y que incluso, para algunos, estos

pueden tener igual o más trascendencia que algunos Estados. Muñoz (2013) en su artículo "*la influencia de los actores no estatales en el sistema internacional*" concluye que:

> (…) a pesar de ser recientes cobran una importante relevancia e influencia en la escena mundial, en parte debido a la incapacidad de los Estados para actuar ante los intereses de estos actores. Se ha observado que su influencia se evidencia en la mayoría de los campos desde la economía, el medio ambiente hasta la política, en especial en los organismos donde se toman decisiones. Estos actores han sido capaces de ejercer presión para que se determinen las políticas y regulaciones que más conviene a sus intereses (Muñoz, 2013, pág. 110).

De esta manera, será importante analizar en el presente trabajo, cómo los actores no estatales pueden ejercer presión para alcanzar sus intereses, a través del uso de la Internet.

Por otra parte, y con el fin de continuar con la definición de los diferentes términos enmarcados en el título, se deberá entender la palabra "interés". Para Rubén Herrero de Castro (s.f) "desde un punto de vista etimológico, podemos definir interés, como una preocupación natural y/o general, así como tener un derecho objetivo sobre algo". Por otra parte, según la definición del diccionario de la RAE este es "el provecho, utilidad o ganancia que se obtiene de algo".

No obstante, lo anterior no nos dice mucho si intentamos pensar en los posibles intereses de los actores internacionales, como los actores estatales y no estatales. Para tal fin, es importante entender el concepto de interés desde las diferentes teorías de las Relaciones Internacionales, el cual nos puede dar luces, sobre el interés que podría perseguir, por ejemplo, los actores estatales.

Desde el realismo se podría entender que el Estado tiene como interés la acumulación de poder. Igualmente, autores como Morgenthau y Waltz comparten en sus teorías que el principal interés de los Estados es la supervivencia. Por otra parte, desde el liberalismo, se podría entender que los Estados persiguen como interés, la paz y la

armonía entre las naciones, lo cual reposa sobre conceptos como la paz democrática de Kant. Igualmente, desde las teorías constructivistas se podría entender el interés de los Estados como la búsqueda de una identidad nacional.

Por otra parte, los intereses de los actores no estatales pueden ser más heterogéneos, pues pueden variar desde el interés de alguna persona poderosa de influir en asuntos de orden nacional e internacional, como el interés de una ONG en hacer visible un tema de derechos humanos o daño ambiental, hasta el interés de una organización ilegal de lucrarse o influir en decisiones políticas regionales.

Así las cosas, en el presente trabajo al mencionar "intereses" estaremos haciendo referencia a aquel provecho que obtienen los actores estatales y no estatales, usando como herramienta la Internet, que pueden ir desde la acumulación de poder por parte de los Estados hasta el ciberactivismo por parte de algunas organizaciones no gubernamentales.

Asimismo, se hace necesario definir otros términos que serán ampliamente utilizados en el presente trabajo, tales como "ciberespacio", el cual es un dominio que se caracteriza por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de la red (Tech Target, 2021). También definido por la RAE como "el ámbito virtual creado por medios informáticos". En el desarrollo del presente escrito estudiaremos ese campo virtual como un "nuevo" escenario de conflicto.

En ese sentido, los Jefes de Estado y de Gobierno de los Estados que integran la Organización del Tratado del Atlántico Norte (OTAN), en la cumbre celebrada en Varsovia entre el 8 y 9 de julio de 2016, se comprometieron a través del documento *Cyber Defence Pledge*, a que la Alianza se mantenga alerta ante las ciberamenazas para ser capaces de defenderse en el ciberespacio "tal y como ocurre en aire, tierra y mar, reconociendo al ciberespacio como quinto dominio de las operaciones, para reforzar las defensas cibernéticas de las infraestructuras y redes nacionales mediante la defensa colectiva" (Departamento de Seguridad Nacional, Gobierno de España, 2016).

Dicho lo anterior, nos lleva a preguntarnos qué sucede cuando dos o más actores estatales han entrado en una confrontación que se lleva a cabo en el mundo virtual. Cuando eso sucede, estamos en presencia de un ciberconflicto, que no es otra cosa que el uso de medios computacionales, a través de microprocesadores y otras tecnologías asociadas, en el ciberespacio con fines malévolos y/o destructivos para afectar, cambiar o modificar interacciones diplomáticas y militares entre entidades (The Washington Post, 2015).

En tanto, que un ataque cibernético, también conocido como ciberataque, es definido por el Diccionario de Cambridge como un intento ilegal de dañar el sistema informático de alguien o la información que contiene, utilizando la Internet. Para los fines del presente escrito ese "alguien" es un actor estatal o no estatal del sistema internacional. También es definido por el Diccionario Collins como un intento de dañar o interrumpir un sistema informático, u obtener información almacenada en él, al entrar en el sistema sin permiso.

Una expresión que está de moda en los últimos años es *fake news* o noticias falsas, la cual hace referencia a historias engañosas que parecen ser noticias, difundidas en la Internet o utilizando otros medios, generalmente creadas para influir en opiniones políticas o como una broma (Cambridge Dictionary, 2021). En el desarrollo de este trabajo sólo nos referiremos a las noticias falsas difundidas en la Internet y con la finalidad de influir en política y en la escena internacional.

Por otro lado, encontramos el ciberactivismo; también conocido como activismo *web*, activismo *online*, activismo en Internet o activismo digital; que es la "utilización de técnicas de socialización y comunicación a través de Internet para crear, operar y administrar cualquier tipo de activismo. Permite a individuos y organizaciones utilizar las redes sociales y otras tecnologías en línea para alcanzar y reunir seguidores, emitir mensajes y avanzar en una causa o movimiento" (Frontline Defenders, s.f.). El ciberactivismo es realizado por actores no estatales, pero directa o indirectamente tiene repercusión en los actores estatales.

Al escribir sobre noticias falsas o sobre ciberactivismo, es imposible no referirnos a las redes sociales, las cuales, al interior del mundo virtual, son el escenario perfecto para la difusión de la información. Entre ellas encontramos a *Facebook, Twitter, Instagram y Youtube*, solo por mencionar algunas. Pero ¿qué es una red social? Según el Diccionario Panhispánico del Español Jurídico (2020):

> Es el servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o videos, permitiendo que estas comunicaciones sean accesibles de forma inmediata para todos los usuarios de su grupo.

En 1995 nació la que es considerada como la primera red social: *SixDegrees*, la cual permitía poner en contacto a amigos, agrupándolos según el grado de relación que tuvieran y permitía la interacción a través del envío de mensajes (Cuaderno de cultura científica, 2020). En 2001, *SixDegrees* desapareció; pero en 2002 se creó *Friendster*, una red social para amantes de los videojuegos; en 2003 aparecieron *MySpace* y *LinkedIn*, consideradas redes más profesionales y orientadas a empresas; en 2004 vio la luz la que es considerada "la red social por excelencia": *Facebook*, creada por Mark Zuckerberg, que daba la posibilidad a los usuarios de agregar "amigos", subir y comentar fotos, dar *likes* o "me gusta" y publicar "estados". En 2005 sería el turno de *Youtube,* que se convirtió rápidamente en un fenómeno audiovisual, al darle la posibilidad a los usuarios de reproducir toda clase de videos (De la Hera, 2020).

En 2006 nació *Twitter*, una red social que le permite a usuarios publicar mensajes en 140 caracteres, en lo que se conoce como *tweet*, o castellanizado como "tuit", o simplemente "trino". Hoy en día, el impacto de esta red es tal que incluso los medios de comunicación dedican espacios enteros a hablar del impacto que algún *tweet*, tendencia o mención especial ha tenido sobre alguna noticia del momento. En 2010, *Instagram* llegó al mercado, posicionándose rápidamente como la red social fotográfica más popular,

superando a competidores con el mismo formato como *Flickr*. *Instagram* y *Twitter* fueron las pioneras en la popularización de los *hashtags*, con la idea de facilitar a sus usuarios el descubrimiento de fotografías que los demás usuarios compartían sobre un mismo tema, y que no podían llegar a visualizarse de otra manera. Los *hashtags*, también conocidos como "etiquetas" funciona en estas redes sociales con el símbolo numeral (#) seguido de la palabra o frase que se quiere hacer popular (De la Hera, 2020).

Hoy en día el acceso a las redes sociales es muy fácil, cualquier persona que tenga un celular o un computador puede crear una cuenta en *youtube* o *instagram* en cuestión de segundos y replicar la información que ahí percibe. Es por eso que las redes sociales pueden ayudar a que las personas tomen conciencia sobre una problemática global de tipo ambiental, como el cambio climático o la deforestación de nuestros bosques, pero al mismo tiempo, también pueden ayudar a propagar rápidamente historias falsas, como aquellas que buscan desacreditar a un candidato a la presidencia de un Estado.

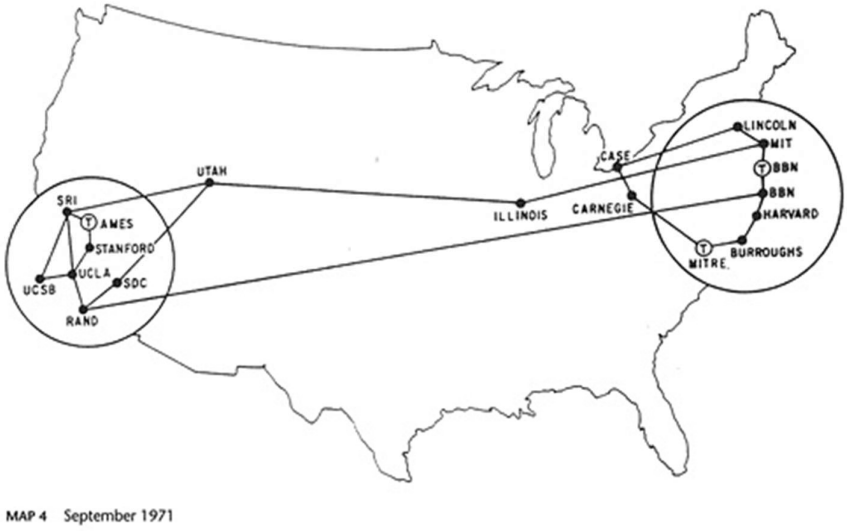
Ahora bien, después de aclarar los términos más relevantes a utilizar, es importante revisar algunos aspectos históricos, particularmente, el origen de la Internet, a fin de entender cómo surgió esta red informática mundial y su evolución. El inicio de la Internet se remonta a la época de la guerra fría, en un escenario bipolar que enfrentaba en todos los frentes a las dos grandes potencias de la época, los Estados Unidos y la Unión Soviética. La carrera tecnológica llevó a la creación por parte del Gobierno norteamericano de ARPA (*Advanced Research Projects Agency*) en 1958.

Según afirma Jessica Petrino (2019), Colaboradora de la Red Federal de Historia de las Relaciones Internacionales del Departamento de Historia de la Universidad Nacional de la Plata, en su artículo "*ARPANET, el "padre" de internet cumple 50 años"*: "Internet es "hija" de la Guerra Fría. Con el lanzamiento del satélite ruso Sputnik – el primer objeto hecho por el ser humano puesto en la órbita de la Tierra – en 1957, Estados Unidos dedicó grandes esfuerzos y recursos para desarrollar nuevas tecnologías de comunicación". Para Petrino, el objetivo de los estadounidenses era crear una red exclusivamente militar para que, en el hipotético caso de un ataque por parte la Unión

Soviética, se pudiera tener acceso a la información de los enemigos desde cualquier punto del país.

El origen de la Internet se remonta a 1969, cuando ARPA logró conectar cuatro sistemas distantes en una red que se denominó ARPANET (A*dvanced Research Projects Agency Network*), cuya misión era mantener las comunicaciones en caso de guerra. "Con ARPANET llegaba una revolución en el campo de las comunicaciones porque era una red que permitía la entrada y salida de conexiones sin que el sistema se viera afectado, y que cualquier usuario pudiera comunicarse con otro desde cualquier parte de la red". Sin embargo, esa red centralizada se consideraba muy insegura en caso de guerra, ya que un solo fallo podría bloquear el sistema (RTVE, 2009). Como se puede observar en el siguiente gráfico, ARPANET tenía 23 puntos conectados en 1971.

Gráfico 1



*Tomado de Universidad Politécnica de Cataluña, Facultad de Informática Barcelona, s.f.

El salto cualitativo de ARPANET se produjo cuando se extendió por el mundo académico. Los científicos la usaron y lograron desarrollarla para compartir opiniones y colaborar en sus trabajos. La red pudo conectar todas las agencias y los proyectos de defensa de Estados Unidos, y en 1972 ya integraba a 50 universidades y centros de

investigación ubicados en diferentes puntos del país. El número de computadores conectados creció, y en las décadas de los 70 y 80 aparecieron otras redes, lo que originó un caos por la variedad de formatos de ordenadores conectados (RTVE, 2009).

Entre las redes que lograron alcanzar cierto protagonismo se destacan: Telenet (1974), versión comercial de ARPANET; Usenet (1979); Bitnet (1981) y Eunet (1982), que unía Reino Unido, Escandinavia y Países Bajos. "En aquel momento el mundo de las redes era un poco caótico, a pesar de que ARPANET seguía siendo el "estándar". En 1982, ARPANET adoptó el protocolo TCP/IP y en aquel momento se creó Internet (*International Network)*" (Universidad Politécnica de Cataluña, s.f.).

En 1989 fue creada la tecnología *World Wide Web* (WWW), que es una red de "sitios" que pueden ser buscados y mostrados con un protocolo llamado *HyperText Transfer Protocol* (HTTP). El concepto de WWW fue diseñado por el ingeniero y físico británico Tim Berners-Lee y algunos científicos del CERN (*Conseil Européen pour la Recherche Nucléaire)* en Ginebra. Estos científicos querían buscar y mostrar fácilmente documentación a través de la Internet. Al principio, el crecimiento en su utilización no fue el esperado, a finales de 1992 solamente había 50 sitios web en el mundo, y en 1993 había 150 (Universidad Politécnica de Cataluña, s.f.).

Pero con la aparición en 1993 del *Mosaic X;* un navegador que resultaba fácil de instalar y de usar, desarrollado por Mark Andreesen, del *National Center for Supercomputing Applications* (NCSA) de Illinois; Se dio una mejora notable en la forma en la que se mostraban los gráficos, ya que era muy parecido a un navegador como los que existen hoy en día. Es por eso, que "a partir de la publicación de la tecnología WWW y de los navegadores se comenzó a abrir Internet a un público más amplio: actividades comerciales, páginas personales, etc. Este crecimiento se aceleró con la aparición de nuevos ordenadores más baratos y potentes" (Universidad Politécnica de Cataluña, s.f.).

Por lo descrito en los párrafos precedentes, podemos decir que la Internet fue concebida, en el escenario de la guerra fría, por el Gobierno estadounidense, desde un principio, con un tinte político. Estados Unidos desarrolló esa incipiente tecnología con

los objetivos de demostrar su superioridad en materia de tecnología a la Unión Soviética y de usarla a su favor en caso de una confrontación bélica contra los soviéticos. La creación de ARPA, órgano del Departamento de Defensa y el posterior desarrollo de ARPANET, dan cuenta de ello.

La evolución de la Internet en las últimas tres décadas ha llevado a tener millones de páginas web, la posibilidad de encontrar información al instante, de hacer negocios, de interactuar con diferentes personas, e infinidad de facilidades que permiten a través de una red global interconectada, acelerar las comunicaciones. Sin embargo, es tal la evolución de esta, que podría ser usada hasta para los fines más impensados, por cualquiera persona y en cualquier momento.

De esta manera, el objetivo principal de este trabajo es intentar dar una respuesta a la interrogante planteada en el título ¿Es la Internet una herramienta usada por los actores estatales y no estatales para alcanzar sus intereses? Si bien el origen de esta herramienta se remonta hacia la década de los 60, como concluye Nebreda (2013) en su tesis titulada *"El origen de Internet. El camino hacia la red de redes",* es importante preguntarnos cómo esta ha ido evolucionando hasta poder ser considerada como un instrumento que utilizan los Estados y los actores no estatales para alcanzar aquello que les interesa, ya sea la desestabilización de un gobierno mediante ataques cibernéticos o defender causas sociales en *Facebook* o *Twitter*, por mencionar ejemplos.

La Internet es un verdadero universo, que desde su creación ha dado paso a un sin número de herramientas virtuales como el correo electrónico o la mensajería instantánea, hasta llegar al día de hoy a las llamadas redes sociales. Tal como cita Navarrete (2014) de Henriquez (2012) "Internet la red, una tela de araña que supera los esquemas del viejo mundo westfaliano, que no conoce fronteras, Estados ni naciones y sobre la que no existen ni cuerpo legal ni gendarmerías".

En consecuencia, en el desarrollo del presente trabajo trataremos de exponer la temática descrita en el título, en el cual la hipótesis que se pretende verificar consiste en demostrar cómo la Internet ha evolucionado al punto de poder ser considerada una

herramienta que utilizan los actores del sistema internacional para alcanzar aquello que les interesa. Por lo tanto, la Internet podría ser usada no solo por los Estados para acumular poder, sino que también podría ser usada por los actores, tanto estatales como no estatales, para desestabilizar gobiernos, influir en elecciones o alcanzar algún otro interés. Para ellos lo dividiremos en dos capítulos.

En una primera parte analizaremos cómo el ciberespacio se ha ido convirtiendo en un escenario de conflicto entre actores estatales y en el segundo capítulo estudiaremos cómo actúan los actores no estatales en el ciberespacio, a partir de dos temáticas particulares como las *fake news* y el ciberactivismo. En ambos capítulos tomaremos como referencia los casos de Corea del Norte, China, Rusia e Irán. Finalmente, se presentarán las conclusiones del tema, que nos ayudarán a establecer si los actores estatales y no estatales utilizan la Internet para alcanzar sus intereses.

Capítulo I

El ciberespacio ¿Por qué se convierte en un escenario de conflicto para los actores estatales?

El desarrollo de la Internet, durante las últimas décadas, ha sido más que frenético. Desde la aparición de la red ARPA, hasta la creación de buscadores, páginas web y redes sociales, que a través de la web pueden operar y han permitido intercomunicar a millones de personas o encontrar cualquier información en cuestión de segundos, hace que el mundo cibernético sea más diverso y complejo de controlar. En una monografía del Ministerio de Defensa del Reino de España, titulada *"Ciberespacio, nuevo escenario de confrontación*" se establece que "en menos de una generación, la informática ha pasado de ser una mera herramienta administrativa que facilitaba los trabajos burocráticos de las oficinas, a constituir por si misma un recurso estratégico nacional para muchas naciones" (De Turiso y Sánchez, 2016, p. 120).

Tal es el caso, que grandes superpotencias, han empezado a estudiar con detenimiento el ciberespacio, hasta el punto de considerarlo como un campo de operaciones. En un artículo de la BBC, Márquez (2011) escribió cómo el ciberespacio era considerado un nuevo "ámbito de guerra" para el pentágono. De esta manera, se describe como para el Departamento de Defensa de los Estados Unidos, el ciberespacio es un campo de operaciones igual a la tierra, mar, aire o espacio y que en este a su vez se pueden llevar a cabo maniobras defensivas y de ser necesario, ataques y represalias. Lo que nos hace inferir que los Estados desde hace ya más de una década, empezaron a observar cómo el ciberespacio podía convertirse en un escenario de conflicto.

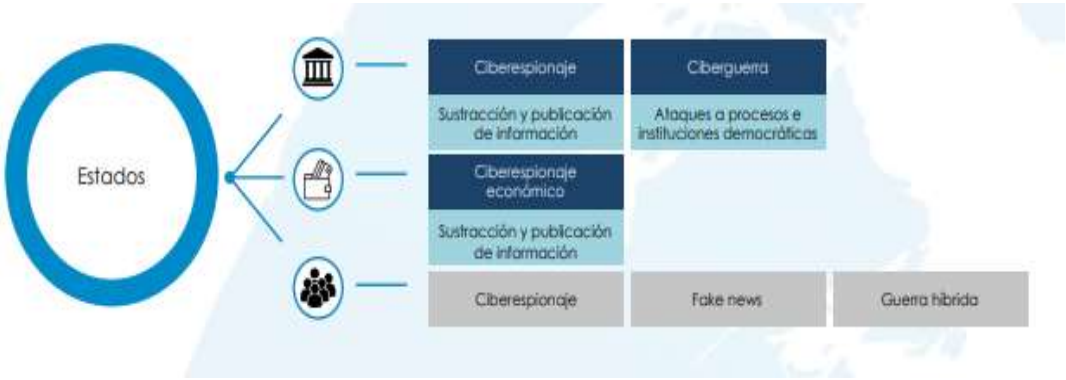
Ahora bien, es importante preguntarnos, si el ciberespacio puede llegar a ser un escenario de conflicto, y en ese caso ¿cuál sería el papel de los actores Estatales en este? Para Gil (2017) los Estados serían el actor principal de los conflictos internacionales.

> Como en las guerras convencionales, serían el actor central y el principal impulsor de los ataques informáticos, utilizando el ciberespacio como un escenario dónde desarrollar los conflictos internacionales. Realizan acciones de espionaje, sabotaje

> o desarrollo de armas cibernéticas, en las que el ciberespionaje, tanto político como industrial, sería la mayor amenaza y lo realizarían los servicios de inteligencia o los departamentos de defensa, con el objetivo de obtener información militar, estratégica o económica (Gil, 2017, Párr. 44).

Así las cosas, lo anterior no solo nos da luces del papel que podrían jugar los actores estatales dentro del ciberespacio, sino también de las herramientas que podrían utilizar para alcanzar sus intereses, que como describía el autor, pueden estar relacionados a la consecución de información militar o económica.

Gráfico 2



*Tomado de CCN-CERT. Ciberamenazas y tendencias 2018.

El gráfico anterior nos muestra cómo los Estados hacen uso del ciberespacio para alcanzar sus intereses. Y es que el origen mismo de la Internet, como ya se describía en párrafos anteriores, buscaba generar una superioridad tecnológica en el marco de la guerra fría que enfrentaba a los Estados Unidos y a la Unión Soviética, pues ahora, el ciberespacio sigue siendo un arma estratégica para llevar diferentes acciones, inclusive de inteligencia militar, como lo es conocer información de un Estado, una entidad o un individuo, como muestra el gráfico. El espionaje se puede llevar a través del ciberespacio y los conflictos ahora pueden llevarse por los actores Estatales a través de la red.

El Centro Criptológico Nacional de España, en 2019, publicó un resumen ejecutivo sobre amenazas en el ciberespacio. En este señala que "los Estados, y los grupos patrocinados por ellos, y sus acciones contra otros países, sus instituciones, empresas y

ciudadanos siguen representando la ciberamenaza más significativa" señala también, que el interés de los actores estatales a través de este tipo de ataques es sustraer información para mejorar su posición estratégica, política, económica o innovadora. Aunque más recientemente se ha evidenciado el interés de usar el ciberespacio para influir en la opinión pública de los países atacados. Esto como veremos, por ejemplo, en el caso de Georgia en 2008.

De igual manera, William J. Lynn III, el subsecretario de Defensa de Estados Unidos, en el Gobierno de Obama, señaló en una entrevista para la BBC, como el ciberespacio se convierte en un escenario de conflicto para los actores estatales, argumentando lo siguiente:

> Los ataques son constantes y están creciendo en frecuencia e intensidad. Pueden destruir estructuras físicas y sistemas operacionales, paralizar ciudades y generar millonarias pérdidas, inclusive costar vidas. Pero los instrumentos de todo este caos no son balas, bombas o tanques; son "bits y bytes" (BBC, 2011. Párr. 1).

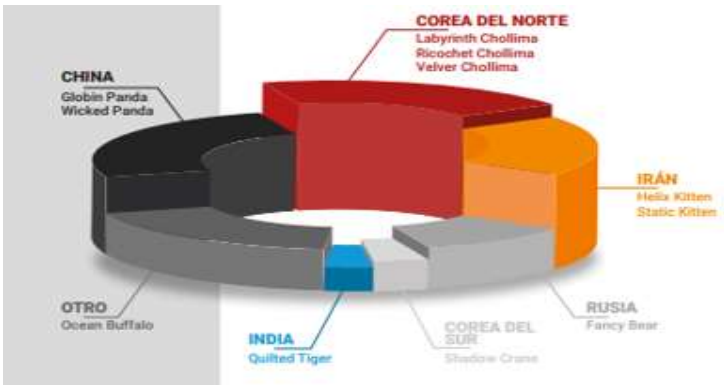
Así las cosas, los actores Estatales encuentran en el ciberespacio, el escenario para poder conseguir información que los ayude a alcanzar sus intereses, no obstante, este también genera retos y amenazas, pues al mismo tiempo pueden ser víctimas de ataques, en un contexto cada vez más dependiente a la Internet, la cual genera mayores vulnerabilidades para los Estados. Y es que los actores estatales pueden ver afectada su seguridad en un escenario que no conoce fronteras y al que cualquiera puede acceder. Gil (2017) señala diferentes casos, que valen la pena mencionarse, ya que evidencia cómo el ciberespacio puede ser un escenario de conflicto entre actores estatales, que cada vez más ven en este, una oportunidad para conseguir información, injerir en situaciones internas de otros Estados e iniciar procesos de sabotaje con fines geopolíticos.

> La posible injerencia de Rusia en las elecciones presidenciales de noviembre de 2016 de Estados Unidos o el ciberataque de *WannaCry* en mayo de 2017, pusieron el foco en las vulnerabilidades del ciberespacio. (…) EUROPOL cifra en alrededor de 900.000 millones de euros los costes del cibercrimen para la

economía global. Por su parte, la OTAN señala que los incidentes informáticos que gestionaron en 2016 supusieron un aumento del 60% respecto al año 2015 (OTAN, 2017c: 24). La tendencia de este tipo de incidentes es vista por muchos analistas como una situación de vulnerabilidad que podría llegar a afectar a suministros que consideramos básicos, como el agua, la telefonía o la electricidad, como ya ocurrió en Ucrania en 2015 (Gil, 2017. Párr. 3).

Dicho lo anterior, se empieza a vislumbrar el ciberespacio como escenario de conflicto, en el cual los actores estatales empiezan a tener participación. En el gráfico 3, se muestra los Estados que han tenido mayor actividad cibernética y que han utilizado sus recursos para a través de "malware" (*software* malicioso), realizan labores, como, por ejemplo, el robo de información.

Gráfico 3



*Tomado de CCN-CERT. Ciberamenazas y tendencias 2019.

Actores estatales como Corea del Norte, China, Irán, Rusia, Corea del Sur e India, aparecen entre los principales creadores de *software* malicioso; ahora bien, lo que no es claro es si estos "malware" tienen intenciones de beneficiar directamente al Gobierno o son realizados por empresas al margen del Estado; por lo cual, en los siguientes párrafos, se abordarán casos de ciberataques realizados presuntamente por actores estatales contra otros Estados, los cuales se realizaron en busca de satisfacer intereses geopolíticos, económicos y llevar a cabo acciones de sabotaje.

1.1 Ciberataques y ciberconflictos

En el siglo XXI, los actores estatales no se conforman con demostrar su poderío en la tierra, el mar, el aire o el espacio. Ahora quieren ser los dominadores de ese ámbito intangible que con el paso del tiempo ha cobrado una relevancia abrumadora: el ciberespacio. Y es que, con el dominio de ese universo virtual, pueden ocasionar daños a los Estados enemigos de una forma más rápida y menos costosa que en un conflicto convencional.

En el presente apartado analizaremos los ataques cibernéticos o ciberataques, cuando estos provienen de un actor estatal y van dirigidos contra otro Estado, con el objetivo de alcanzar sus intereses. No obstante, como veremos en el desarrollo de este escrito, por las características propias del ciberespacio, es muy difícil atribuir autorías en ese tipo de ataques.

Cuando hay respuesta del Estado afectado a esa agresión cibernética, nace un nuevo conflicto, que por la velocidad y la intangibilidad del mismo es conocido como ciberconflicto. Tal como lo explica el Ministerio de Defensa español, haciendo énfasis en el aspecto temporal del mismo, en su publicación de 2010 "*Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*":

> Dando por supuesto que los ciberconflictos son inevitables, se pueden establecer varias implicaciones desde la variable tiempo de la que depende el ciberespacio. Esta dependencia del tiempo se puede explicar como "el cambio en la estructura y contenido del ciberespacio a lo largo del tiempo". El tiempo en el ciberespacio puede ser relativamente corto: minutos, a menudo incluso segundos o fracciones de segundo. Basándose en esto, se pueden deducir implicaciones como el potencial de los rápidos desarrollos de acciones ofensivas y defensivas, la viabilidad de trazar el mapa del ciberespacio y la necesidad de patrullarlo y reconocerlo constantemente. Los cambios rápidos en el ciberespacio implican que se necesita poco tiempo para realizar un ataque o para implementar nuevas

defensas, comparado con el espacio físico (Ministerio de Defensa del Reino de España, 2010, pp. 55-56).

Es así, que por la facilidad de generar afectaciones graves a otros Estados o defenderse de las mismas y contraatacar, sin la necesidad de movilizar tropas, con los costos económicos y humanos que ello implica, los actores estatales han apostado por desarrollar capacidades que los haga líderes en esta "nueva" forma de generar conflictos.

Sin embargo, aunque exista la amenaza latente y los medios de comunicación escriban mucho sobre el tema, a la fecha no se ha presentado un ciberconflicto propiamente dicho, ya que nunca hemos estado en presencia de una agresión cibernética mutua entre Estados. Sólo se han presentado ataques cibernéticos de una parte, que generan repercusiones negativas en la otra. Por mencionar un ejemplo, la llamada ciberguerra entre Rusia y Estonia, que en realidad nunca fue tal, como lo analizaremos más adelante.

Si bien, nunca ha existido un conflicto cibernético como tal, existe la posibilidad de que en un futuro inmediato seamos testigos de alguno, por lo que el tema siempre estará en el tintero. Lo que sí no se puede negar es la existencia de ciberataques contra Estados, probablemente ocasionados por otros Estados, que terminan afectando a su población. Es por eso que el Comité Internacional de la Cruz Roja (CICR) emitió un documento de posición en noviembre de 2019 titulado "*Derecho internacional humanitario y ciberoperaciones durante conflictos armados*". Pero antes de referirnos al contenido de ese documento, es necesario hacer un par de aclaraciones.

El derecho internacional humanitario (DIH), tal como lo define el CICR es un "conjunto de normas destinado a limitar, por razones humanitarias, los efectos de los conflictos armados. Protege a las personas que no participan o que han dejado de participar en las hostilidades e impone restricciones a los métodos y medios bélicos". En otras palabras, el DIH es el derecho de la guerra, que se encuentra plasmado particularmente en los Convenios de Ginebra de 1949 y sus Protocolos adicionales,

además del derecho consuetudinario, que es aquel construido por la costumbre internacional (CICR, 2021).

Por su parte, el CICR es un organismo fundado en 1863, que trabaja en todos los continentes del planeta para prestar ayuda humanitaria a las personas afectadas por los conflictos y la violencia armada, y para promover las leyes por las que se protege a las víctimas de la guerra. Es un actor preponderante en el DIH y una institución independiente y neutral (CICR, 2021).

Por lo anterior, el CICR es una voz autorizada para pronunciarse sobre los conflictos que se presentan en la escena internacional, y en vista de los desarrollos tecnológicos y ante la posibilidad latente de un ciberconflicto y la realidad de los ciberataques, que pueden presentarse incluso en medio de conflictos bélicos, emitió su posición, de la cual concluyó que el recurso a las ciberoperaciones como medios y métodos de guerra en conflictos armados plantea un riesgo real para las personas civiles e instó a los Estados a aseverar que el DIH se aplica a los ciberataques durante los conflictos armados, "partiendo de la comprensión de que esa afirmación no incentiva la militarización del ciberespacio ni legitima la guerra cibernética. Al mismo tiempo, el CICR considera que es necesario seguir debatiendo, sobre todo entre los Estados, de qué manera debe interpretarse y aplicarse el DIH en el ciberespacio" (CICR, 2019, p. 11).

Para el CICR, "existe una necesidad urgente de que se entable ese diálogo, ya que los Estados que decidan desarrollar o adquirir las capacidades cibernéticas que se consideran armas, medios y métodos de guerra, ya sea con fines ofensivos o defensivos, deben procurar que esas capacidades puedan utilizarse conforme a las obligaciones que les competen en virtud del DIH". El diálogo debe estar fundado en una profunda comprensión del desarrollo de las capacidades cibernéticas militares, su posible costo humano y la protección que confiere el derecho vigente (CICR, 2019, p. 11).

El documento de posición del CICR termina afirmando que los actores estatales deben:

> Determinar si las normas actuales son adecuadas y suficientes en relación con los desafíos que plantea el carácter interconectado y ampliamente digital del ciberespacio o si deben adaptarse en función las particularidades de este último. En caso de que se formulen nuevas normas para proteger a la población civil de los efectos de las ciberoperaciones o por otros motivos, deberían basarse en el marco jurídico actual, incluido el DIH, y fortalecerlo" (CICR, 2019, p. 11).

Así como en todo ataque bélico convencional, el componente del Estado más afectado resulta ser la población civil, también de la misma manera ocurriría con los ataques cibernéticos, ya que lo que busca el Estado agresor es generar el mayor daño posible al otro Estado, que no solamente se lograría afectando el funcionamiento de sus instituciones, sino también generando el mayor perjuicio posible en sus habitantes. Por esa razón el DIH buscar anticiparse y entrar a regir en esas situaciones.

No obstante, de los ciberataques que se han presentado hasta la fecha, aunque haya indicios de que fueron llevados a cabo por un actor estatal contra otro, para alcanzar sus intereses, y probablemente haya sido así, aún no se ha comprobado. Es decir, actualmente no hay ciberataques que se puedan atribuir con certeza absoluta a algún Estado, como veremos en los casos que estudiaremos a continuación.

1.2 Casos de ciberataques

En el presente apartado estudiaremos los casos de ciberataques presuntamente cometidos por los Estados mencionados en el título del presente trabajo; que como ya vimos, son los principales creadores de *software* malicioso: Corea del Norte, China, Rusia e Irán.

1.2.1 Corea del Norte

La República Popular Democrática de Corea (RDPC), como reza su nombre oficial, es un Estado independiente liderado por Kim Jong-un, quien se proclamó como Líder Supremo de la RDPC, tras el fallecimiento de su padre Kim Jong-il en diciembre

del 2011. Corea del Norte cuenta con una población estimada para 2021 en 25.831.360 habitantes y un área de 120.538 km2 según datos del *World Factbook* de la Agencia Central de Inteligencia de Estados Unidos (CIA). Limita al norte con China y al sur con Corea del Sur. Su capital es Pyongyang.

Gráfico 4

*Tomado de La Vanguardia, 2017.

No obstante, para entender la realidad de Corea del Norte debemos dirigirnos a 1910, cuando el Imperio de Japón anexó a su territorio la Península de Corea, lo que dio inicio a un periodo de dominación que duraría hasta 1945, fecha de la rendición japonesa en la Segunda Guerra Mundial. Posterior a eso, las fuerzas soviéticas lograron el dominio de la parte norte de la Península y la parte sur fue administrada por Estados Unidos, por lo que el país fue dividido en dos zonas ocupadas que tomaron caminos muy diferentes: el Norte fue conducido hacia los preceptos tradicionales del comunismo y el Sur hacia el capitalismo del libre mercado (BBC, 2009).

El exlíder guerrillero antijaponés Kim Il-sung -Abuelo de Kim Jong-un y padre de Kim Jong-il- escaló dentro de las filas del Partido Comunista Norcoreano y se transformó en primer ministro en 1948. Con ayuda soviética, Kim comenzó un proceso

de militarización que culminó en 1950 con la ofensiva sobre Corea del Sur bajo la bandera de la liberación y reunificación del país: el inicio de la Guerra de Corea, en la cual, tropas de diferentes estados bajo el mandato de las Naciones Unidas intervinieron en favor de la parte sur, "disparando un conflicto -básicamente una guerra entre superpoderes- que duró por tres años y terminó en tablas" (BBC, 2009). Tras la firma del Armisticio de Corea, instrumento que dio fin a los ataques bélicos entre las partes, se estableció la actual zona desmilitarizada de Corea tomando como referencia el paralelo 38 norte, que sirve como frontera entre ambos países, como se puede observar en el gráfico 4.

Luego de la guerra, Kim Il-sung cambió la doctrina marxista-comunista por su propia doctrina: la "*Juche"*, que predica por la autosuficiencia en todos los aspectos del desarrollo nacional. Sus políticas convirtieron a Corea del Norte en un actor aislado y hostil hacia Occidente. Kim comenzó a perpetuar un culto a su personalidad, colocándose a sí mismo como el "Gran Líder", al tiempo que el régimen pasó a controlar cada aspecto de la vida de sus ciudadanos. Muchos de ellos intentan escapar de territorio norcoreano en busca de más libertades y una mejor calidad de vida, quienes lo consiguen y no mueren o son enviados a campos de trabajo forzoso, son llamados comúnmente "desertores", aunque para las autoridades norcoreanas son "traidores" (BBC, 2009).

Actualmente Corea del Norte, tiene una economía débil e inestable, cuyo Producto Interno Bruto (PIB) per cápita para 2015 se estimaba en USD$1.700 según datos del *World Factbook* de la CIA. Sin embargo, ha logrado incrementar sus capacidades militares con el desarrollo de armas nucleares, que logran intimidar a sus oponentes políticos. Al mismo tiempo, Corea del Norte ha ido desarrollando su capacidad cibernética, y al día de hoy los ciberataques originados desde su territorio son temidos por los países desarrollados.

Aunque Corea del Norte restringe el acceso a internet a casi toda su población, de acuerdo con un informe publicado por el Centro Internacional de Política Cibernética del Instituto Australiano de Política Estratégica, en 2017 el país contaba con más de 5.000 *hackers* empleados a su servicio. Esto con fines económicos y políticos (France 24, 2017).

Caso 1: *WannaCry*

En mayo de 2017 un grupo de *hackers* puso en vilo al planeta con un ciberataque a escala global que afectó a unos 150 países. El Gobierno de Estados Unidos culpó a Corea del Norte del cibersecuestro de más de 200.000 ordenadores, llevado a cabo mediante el virus *WannaCry*. Thomas P. Bossert, asesor de seguridad de la Administración Trump, realizó la acusación directa al régimen norcoreano mediante un comunicado oficial, en el que afirmó que "el ataque tuvo lugar a nivel internacional y costó millones de dólares. Corea del Norte es directamente responsable", y recalcó que la operación costó miles de millones de dólares y puso vidas en riesgo. El ataque comenzó el 12 de mayo y alcanzó rápidamente escala global. El virus se apoderaba del computador y emitía un mensaje en el que se pedía un rescate de 300 dólares para poder volver a acceder a los archivos (El País, 2017).

El asesor Bossert aseguró que el Gobierno tenía pruebas de que Corea del Norte era el responsable de la operación. Asimismo, indicó que el ataque puso en riesgo la vida de varias personas en el Reino Unido al comprometer su sistema sanitario. También manifestó que el objetivo principal del ciberataque fue causar estragos, y que “fue un ataque cobarde, costoso y descuidado” y “fue generalizado y costó miles de millones”. (France 24, 2017).

En un informe secreto de la Agencia de Seguridad Nacional (NSA) publicado por *The Washington* Post en junio de 2017, se establecía, con “confianza moderada” que el ciberataque fue orquestado por un grupo de *hackers* denominado *Lazarus*, controlado por el régimen norcoreano. “Aquel informe apuntaba que, pese a lo global del asedio informático, los piratas apenas recolectaron 140.000 dólares en bitcoins, la moneda virtual, y que al menos hasta entonces no las habían podido utilizar por miedo a dejar rastro” (El País, 2017).

Corea del Norte negó la acusación lanzada por Estados Unidos sobre su responsabilidad en el ciberataque con el virus *WannaCry* a través de una declaración de su Ministerio de Asuntos Exteriores, en la que expresaba que “Estados Unidos trata de

incitar a una confrontación global en nuestra contra vinculando a la RPDC al último incidente de ciberataque"; y que "Washington, origen de todos los males sociales y de cibercrímenes globales, está acusando a la RPDC de forma irrazonable y sin ninguna prueba"; asimismo, afirmaron no tener nada que ver con el ciberataque y que nunca tolerarán este tipo de acusaciones que constituyen una provocación política. (Televisa News, 2017).

Caso 2: Ciberataque a central nuclear india

La Corporación de Energía Nuclear de la India (NPCIL, por sus siglas en inglés) confirmó en octubre de 2019 que la mayor planta nuclear del país, Kudankulam, fue atacada con un *software* maligno. El virus empleado se ha encontrado anteriormente en ciberataques vinculados a grupos de Corea del Norte. La NPCIL se encargó de decir, que, pese al ataque, los sistemas de la planta no habían sido afectados y los circuitos estaban siendo vigilados continuamente. No obstante, expertos en ciberseguridad; entre los que se destaca Pukhraj Singh, quien trabajó para la Organización Nacional para la Investigación Técnica (NTRO), el equivalente indio de la Agencia de Seguridad Nacional de Estados Unidos, y quien había publicado en *Twitter* la alarma a las autoridades indias sobre este ciberataque; contradicen la versión oficial y creen que alcanzó información clave (BBC, 2019).

Los expertos señalan que este virus había sido usado antes en un ataque de 2016 en el que fue robada información financiera de millones de indios, posiblemente por *hackers* norcoreanos. Por otra parte, la empresa de ciberseguridad rusa *Kaspersky* aseguró que el virus guarda similitudes con la campaña *DarkSeoul*, "un programa de espionaje a bancos y medios de comunicación surcoreanos atribuido al famoso Grupo *Lazarus*, conectado con grupos ciberterroristas de Corea del Norte" (BBC, 2019).

El primer ministro indio, Narendra Modi, en el poder desde 2014, quiere llevar el servicio de internet a la vasta población del país en el marco del programa India digital. Sin embargo, su gestión es criticada por la ausencia de leyes de ciberseguridad y un marco legal actualizado (BBC, 2019). El Gobierno indio minimizó el incidente, probablemente

para no mostrar a India como un Estado débil o vulnerable a ataques cibernéticos. Pero no es un secreto que Corea del Norte ha logrado fabricar armas nucleares y es posible que la información obtenida por los *hackers* norcoreanos sea valiosa para desarrollar sus capacidades en esa materia.

Conclusión de los casos

Según un informe de Naciones Unidas de 2019, Corea del Norte obtuvo 2.000 millones de dólares de bancos y casas de cambio de criptomoneda mediante ciberataques con el objetivo de financiar su programa de misiles nucleares. La ONU se encuentra investigando al menos 35 instancias reportadas de Corea del Norte "atacando a instituciones financieras y cambios de criptomoneda, y realizando actividades diseñadas para ganar divisa extranjera" (Swiss info, 2019).

La ONU apunta que "los ataques masivos contra cambios de criptomoneda permiten a Corea del Norte generar ingresos de maneras difíciles de rastrear y sujetas a una menor supervisión y regulación gubernamental que el sector bancario tradicional". Y que, "actores cibernéticos, muchos de ellos trabajando bajo la dirección del *Reconnaissance General Bureau* (RGB) -el servicio de inteligencia norcoreano- recabaron dinero para sus programas de armas de destrucción masiva" (Swiss info, 2019).

En otro informe de Naciones Unidas, que hace parte del reporte anual al Comité de Sanciones a Corea del Norte del Consejo de Seguridad, y que salió a la luz en 2021, explica que Corea del Norte en 2020 "produjo material fisionable, mantuvo instalaciones nucleares y mejoró su infraestructura de misiles balísticos". Asimismo, detalló que, para lograrlo, el régimen habría usado alrededor de 300 millones de dólares robados a través de *hackers.* De esta manera, el informe indica que Corea del Norte habría recurrido a socios internacionales para acceder a materiales y tecnología (France 24, 2021).

Lo narrado en los párrafos anteriores y lo expuesto en los casos dan cuenta del poderío cibernético con el que cuenta la República Popular Democrática de Corea, un país pequeño con una economía empobrecida, pero que ha usado la Internet como un

medio para ser considerado un actor importante en la escena internacional y en particular, ha ayudado al régimen a sobrevivir.

Una muestra de ello fue el enorme interés que tuvo la administración Trump en este país. El expresidente de Estados Unidos se reunió en 3 oportunidades con Kim Jong-un; una de ellas en la frontera que divide a las dos Coreas, convirtiéndose en el primer presidente estadounidense en pisar suelo norcoreano (El País, 2019).

1.2.2 China

La República Popular China es el país más poblado del planeta con 1.437.651.014 habitantes, según datos de octubre de 2020. Asimismo, es el cuarto más grande, detrás de Rusia, Canadá y Estados Unidos, con una superficie de 9.596.900 km2, su capital es Beijing. Desde 2013 el presidente es Xi Jinping. En China rige un sistema político conocido como "socialismo con características chinas", que se basa, desde el punto de vista económico, en la economía mixta, es decir, economía de mercado, pero con predominio de la propiedad pública; y, desde el punto de vista político, en el liderazgo del Partido Comunista, que ostenta el control de las diversas estructuras políticas (Ministerio de Asuntos Exteriores, Unión Europea y Cooperación del Reino España 2021).

Gráfico 5

*Tomado de Mapas del Mundo, 2013.

Al hablar de ataques cibernéticos es imposible no hablar de la República Popular China, un actor estatal que ha cobrado gran relevancia en las últimas décadas en la escena global, tanto en el aspecto económico como en el militar, al tiempo que se ha convertido en uno de los actores más fuertes del ciberespacio. Si bien no se ha comprobado que el Gobierno chino esté directamente relacionado con los ataques cibernéticos originados desde su país, hay grandes indicios de que podría ser así, como veremos en las siguientes líneas.

Es importante destacar que en los casos de ciberataques que estudiaremos, relacionados con China, podremos observar cómo estos son realizados por grupos de *hackers,* que tengan conexión con el Gobierno o no, lo cierto es que su actuar favorece los intereses del Estado chino, y se manifiestan a través de ataques que buscan la extracción de propiedad intelectual de compañías extranjeras, la obtención de información sensible de otros gobiernos o simplemente el daño de equipos y sistemas de sus competidores políticos y económicos.

Caso 1: APT1 – Unidad 61398

Según un informe de 2013 de la empresa de seguridad cibernética *Mandiant* de Estados Unidos, una unidad militar china sería el mayor *hacker* de los sistemas informáticos estadounidenses. *Mandiant* publicó 3.000 indicadores digitales, incluyendo nombres de dominio y direcciones IP vinculados con ataques de *hackers*, sobre la actividad del grupo APT1 (*Advanced Persistent Threat*), al que consideran uno de los más prolíficos en cuanto a la cantidad de información que ha robado. El resultado de la investigación fue que ATP1 estaría vinculado con la Unidad 61398 del Ejército Popular de Liberación con sede en Shanghai (DW, 2013).

Se estima que la Unidad 61398 llevaba siete años saqueando los secretos de 140 organizaciones comerciales, políticas y militares. Uno de sus principales objetivos era el robo de propiedad intelectual. Según el informe, los piratas se infiltraron en la firma de ciberseguridad *RSA*, encargada de proteger las bases de datos del Gobierno

norteamericano, en *Coca Cola*, y en la compañía de aeronáutica militar *Lockheed Martin*. También vulneraron los sistemas de diarios como *The New York Times* y *The Wall Street Journal* poco después de que publicaran artículos críticos sobre el régimen chino, y lograron operar a distancia infraestructura eléctrica, acueductos y oleoductos (Semana, 2013).

Los *hackers* de APT1 invadían los sistemas con correos electrónicos que enviaban a nombre del jefe o un colega del objetivo. La operación era replicada millones de veces hasta que alguien lo abriera y automáticamente se instalara un programa espía que daba acceso a contactos, documentos, redes internas y bases de datos. La información era comprimida y enviada a China. Se calcula que Estados Unidos perdió 300.000 millones de dólares en secretos industriales por estos robos en 2012 (Semana, 2013).

En su momento, la publicación del informe causó mucho malestar en China, por lo que el Ministerio de Asuntos Exteriores chino calificó las denuncias del reporte como carentes de fundamento. El portavoz del Ministerio, Hong Lei, expresó que “las críticas infundadas son irresponsables y poco profesionales, y no ayudarán a resolver el problema”. Hong dijo que China está comprometida con la lucha contra el crimen cibernético y que también fue una gran víctima de ataques. Según la Cancillería china, expertos del gobierno hallaron 73.000 direcciones de IP extranjeras que fueron vinculadas con ataques contra 14 millones de computadoras en China, y la mayoría de esos ataques fueron originados en Estados Unidos (DW, 2013).

Al no comprobarse totalmente la participación del Estado chino en los ataques cibernéticos, la Casa Blanca y el Departamento de Estado de Estados Unidos no hicieron comentarios al respecto. Sus portavoces aseguraron que la información forma parte de asuntos de inteligencia. No obstante, resaltaron la necesidad de aumentar el diálogo con el Gobierno de Pekín sobre este tema. La portavoz de la Casa Blanca en ese entonces, Jay Carney, expresó que "no tengo comentarios sobre el informe ni las acusaciones específicas. Pero hemos planteado repetidamente nuestras preocupaciones sobre el robo cibernético con los altos niveles del Gobierno chino, incluido el Ejército, y lo seguiremos haciendo" (RTVE, 2013).

Caso 2: El Covid-19 y los ciberataques

En el año 2019 se conoció el primer caso de una nueva enfermedad que afectaba el sistema respiratorio de las personas y que podía llegar a ser mortal. Esto se dio en la ciudad de Wuhan, China. A la enfermedad se le dio el nombre de Covid-19, y pronto se convertiría en una pandemia que aún está ocasionando estragos en los sistemas de salud pública de la mayoría de los países del globo terráqueo y en sus economías. El Covid-19 llegaría para revolucionar la forma de relacionamiento en el que prima la virtualidad, no solo entre las personas, sino también entre los Estados, al tiempo que iniciaba una carrera por la vacuna entre las principales potencias.

Mientras China luchaba con todo su arsenal científico para ser el primer país en producir una vacuna que resultara exitosa contra la "nueva" enfermedad, los *hackers* asentados en su territorio intentaba conseguir información útil en la fabricación de la vacuna. En mayo de 2020, funcionarios de la Administración Trump, específicamente de la Oficina Federal de Investigaciones y la Agencia de Seguridad de la Ciberseguridad e Infraestructura (CISA- por sus siglas en inglés), frente cibernético del Departamento de Seguridad Nacional, acusaron a *hackers* chinos de intentar robar propiedad intelectual relacionada con tratamientos y vacunas contra el coronavirus a universidades estadounidenses, farmacéuticas y otras empresas de atención médica, y apuntaron que los ciberataques podrían poner en peligro el progreso de la investigación médica (La República, 2020).

Los ataques cibernéticos procedentes de China fueron vistos por los funcionarios del Gobierno de Trump como un ataque directo a la salud pública de los Estados Unidos, porque pudieron haber obstaculizado la investigación de vacunas en algunos casos. Sin embargo, la CISA no dio los nombres de las víctimas de los ciberataques y no explicó cómo llegaron a la conclusión de la responsabilidad de Pekín en estos ataques. Por su parte, el portavoz del Ministerio de Relaciones Exteriores de China, Zhao Lijian, dijo que China se oponía a los ataques cibernéticos de todas las formas y lideraba la investigación para una vacuna y tratamiento de Covid-19, y reiteró que "es inmoral que cualquiera se

involucre en la propaganda de rumores sin presentar ninguna evidencia" (La República, 2020).

La siguiente víctima de los ciberataques chinos sería Australia. Todo comenzó con el malestar que causó en China el liderazgo de Australia entre los países que pedían una investigación sobre el origen del coronavirus en Wuhan. Los chinos veían motivaciones políticas del que consideran uno de los aliados más fuertes de Estados Unidos. Las tensiones se hicieron más fuertes cuando el embajador chino en Australia, Cheng Jingye, sugirió como respuesta un boicot a los productos australianos. China cumplió su amenaza en mayo de 2020 y suspendió las importaciones de carne australiana (El Mundo, 2020).

Semanas después, en junio de 2020, el primer ministro de Australia, Scott Morrison, denunció que su gobierno y sus instituciones estaban siendo blanco de ataques cibernéticos por parte de un "agente estatal". Morrison dijo que los ciberataques son generalizados y que han afectado al Gobierno así como a proveedores de servicios esenciales y empresas australianas. Sin embargo, se rehusó a mencionar directamente el nombre de China (BBC, 2020). Para Morrison no había duda de que el ataque había sido ordenado por otro Estado, según expresó: “sabemos que es un ataque cibernético sofisticado vinculado a un Estado debido a la escala y los objetivos” (El País, 2020).

No obstante, fuentes gubernamentales citadas por la cadena ABC, confirmaron que creen que China es el responsable de los ciberataques (El País, 2020). En ese sentido apuntó Tom Uren, analista senior del Centro de Política Cibernética del Instituto de Política Estratégica de Australia, quien explicó que sólo países como China, Estados Unidos, Reino Unido y Rusia tendrían esa capacidad, y manifestó que “es una lista muy pequeña, y si piensas en quién querría hacerlo, hay una lista de uno” (El Mundo, 2020).

Estas declaraciones no cayeron muy bien en China, por lo que desde el Ministerio de Relaciones Exteriores rechazaron rotundamente las sugerencias de un ataque cibernético a gran escala contra los departamentos del Gobierno australiano. El portavoz del Ministerio, Zhao Lijian, apuntó a que los reclamos de ciberataques se originaron en

el Instituto de Política Estratégica de Australia, un centro de pensamiento, que según él es financiado por compañías de armas estadounidenses y por eso hacen reclamos ficticios sobre China (El Mundo, 2020).

Los ataques cibernéticos relacionados con el Covid-19 originados en China siguieron presentándose y en el 2021 la víctima fue India. Según un informe de la empresa de ciberinteligencia *Cyfirma,* un grupo de piratas informáticos presuntamente respaldado por el Estado chino atacó entre enero y febrero de 2021 los sistemas de dos fabricantes de vacunas indios cuyas inyecciones para el Covid-19 se utilizan en la campaña india de inmunización. *Cyfirma,* respaldada por la estadounidense *Goldman Sachs*, uno de los grupos de inversiones y valores más importantes del mundo, indicó que el grupo de *hackers* chinos conocido como APT10 o *Stone Panda* había identificado vulnerabilidades en el *software* de la cadena de suministro de *Bharat Biotech* y el *Serum Institute* de la India (SII), compañías que finalmente resultaron afectadas (Reuters, 2021).

A marzo de 2021 se estimaba que India producía más del 60% de las vacunas que se venden a nivel global, y que el *Serum Institute* de la India era el mayor fabricante de vacunas del planeta. Según afirma el director ejecutivo de *Cyfirma*, Kumar Ritesh "la verdadera motivación aquí es la sustracción de la propiedad intelectual y la obtención de una ventaja competitiva sobre las empresas farmacéuticas indias". En tanto que la Embajada de China en Nueva Delhi se pronunció acotando que "China se opone firmemente a todas las formas de ciberataques" y que "la especulación y la fabricación no tienen ningún papel en la cuestión de los ciberataques" (Reuters, 2021).

Conclusión de los casos

Lo que acabamos de ver constituye solo una pequeñísima muestra del tipo de ataques cibernéticos que provienen desde China, que no se pueden atribuir con total seguridad al Gobierno del Partido Comunista Chino, pero que para los afectados no hay dudas de que es así. Solo basta con darse cuenta de los ataques a Estados Unidos originados desde una unidad militar de Shanghai o el hecho de que Australia haya sido víctima de ciberataques justo después de tener fricciones con el Gobierno chino.

Si aceptáramos cien por ciento la hipótesis de que el Gobierno es el responsable de todos estos ataques, encontramos cómo China usa verdaderamente la Internet para alcanzar sus intereses, tanto políticos como económicos. Los ataques a compañías extranjeras benefician grandemente a las empresas chinas, que podrían usar la información y los secretos extraídos por los *hackers* para su beneficio, lo que llevaría al mediano plazo a acelerar el crecimiento de la economía china.

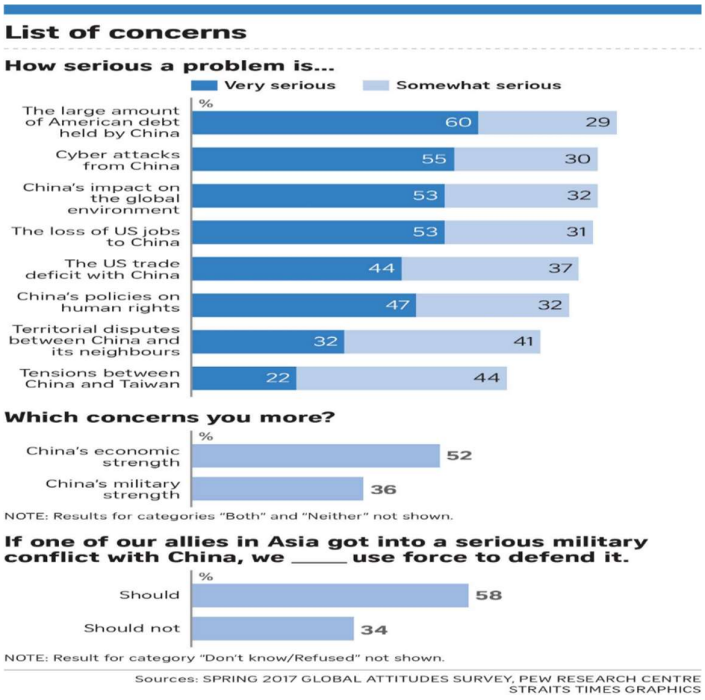
La promoción de una economía digital ha surgido como un componente integral de la estrategia de China para asegurar su desarrollo futuro, y los ciberataques podrían ser una herramienta muy útil para ese objetivo. De hecho, el primer ministro chino Li Keqiang ha destacado en sus informes de trabajo de 2018 y 2019 la importancia de integrar lo digital con la economía real como fuente de crecimiento. Los gigantes digitales de China: *Alibaba, Baidu* y *Tencent*, obtienen ingresos anuales estimados en 87.300 millones de dólares; y a partir de 2018, la economía digital de China se clasificó como la segunda más grande del mundo, detrás de Estados Unidos, estimada en alrededor de 3,5 billones de dólares. Una proyección oficial sugiere que la economía digital podría hacer una contribución anual de 16 billones de dólares para 2035. Cada vez más, las empresas chinas que han tenido éxito en su mercado interno están buscando nuevos mercados y oportunidades en todo el mundo, a menudo de una manera que encaja con los objetivos geopolíticos de China (International Institute for Strategic Studies, 2019).

El Gobierno chino durante los últimos años ha ejercido un control más estricto sobre las empresas del país. En la actualidad, prácticamente todas las principales empresas de tecnología e internet de China, incluidas *Baidu, Huawei* e *iFlytek,* han establecido comités conformados por altos ejecutivos que al tiempo cumplen con la función de secretarios del Partido Comunista. Hasta cierto punto, su papel es simbólico, destinado a permitir el acceso e influencia del Partido y la demostración de la lealtad de las empresas. Este nivel de interferencia estatal podría tener un impacto negativo en la reputación de estas empresas, pero lo que es una realidad es su indiscutible crecimiento con el acompañamiento siempre vigilante del Estado chino (International Institute for Strategic Studies, 2019).

En el campo político, el Gobierno es el que se ve favorecido con los ataques a los sistemas y bases de datos de entidades gubernamentales de otros Estados, porque así conoce de primera mano los planes e información valiosa de sus competidores, al tiempo que les causa grandes perjuicios, como lo han hecho los *hackers* chinos contra Estados Unidos y Australia. Asimismo, vimos cómo han "castigado" a aquellos que hablan mal del Partido Comunista en el exterior.

Un estudio sobre los temas de la agenda bilateral con China realizado en Estados Unidos en 2017 -previo a un encuentro entre el entonces presidente Donald Trump con su homólogo chino Xi Jinping en el que tratarían temas comerciales- por *Pew Research Center*, un grupo de expertos estadounidense dedicado a analizar las actitudes públicas, arrojó que un número menor de estadounidenses se preocupa por el déficit comercial. En cambio, un número mayor está preocupado por los ataques cibernéticos procedentes de China, el 55% de los encuestados lo consideró como un problema serio (The Straits Times, 2017), como podemos evidenciar en el gráfico 6.

Gráfico 6



*Tomado de The Straits Times, 2017.

Aunque el estudio fue realizado sólo en Estados Unidos, nos permite imaginar que tan grande es el poderío de los chinos en el ciberespacio, si son capaces de ocasionar daños a la máxima potencia militar y económica del planeta usando la Internet y han generado cierto temor en la sociedad estadounidense, tienen la capacidad de atacar las redes de cualquier país del planeta.

Finalmente, podemos decir que todos los ataques cibernéticos presuntamente cometidos por China terminan de la misma forma: con un pronunciamiento por parte del Gobierno en el que niega rotundamente su participación, minimiza las acusaciones y las reduce a rumores y el clásico "China se opone firmemente a todas las formas de ciberataques".

1.2.3 Rusia

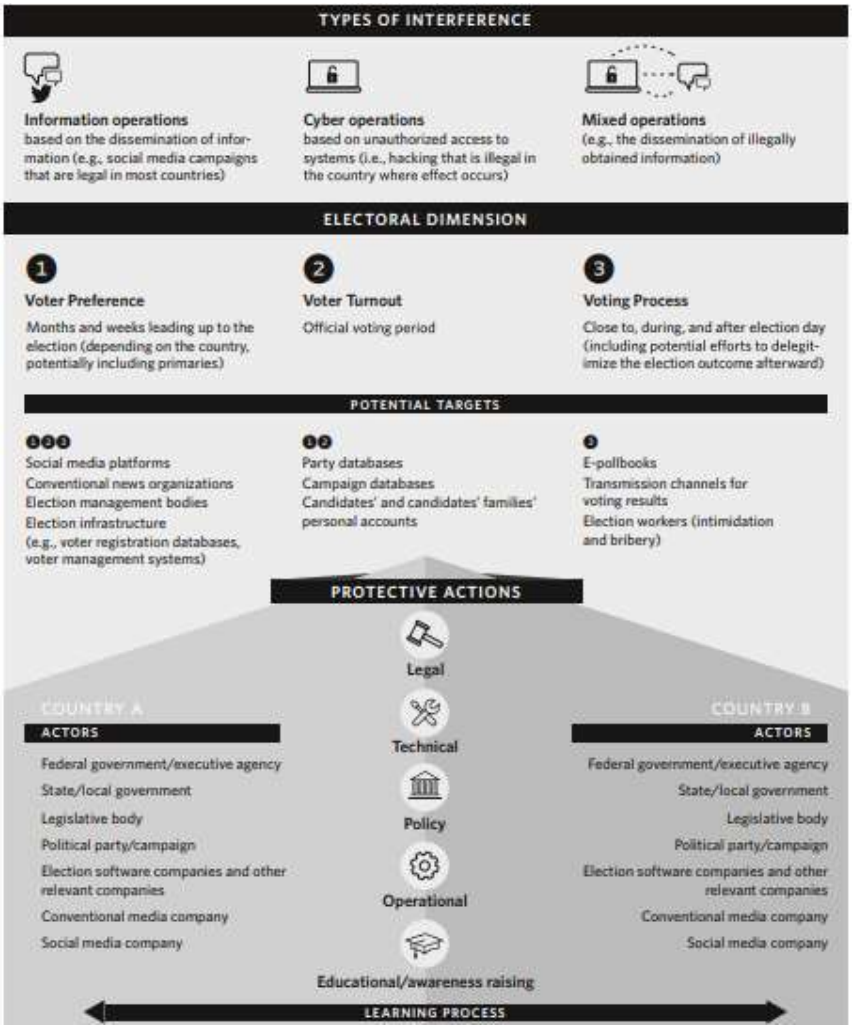
Rusia, o la Federación Rusa, es el país más extenso del mundo con una superficie de 17.075.400 km2, su capital es Moscú y limita con 16 países, entre los que se encuentran China, Ucrania, Polonia, Corea del Norte, Estonia y Letonia – de estos dos hablaremos posteriormente- también limita por sus aguas territoriales con Japón y Estados Unidos. Rusia es el noveno país con mayor población en el mundo; según datos de octubre de 2019 contaba con 144.868.902 habitantes. Por otra parte, la Federación Rusa cuenta con una forma de gobierno de República semiparlamentaria en la cual el actual presidente, desde 2012, es Vladímir Putin, un político, abogado y exagente del KGB -Comité para la Seguridad del Estado-, y quien anteriormente también había liderado al país entre 1999 y el 7 de mayo de 2008 (Ministerio de Relaciones Exteriores, Unión Europea y Cooperación del Reino de España, 2021).

Gráfico 7

*Tomado de: Ministerio de Relaciones Exteriores, Unión Europea y Cooperación del Reino de España, 2021

Ahora bien, cuando pensamos en casos de ciberataques, tendemos a asociarlos con Rusia; y es que si bien la mayoría de ataques cibernéticos no provienen de este país, como se observaba anteriormente, si hay casos relevantes que lo han tenido como protagonista. Casos como Estonia 2007, el cual es considerado por muchos como el primer ataque cibernético a gran escala contra un Estado, Letonia 2008, Georgia en ese mismo año, considerada la primera guerra híbrida, o casos un poco más recientes como una posible injerencia en las elecciones de los Estados Unidos de 2016 apuntan a la Federación Rusa.

Gráfico 8



*Tomado de Carnegie Endowment for International Peace, 2018.

Un estudio de *Carnegie Endowment for International Peace* del año 2018, revela que las principales modalidades de interferencia utilizados por Rusia son operaciones de información, basados en la difusión de información a través de redes sociales; ciber operaciones que permiten ingresar de manera ilegal a páginas estatales, entre otras. Estas son relevantes, ya que permitirá encontrar similitudes con los siguientes casos de ciberataques: Estonia 2007 y Georgia 2008, en los cuales, si bien la participación del Gobierno ruso no fue totalmente comprobada, se infiere por muchos, que hubo una participación debido a los acontecimientos sociales y políticos que se produjeron.

Caso 1: Estonia 2007

Si tuviésemos que catalogar a los países más vulnerables a un ciberataque, probablemente Estonia ocuparía los primeros puestos. Este pequeño país europeo con una población de 1,3 millones de personas, que limita al este con Rusia y al sur con Letonia y que estuvo bajo la influencia de la ex Unión Soviética, fue blanco de ataques cibernéticos a gran escala en el año 2007. Tras su etapa postsoviética, Estonia realizó grandes esfuerzos por modernizarse, a tal punto que fue el primer país que permitió a sus ciudadanos votar a través de internet. Además, el 97% de su actividad bancaria se realiza también a través de medios virtuales; de hecho, en este país se considera que el acceso a internet es un derecho humano básico. De esta manera, este país cuenta con la mayoría de los servicios gubernamentales de manera digital, lo que facilita a las personas realizar sus actividades, pero al mismo tiempo, la digitalización de todos sus servicios y tener gran parte de información nacional y gubernamental en la Internet, volvió vulnerable a esta nación báltica a los ataques cibernéticos, tal como ocurrió en el año 2007.

En el año 2007, Estonia se enfrentó a un ciberataque que amenazó con paralizar al Gobierno, a la banca y a los medios de comunicación. Fue un ataque sin precedentes, por considerarlo el primer ataque cibernético a gran escala. El origen de este ataque estaba en la historia misma del país; el monumento denominado “el soldado de bronce”, un monumento soviético que, para la minoría rusa en Estonia, representaba un homenaje al patriotismo; sin embargo, para los estonios, era el recuerdo de la era soviética, un símbolo

de lo que fue la ocupación de su país. El Gobierno de Estonia decidió trasladar este monumento del centro de Tallin a un cementerio militar. Tras esta decisión se empezaron a realizar una serie de protestas en el país.

El 27 de abril de 2007, el soldado de bronce fue traslado, sin que nadie se enterara. No obstante, este mismo día las páginas web gubernamentales empezaron a colapsar, el acceso a la banca *online* fue bloqueado y las páginas de noticias no funcionaban. Los ataques empezaron a ser recurrentes y se logró incomunicar a Estonia del resto del mundo. Para Ganuza (s.f) en su texto: *situación de la ciberseguridad en el ámbito internacional y en la OTAN*, los ciberataques en Estonia se pueden dividir en dos fases. La primera comprende entre el 27 al 29 de abril "en donde los ataques debida a la inmediatez del conflicto tenían un componente emocional y esto en sí mismo constituía la motivación para unirse a los ciberataques". Durante esta primera fase, se evidenciaron también, ataques a sitios web del Ministerio de Defensa de Estonia y de los principales partidos políticos.

La segunda fase, para Ganuza (s.f) fue entre el 30 de abril y el 18 de mayo. Una fase más compleja con herramientas más sofisticadas y con una coordinación más evidente.

> (…) el conflicto en las calles se difumina trasladándose al ciber espacio, donde los ánimos de los ciudadanos de Estonia (rusos y estonios) se calman y no hay lugar para ataques emocionales, en esta situación más fría los ataques se volvieron más complejos tanto en el aspecto técnico como en el organizativo y en la coordinción; sucediéndose ataques mucho más sofisticados que necesitaban de un mayor conocimiento de las herramientas de ciber guerra, al menos por parte de los organizadores y de un uso de grandes "*botnets*" y de una coordinación minuciosa y precisa (Ganuza, s.f, pág. 179).

Desde otra perspectiva, los ciberataques en Estonia, tuvieron tres oleadas. En una entrevista realizada a Heli Tiirmaa-Klaar, Ciberembajadora de Estonia, quien es a su vez asesora de la OTAN y encargada de diseñar la política europea del ciberespacio,

respondió lo siguiente cuando le preguntaron sobre el tipo de ataque sufrido en Estonia en 2007:

> Hubo tres oleadas. Primero fue la activista, luego una más profesional y al final otra más seria. Durante tres semanas**.** Fue contra servicios *online* y contra periódicos para bloquear la información que ocurría en el país. Imagina que tienes disturbios y los medios no funcionan. Los estonios usan poco la radio y los viejos canales de tele, que sí funcionaban. Las webs gubernamentales fueron bloqueadas, los bancos *online* también. Toda la infraestructura de internet que usábamos era atacada (El País, 2020).

En los ataques sufridos por Estonia se encontraron: (I) ataques de denegación de servicios (DoS). Los cuales buscan que un sistema de información sea inaccesible a los usuarios legítimos. (II) ataques de desfiguración de sitios web, el cual sirve para modificar el aspecto visual de una página web. "Uno de los principales objetivos en estos ataques fue el primer ministro de Estonia Andrus Ansip. En uno de estos ataques los *hackers* modificaron el contenido del sitio web del partido político del primer ministro y entre otras cosas emplazaron una fotografía de Andrus Ansip con bigote tipo Hitler" (Ganuza, s.f, pág. 183). (III) correo basura. En el caso de Estonia, estos correos basura se enviaron a direcciones oficiales gubernamentales con el fin de que las cuentas colapsaran.

Caso 2: Georgia 2008

Las ciber operaciones realizadas en Estonia 2007 y luego las realizadas en Letonia 2008, podrían ser consideradas una nueva variante para generar conflicto, o por lo menos, esto es lo que algunos autores creen. Para Linares (2019), Rusia ganó experiencia con la desestabilización de países a través de ataques cibernéticos; y en Georgia 2008 recurrió a una combinación del uso del ciberespacio con operaciones armadas convencionales, una "guerra híbrida".

El 8 de agosto de 2008 empiezan las hostilidades entre Georgia y Rusia y al día siguiente es declarado oficialmente el estado de guerra. Esta se produjo debido un ataque

de Georgia contra fuerzas separatistas en Osetia del Sur, una región de conflicto debido a una disparidad de criterios en territorios con intenciones de autodeterminación y cuya independencia es reconocida por Rusia, pero no por Georgia, como se aprecia en el gráfico 9.

Gráfico 9

*Tomado de La Vanguardia

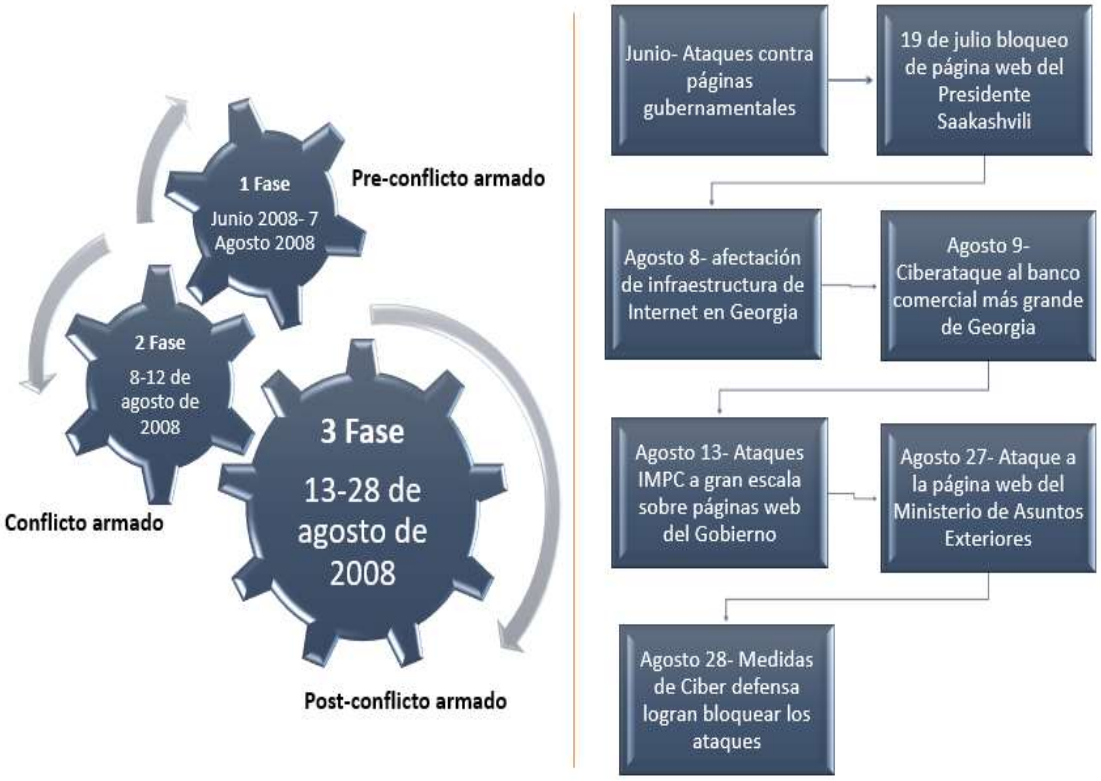
No obstante, más allá de la guerra comprendida entre el 8 y 12 de agosto de 2008, existió una serie de ataques cibernéticos que afectaron a Georgia, aunque, vale la pena aclarar, que, a diferencia de Estonia, este país contaba con menos dependencia a la tecnología, lo que afectó en menor medida sus operaciones.

Como podremos detallar en el gráfico 10, los ataques cibernéticos no solo se remontan a la fecha que comprendió el conflicto armado, sino que incluso en los meses anteriores, se presentaron ataques a las páginas de Gobierno de Georgia. Esto también en el marco de las tensiones políticas que ya se vivían entre Rusia y Georgia para la época.

De manera similar, a lo ocurrido en Estonia, se presentaron ataques de DDoS contra sitios oficiales de Georgia, lo cual afectó a diferentes sitios web, entre ellos los de la Banca, además de ataques a la infraestructura misma de la Internet local, lo que afectó las comunicaciones en el país. Los ataques cibernéticos incrementaron en la medida que

el conflicto armado se propagaba y estos no cesaron, sino hasta días después del cese al fuego y la aceptación del plan de paz propuesto por la Unión Europea.

Gráfico 10



*Elaboración propia a partir del texto "*la situación de la ciberseguridad en el ámbito internacional y en la OTAN"*

Para Ganuza (s.f), como para muchos autores, no se puede comprobar la participación directa del Gobierno ruso en los ataques cibernéticos ocurridos en Georgia, sin embargo, es más que claro que independientemente de quien ordenara estos ataques, estos afectaron a Georgia, el cual además de la una guerra convencional, tuvo que enfrentar una serie de ataques cibernéticos que mermaron la capacidad de comunicación e intentaron influenciar en la opinión pública hacia la postura defendida por Rusia, a través de ciber propaganda.

Conclusión de los casos

En lo ocurrido en Estonia y Georgia no se puede determinar que hubo una participación del gobierno ruso en los ataques; no obstante, Martínez (2015) afirma que es evidente para ella que el gobierno ruso sabía de los ataques "y no solo hizo nada para detenerlos, sino que les parecieron bien, ya que les ayudaban a conseguir sus intereses políticos y militares". Para Ganuza (s.f), la impresión es similar, señala al gobierno ruso como "cómplice" y lo sustenta en tres hechos:

> A) la falta de cooperación de Rusia para identificar a los responsables; b) Rusia es el principal o único beneficiario de los resultados de la ofensiva cibernética y c) los ciber ataques evolucionaban acorde con la evolución de las operaciones armadas y para ello se necesitaba información que solo era accesible por parte de las autoridades políticas y militares rusas (Ganuza, s.f, pág 202).

De manera similar, para Linares (2019) el gobierno ruso es cómplice de los ataques cibernéticos en Estonia y Georgia, aunque ella va un poco más allá al establecer que aplicando en el campo cibernético *The Harbouring Doctrine*, al gobierno ruso se le podría atribuir los ataques, por salir desde su territorio y tolerarlos, y por su falta de cooperación para rastrear a los autores materiales de los hechos. Así las cosas, la participación del Gobierno ruso es más controversial, ya sea por acción u omisión y en los casos específicos anteriormente mencionados se puede evidenciar un beneficio del gobierno ruso con los ataques sufridos por Estonia y Georgia.

1.2.4 Irán-Estados Unidos-Israel: Un conflicto silencioso

En este punto hemos hablado de casos de ataques cibernéticos los cuales han tenido origen en países como Corea del Norte, China y Rusia; sin embargo, a falta de evidencia no se puede atribuir ninguno de estos directamente a cada gobierno. Es precisamente la dificultad de atribuir un ataque, lo que hace del ciberespacio un escenario impredecible y a la vez silencioso. Miles de ataques cibernéticos tienen lugar a diario, de los cuales no nos enteramos en las noticias. En esta parte del trabajo queremos abordar

una situación, que, si bien todos conocemos por sus tensiones políticas, poco sabemos de los diferentes ataques cibernéticos que se han producido en el marco de la difícil relación de Irán con Israel y Estados Unidos.

Por un lado, Irán o como reza su nombre oficial, República Islámica de Irán, es un país de Oriente Medio con una superficie de 1.745.150 Km², lo ubica como el 18° país más extenso del mundo y cuenta con una población de casi 80 millones de personas, su capital es Teherán. Según la Constitución de 1979, la cual define a Irán como una República Islámica, "el sistema se basa en la distinción entre un Ejecutivo encabezado por el presidente de la República quien gestiona la administración del país, y un Legislativo que de manera efectiva aprueba las leyes y vota a los candidatos a ministros propuestos por el presidente. Pero por encima de esta realidad republicana, se encuentra el Líder Supremo". Desde el 3 de agosto de 2013, su presidente es Hasán Rohaní y su Líder Supremo es Alí Hoseiní Jamenei quien ostenta el cargo desde 1989 (Ministerio de Relaciones Exteriores, Unión Europea y Cooperación del Reino de España).

Gráfico 11

*¨Tomado de BBC Mundo

Por otro lado, se encuentra Israel, que como se puede observar en el gráfico anterior, no comparte fronteras con Irán, pues en medio de los dos se encuentra Jordania, Siria e Irak, pero que se encuentran en una región volátil y que los ha enfrentado históricamente en una guerra geopolítica e ideológica. El Estado de Israel, el único Estado Judío del mundo, con una población de casi 9 millones de habitantes y con un territorio de 20.325 km2, es aproximadamente 85 veces más pequeño que Irán y tuvo como primer

ministro a Benjamín Netanyahu, quien estuvo en el poder más de 12 años, hasta el 13 de junio de 2021.

Finalmente, se encuentra Estados Unidos, una de las grandes superpotencias mundiales, por su poderío económico y militar y gran aliado en la región de Israel. Estados Unidos tiene participación del conflicto que se vive en el Medio Oriente, a través de su ayuda constante al Estado judío. "Desde 1979 (año en que triunfó la Revolución Islámica) el primer objetivo de Irán ha sido luchar contra Israel, y por su parte Israel ve a Irán como un país que patrocina el terrorismo y ha calificado su influencia en el Medio Oriente como la amenaza más grande del planeta" (BBC, 2018). Estados Unidos, entre otras cosas, ve también a Irán como una posible amenaza nuclear, la cual ha tratado de contrarrestar desde la administración Bush (2001-2009), así como también Barack Obama (2009-2017) y Donald Trump (2017-2021) quien retiró al país del acuerdo nuclear con Irán, lo cual intensificó las tensiones entre los 3 países. Lo anterior ha hecho que actualmente tengamos una confrontación a tres bandas que también ha implicado una serie de ciberataques como se hablará en los siguientes dos casos.

Caso 1: Operación juegos olímpicos y virus *Flame*

Al hablar de la tensa relación actual entre Irán, Israel y Estados Unidos, nos podemos imaginar una de las causas: el programa nuclear de Irán. Este problema, que se remonta a alrededor del año 2002 cuando se descubrieron centros clandestinos de uranio en Natanz, es el centro de las tensiones y a la vez lo que incentivó la creación de la operación denominada "Juegos Olímpicos". Según Alantede (2012) en el Gobierno de Barack Obama se llevó a cabo una campaña secreta de ciberataques contra el programa nuclear de Irán, el cual con ayuda de Israel "llegó a deshabilitar 1.000 centrifugadores de la planta de Natanz, un quinto de los que estaban en activo. El virus empleado escapó de Natanz en 2010, se replicó en la Red aprovechando un fallo en el sistema operativo *Windows* y fue bautizado por los expertos en seguridad como *Stuxnet."*

Sin embargo, el Diario El Mundo (2012) detalla que la idea de atacar a Irán a través de la Internet surgió desde la administración Bush pero fue durante la

administración Obama que se ordenó que se "acelerara la acción secreta con el nombre en clave de *Olympic Games* (Juegos Olímpicos)". Esta operación, según afirma David E. Sanger, corresponsal del *New York Times*, logró retrasar el programa nuclear iraní entre 18 y 24 meses hasta que el virus *Stuxnet,* fue detectado, al salir de manera accidental de la central de Natanz y propagarse por la Internet.

Además de lo anterior, el descubrimiento de un nuevo y complejo virus informático abrió una nueva etapa en los ataques cibernéticos. *Flame* un virus creado como una potente arma de espionaje, operó en la sombra durante varios años, hasta que fue descubierto en 2012 por la empresa de seguridad en internet *Karspersky.* Según Reventós (2012) más de 600 ordenadores fueron afectados, la mayoría de ellos en Irán. "Por su complejidad, ámbito de acción geográfica, naturaleza de infecciones y comportamiento, la empresa de seguridad informática considera que *Flame* es obra de un Estado y no cibercriminales comunes". Si bien no mencionan posibles países implicados, por la similitud del virus con *Stuxnet*, se relaciona a Estados Unidos e Israel (El País, 2012).

De esta manera, para Gayarre (2012) la realización de *softwares* malignos como *Stuxnet y Flame* "podrían ser consideradas como las primeras armas utilizadas en un ciber sabotaje a largo plazo contra uno de los enemigos de Estados Unidos".

Caso 2: Irán-Israel 2020

Tras la cantidad de ataques cibernéticos sufridos por Irán, este país islámico decidió invertir en ciber seguridad y hoy en día es considerada como una potencia cibernética. Aunque no está oficialmente reconocido como una entidad que trabaje para el gobierno, Irán cuenta con un ejército cibernético el cual ha realizado diferentes ataques afectando la seguridad nacional de diversos países; pero mayoritariamente, dirigidos a Israel.

Para Kirkpatrick y Bergman (2020), columnistas de *The New York Times,* "los ataques cibernéticos son un arma que puede causar daños graves al otro lado del planeta

a bajo costo y con pocas posibilidades de rastreo" lo cual lo ha hecho atractivo para Irán a la hora de generar afectaciones en países como Estados Unidos, Arabia Saudita, Israel, entre otros. Expertos en ciberseguridad y funcionarios gubernamentales estadounidenses han descubierto un incremento de las actividades maliciosas realizadas por *hackers* que provienen del territorio iraní, lo cual hace prever que los ataques cibernéticos desde Irán seguirán en aumento y cada vez serán más severos (The New York Times, 2020).

En el 2020, durante un intercambio de ataques cibernéticos entre Irán e Israel se cayeron los sistemas que regulan el flujo de mercancías en el puerto iraní de Shahid Rajaee, provocando atascos en mar y tierra y como respuesta a este se produjo un ataque al sistema hídrico de Israel. Cembrero (2020) cita las palabras de Yigal Unna, responsable de ciberseguridad en Israel, lo que para él fue el ataque a la central hídrica en abril de 2020. "Fue un ataque sincronizado y organizado" contra una planta de tratamiento de aguas para consumo humano en el cual el atacante se apoderó de algunas contraseñas y trató de alterar el programa informático para incrementar la cantidad de cloro para que el agua resultase nociva para la salud de las personas.

Pero el ataque de abril de 2020, no fue el único sufrido por Israel, en noviembre del mismo año se reportaron apagones de luz durante aproximadamente una hora en ciudades como Tel Aviv, Jerusalem, Ashdod y Haifa. Un académico islámico iraní expresó en un sermón reciente que "la fuerza cibernética de Irán llevó a cabo al menos dos ataques contra Israel este año, el reciente dirigido con éxito a las plantas de energía" en Israel (AJN, 2020).

Así las cosas, sin disparar un misil, pero con alto nivel de afectación a la población, los ciberataques se abren paso, como es el caso de Irán e Israel, dos países antagonistas que llevan realizando labores de ciber espionaje y ataques cibernéticos el uno contra el otro durante los últimos años. Para Lior Frenkel, presidente del Foro de Empresas Cibernéticas de Israel, "los ataques de Irán contra Israel continuarán".

> Es solo cuestión de tiempo hasta que se produzca otro ataque informático contra compañías industriales y de infraestructura en el país (…) los iraníes preferirán

llevar a cabo operaciones relativamente "pequeñas", como apagar el sistema de semáforos en Tel Aviv, antes que derribar un avión israelí (Ynet, 2021).

Conclusión de los casos

De esta manera, lo visto en Irán, Estados Unidos e Israel, se han atribuido ataques cibernéticos procedentes de cada uno de estos países, aunque no se sabe la responsabilidad directa del gobierno de cada uno de estos, lo que sí es claro es que se encuentran inmersos en una serie de ciberataques desde hace ya más de una década que corresponde a un conflicto basado principalmente por las tensiones vividas en la región de Oriente Medio, el programa Nuclear de Irán y un conflicto histórico.

Los ataques cibernéticos a la central nuclear en Natanz vividos desde hace más de 10 años, coinciden con el interés de Estados Unidos y de Israel para que Irán no continúe con la intención de crear armas nucleares. Por su parte, los ataques provenientes desde la República Islámica han demostrado que pueden paralizar la vida cotidiana de un Estado tan pequeño, pero tan estratégico como Israel. Una serie de ciberataques que dan a entender una pequeña prueba del riesgo en que cada país puede estar por ataques que provienen del ciberespacio. Así las cosas, para Estados Unidos, Israel e Irán, la ciberseguridad se ha convertido en un papel importante y esta permitirá defenderse de los diferentes ciberataques que seguirán ocurriendo.

Cierre del primer capítulo

Después de diferentes casos en los que estuvieron involucrados los 4 Estados de referencia, se puede concluir, como ya se mencionó, que es difícil atribuir los ataques cibernéticos a un gobierno en particular. Sin embargo, en muchos de ellos pareciera haber un beneficio directo de cada Estado con los diferentes ataques, como evidenciábamos con los ataques de Rusia, por ejemplo.

Por otra parte, y sobre la pregunta de este primer capítulo: *El ciberespacio ¿Por qué se convierte en un escenario de conflicto para los actores estatales?* podemos

concluir, que el ciberespacio es un escenario que permite a los actores estatales equilibrar sus cargas, pues en un conflicto convencional se requieren muchos más recursos y generalmente, quienes tengan el mayor poderío militar son quienes se imponen. No obstante, el ciberespacio permite realizar daños a pequeña y gran escala con recursos más limitados, como es el caso de la República Popular Democrática de Corea, que incluso le ha permitido tener réditos económicos.

Además de lo anterior, el ciberespacio es visto actualmente por los actores estatales como un escenario de conflicto y por esto, han decidido invertir cada vez más en programas de ciberseguridad, como lo es el caso del pentágono de Estados Unidos que, desde hace una década, ve al ciberespacio como un nuevo ámbito de la guerra y se planteó estrategias para operar en el ciberespacio (Márquez, 2011). Similar a esto, Irán como mencionábamos durante el capítulo decidió crear un "ejército cibernético", que les permitieran no solo contrarrestar ataques sino responder ante posibles amenazas.

Igualmente, los casos de referencia permiten evidenciar que "casualmente" cada uno de los ataques cibernéticos originados desde los 4 Estados en estudio, les generó a cada uno de ellos algún tipo de beneficio a largo o corto plazo, como por ejemplo Corea del Norte y China que se benefician directamente de los ataques, de manera económica y política. Incluso, se puede hablar de beneficios circunstanciales, demasiado convenientes para la situación como Rusia con sus conflictos en Estonia y Georgia.

Finalmente, aun cuando el ciberespacio puede ser visto como un escenario de conflicto entre los actores estatales, no podemos decir que se ha llevado a cabo alguna ciberguerra. Lo ocurrido entre Irán, Israel y Estados Unidos, nos demuestra una serie de ataques en la red que no han llevado a una confrontación directa, por lo menos por el momento. O incluso, lo visto en Estonia y Georgia, detalla una guerra híbrida con ataques convencionales que se combinan con ataques cibernéticos. La ciberembajadora de Estonia, Heli Tiirmaa-Klaar, piensa que no habrá ninguna ciberguerra. Asegura que habrá una guerra real con una faceta ciber y que siempre hay una razón política que pueda llevar a un ataque entre Estados (El País, 2020).

Capítulo II

Actores no estatales en el ciberespacio ¿Cuáles son sus intereses?

El ciberespacio, como se señaló en el capítulo anterior, ha tomado gran importancia para la sociedad actual. El desarrollo de la Internet y su acelerado uso ha hecho que sea escenario de preocupación para los Gobiernos y sus fuerzas armadas, los cuales empezaron a desarrollar estrategias de ciberdefensa. Es así que, algunas características especiales como su naturaleza asimétrica, la dificultad para atribuir ataques, su bajo costo, la ambigüedad legal y su papel como medio más que eficiente para generar protestas, crimen, espionaje y agresiones, hacen del mundo virtual un escenario atractivo para los actores estatales, tal como pudimos ver en el capítulo anterior, pero también para los actores no estatales (Sigholm, 2016).

De esta manera, en el presente capítulo, analizaremos el papel de los actores no estatales en el mundo virtual. Para esto, se debe partir de la idea de que el conocimiento tecnológico no es exclusivo de los Estados y sus centrales de inteligencias asociadas. Actualmente, los actores no estatales pueden irrumpir en las redes informáticas, conseguir información financiera y militar, propagar noticias falsas, inhabilitar páginas web estatales, entre otras actividades que los lleven a alcanzar sus intereses (Berenicefn, 2018).

El Ciberespacio es de dominio global, ya que cualquier persona con acceso a la Internet puede acceder a él. En este mundo virtual, coexisten diversos actores con diferentes necesidades y objetivos, como observaremos en el gráfico posterior. Algunos de estos actores pueden actuar solos, otros con estructuras más formales, pero en ambos casos, utilizan el mundo virtual como un escenario que permite ser más imperceptible, un escenario que no refleja los mismos patrones del mundo real, como se recoge de las palabras de Clotet (2010):

> Internet se revela como un mundo virtual donde no existen los mismos patrones sociales del mundo real, un mundo al que nos asomamos ocultos tras la pantalla, creyendo ser anónimos y asumiendo nuevos roles. Donde la protección que ofrece

la facilidad de crear identidades ficticias supone un acicate o desinhibidor de nuestros temores frente a las barreras sociales, impulsándonos a veces a superar la legalidad establecida (Clotet, 2010, p. 135).

Gráfico 12

Actor	Motivación	Blanco objetivo
Ciudadano común	Ninguno (Débil)	Cualquiera
Script Kiddies	Curiosidad, emociones, ego	Personas, compañías, gobiernos
Hacktivistas	Cambio político o social	Tomadores de decisiones o víctimas inocentes
Hackers de sombrero negro	Ego, diversión, ganancia económica	Cualquiera
Hackers de sombrero blanco	Idealismo, creatividad, respecto a la ley	Cualquiera
Hackers de sombrero gris	Ambiguo	Cualquiera
Hackers patriotas	Patriotismo	Adversarios de su propio país
Cyber Insiders	Ganancia económica, venganza, protesta	Empleador
Terroristas cibernéticos	Cambio político o social	Víctimas inocentes
Creadores de Malware	Ganancia económica, ego, diversión	Cualquiera
Estafadores cibernéticos	Ganancia financiera	Personas, compañías pequeñas
Ciber criminales organizados	Ganancia financiera	Personas, compañías
Corporaciones	Ganancia financiera	Infraestructura privada y pública, sistemas basados en tecnologías de la información
Agentes de ciber espionaje	Ganancias financieras y políticas	Personas, compañías y gobiernos
Milicias cibernéticas	Patriotismo, desarrollo profesional	Adversarios de su propio país

*Traducido de Sigholm, 2016

El gráfico anterior nos muestra como diferentes actores no estatales coexisten en el ciberespacio, cada uno con motivaciones, objetivos y métodos diferentes. Los actores no estatales, solo por nombrar algunos, pueden ser desde: 1) un ciudadano común sin un interés u objetivo específico; 2) *Hacktivistas,* como se podrían catalogar por ejemplo a *Anonymous* y *Wikileaks*, los cuales pueden actuar solos o con estructuras más organizadas, pero que en general son motivados por una insatisfacción social o política. 3) *Hackers,* los cuales pueden ser de diferentes categorías y al mismo tiempo con diferentes motivaciones como económicas o el patriotismo. 4) milicias cibernéticas, las cuales pueden estar motivados por el patriotismo, el desarrollo profesional y sus objetivos son los adversarios de sus propios Estados.

Aunado a los anterior y teniendo en cuenta los actores no estatales mencionados, nos centraremos en la definición de los siguientes términos: Hacktivistas, *Hackers,* Milicias cibernéticas y corporaciones por considerar a estos 4 actores de gran relevancia a la hora de abordar los casos que se estudiarán posteriormente en este capítulo.

Hacktivistas

El término hacktivista, el cual proviene de las palabras *hacker* y activismo, es definido por Avogrado (2011) como "el activismo político realizado por personas idóneas en informática, que generan estos movimientos políticos desde sitios electrónicos ubicados en internet". Para otros autores como Burgos (2014) "el hacktivismo es una forma emergente de acción social que pretende cuestionar y transformar el orden social existente a través del activismo tecnológico. Dicho activismo se sustenta en los principios de la socialización del conocimiento, la cooperación tecnológica y la autogestión comunicacional".

Dicho lo anterior, el hacktivismo puede verse como una acción de irrupción en la red para difundir algún tipo de mensaje social o político. No obstante, no hay que dejar de lado que los hacktivistas han ido evolucionando al mismo tiempo que la Internet. Así las cosas, "a medida que internet conecta cada vez más cosas y personas, es más atractivo utilizar estas habilidades para hacer llegar más lejos un mensaje político". Es así como se

evidencia también un elemento trasnacional del *hacktivismo*, al ser movimientos sociales que trascienden fronteras y que se involucran en causas sociales o políticas más allá del país desde donde se origina la acción hacktivista. (Rodriguez, 2020).

Gráfico 13

1989	**El *"WANK worm"*** Una infiltración en la red de computadores de la NASA en protesta de las armas nucleares y el uso de plutonio radioactivo como combustible para el sistema de refuerzo de Sonda de *Galileo.*
1995	***The Strano Network sit-in*** Una huelga dirigida contra los computadores del gobierno francés como protesta a las políticas sobre problemas nucleares y sociales.
1998	**Hackeos de caos urbano** Desconfiguración de los sitios web del gobierno de Indonesia focalizados en la opresión de los habitantes de Timor Oriental
1998	**Disturbios electrónicos *"Web Sit-ins"*** Ataques de negación de servicio, a las páginas web del pentágono y del gobierno mexicano, en apoyo a los zapatistas.
1999	**Equipo *Sploit* hackeos anti guerra** Desconfiguración web para llamar al fin del conflicto en Kosovo

*Traducido de Sigholm, 2016

El gráfico anterior, tomado de Sigholm 2016 *"Non-State Actors in Cyberspace Operations"* recoge las primeras acciones hacktivistas, las cuales tenían un mensaje de oposición a las armas nucleares como la infiltración a la red de la NASA en 1989, el apoyo a un grupo que exigía mayor reconocimiento de derechos para los pueblos indígenas mexicanos, como los zapatistas en 1998 o el mensaje pidiendo finalizar el conflicto en Kosovo en 1999.

De esta manera, se puede evidenciar como los hacktivistas han desarrollado sus acciones desde el mismo año (1989) en que fue creada la tecnología *World Wide Web* (WWW). Esto para demostrar que el progreso mismo de la Internet ha ido de la mano de la utilización misma de los diferentes actores para alcanzar sus intereses, como lo es en este caso específico de los hacktivistas, manifestar su insatisfacción social o política.

Actualmente, el grupo hacktivista más importante es *Anonymous*, cuya imagen está inspirada en la película *V de Venganza*, busca forzar los cambios que quieren ver en

el sistema, accediendo y atacando las redes de comunicaciones de otros; los cuales pueden ser ataques a organizaciones, como el caso del ataque a la iglesia de la cienciología en 2008 o el ataque a miembros del *Ku Klux Klan* en Estados Unidos. Igualmente, si bien los hacktivistas actúan solos y no están afiliados a ningún Estado, en algunas ocasiones, Estados y hacktivistas encuentran objetivos comunes como por ejemplo el ataque de *Anonymous* en 2015 contra el grupo terrorista *Dáesh,* tras los atentados a la revista *Charlie Hebdó* en París; el cual logró desactivar miles de usuarios de *Twitte*r, páginas web y videos relacionados con el grupo yihadista (Rodriguez, 2020).

Aunado a lo anterior, también se pueden mencionar manifestaciones más recientes de hacktivismo, como por ejemplo las realizadas por un grupo de fans del K-pop surcoreano, denominado *los K-popers.* Este grupo, "de manera coordinada se han encargado de modificar las tendencias en *Twitter* posicionadas por los grupos de derecha más radical. Con ese norte, ingresaron a Colombia para hacer frente a los *hashtags* que apoyan los discursos oficiales en contra de las protestas sociales ocurridas desde el 28 de abril". Este grupo también ha tenido participación en protestas por acciones sociales no solo en Colombia, sino que también se conoce de su participación en apoyo al movimiento #BlackLivesMatters en Estados Unidos (Galindo y Rivero, 2021).

Hackers

En palabras de Clotet (2010), la palabra *hacker* se origina **"**en la vulneración de las redes telefónicas para efectuar llamadas gratuitas, accediendo a centrales o interceptando llamadas, con la extensión de la red para uso de la comunidad universitaria y científica". Para Salcedo et al. (2011) "Inicialmente, se les llamaba *hackers* a los técnicos de telefonía por la forma en que solían reparar los teléfonos. Mediante un golpe seco y certero ponían de nuevo en marcha el teléfono (*hack* es hachazo en inglés)".

No obstante, la palabra *hacker* ha mutado en su significado y luego se asoció "al *hacker* con el experto informático que era capaz de detectar los fallos de programación y entrar en los sistemas informáticos vulnerando las medidas de seguridad" (Clotet, 2010). Este cambio en su significado se asemeja a la de Sigholm 2016, quien lo define como las

personas con un profundo conocimiento de la tecnología, que conocen cómo interactúa el *hardware*, *software* y la red. Sin embargo, INTECO -Instituto Nacional de Tecnologías de la Comunicación- de España, establece que:

> Actualmente, el término *hacker* puede tener connotaciones positivas y negativas en función del concepto que se maneje. Así, la palabra se utiliza tanto para definir a un desarrollador de software apasionado por la informática que depura y arregla errores en los sistemas, como para referirse a aquel que se infiltra en un sistema informático con el fin de eludir o desactivar las medidas de seguridad (INTECO, s,f, p. 1).

Así las cosas, la palabra *hacker* puede tener una visión positiva o negativa, ya que dependiendo de sus intereses se clasificarán según el "el color de su sombrero". *Hackers* de sombrero blanco, negro o gris. En primer lugar, los *hackers de sombrero blanco,* o *hackers* éticos, son aquellos que se especializan en probar sistemas empresariales, gubernamentales o particulares con el fin de garantizar la seguridad cibernética de los sistemas web. Por otra parte, están los *hackers de sombrero negro,* son personas que explotan sus conocimientos de sistemas computacionales y la red para su propio beneficio, actúan sin respeto de la ley y son vistos como actores más malignos en la esfera de los *hackers*. Finalmente están los *hackers de sombrero gris,* son aquellas personas que hacen tanto acciones de testeo de sistemas como acciones delictivas, son una especie de híbrido entre las dos clases de *hackers* anteriormente mencionadas (Sigholm 2016).

Otra categoría de *hackers*, son los *hackers patriotas*, los cuales son aquellas personas que su principal motivación son ayudar a su propio Estado, por ejemplo, en una guerra real o conflicto y por lo tanto llevan acciones contra el adversario. Un ejemplo de estos son el denominado "*Honker Union of China*" quienes han publicado un manifiesto expresando su misión patriótica a favor de los intereses del gobierno chino.

Milicias cibernéticas

Las milicias cibernéticas o ciber milicias son definidas por Sigholm (2016), como un grupo de voluntarios que realizan ciberataques con el fin de alcanzar un objetivo político. Igualmente, y como se observa en el gráfico 12, sus motivaciones son también de índole patriótico y su objetivo son los adversarios de su propio Estado. Por otra parte, las milicias cibernéticas, como establece Bejarano (2011) pueden ser una fuerza útil del poder en el ciberespacio que puede tener un Estado.

> (…) una cibermilicia donde los miembros se comunican principalmente vía Internet y como norma, esconden su identidad. Lo que estos ciberguerreros puedan carecer en formación y recursos, lo suplen con su número. Sin embargo, incluso una cibermilicia *ad-hoc* que no está bajo control directo de un estado puede ser una extensión útil del poder cibernético de un estado. Por otra parte, ellos también pueden convertirse en una amenaza a la seguridad nacional. Debido a la naturaleza global de Internet, esta amenaza proviene probablemente de múltiples jurisdicciones, lo que limita la aplicación de la ley o las opciones militares del estado (Bejarano, 2011, p. 57).

Corporaciones

Por otra parte, otro actor no estatal a considerar son las corporaciones. Usualmente, las corporaciones que actúan en el ciberespacio son entidades que respetan la ley y esto las hace diferentes a una organización de crimen organizado. Sin embargo, las corporaciones pueden llevar a cabo actividades, en algunas ocasiones, auspiciadas por actores estatales en las que se encuentran acciones de ciberespionaje o tráfico de datos. (Sigholm 2016).

Estas acciones realizadas por las corporaciones son realizadas a través de los medios de comunicación o*nline* y las redes sociales, las cuales son usadas como herramienta para alcanzar sus intereses. Para Díaz (2016), "la capacidad de acción de los medios de comunicación sobre el sistema internacional se ve reflejada a través de bases

teóricas que sustentan su mutua dependencia para lograr su fin último: la interacción y conectividad.”. De esta manera, los medios de comunicación como herramienta de actores no estatales, como las corporaciones, pueden tener el fin de unir a las personas en pro de un objetivo social o político.

Ahora bien, podemos entender que los actores no estatales, son diversos y actúan motivados por diferentes intereses, ya sean de orden político, social o económico. Sin embargo, algo que también es claro es que cualquier persona, ya sea un ciudadano de a pie, un *hacker*, un hacktivista o un integrante de una milicia cibernética puede acceder a la red; no obstante, el grado de conocimiento informático y del ciberespacio influirá en el tipo de acción que pueda realizar.

Las acciones que un actor no estatal puede realizar en el ciberespacio pueden variar desde ataques elaborados, campañas de ciberactivismo o simplemente replicar una noticia falsa. Según Soler (2020), una gran amenaza para la ciberseguridad son las campañas de desinformación, pues para ella, la información errada difundida de manera intencionada hace que mueva más a las personas que la información objetiva. En este escenario, el ciberespacio juega un papel muy importante pues permite que las noticias falsas vayan a una gran velocidad de transmisión y hace que tengan un mayor alcance.

Otra acción que puede ser ejecutada por los actores no estatales en el mundo virtual es el ciberactivismo; que comenzó gracias a los *hackers* que buscaban defender una causa específica; pero que ha ido evolucionado a la par de la Internet y hoy tiene como principal herramienta las redes sociales. podríamos decir que el hacktivismo es una especie dentro del género "ciberactivismo" como veremos en la segunda parte del presente capítulo, ya que este último puede ser llevado a cabo no solo por *hackers*, sino también por organizaciones, individuos del común o grupos de personas. González (2015) establece que:

> El activismo en red, cuyo origen lo encontramos en el hacktivismo, utiliza redes sociales y *blogs* para la realización de acciones que llamen la atención de la sociedad y así intentar conseguir cambios políticos o legislativos, es decir, usar

> las herramientas de las web 2.0 para conseguir un espacio de difusión de ideas y debate (…) al tiempo que origina un nuevo tipo de ciudadano, el ciudadano digital que reclama nuevos espacios y escenarios para el debate público y que encuentra en la red un espacio idóneo para expresarse con libertad, evitando censuras, pudiendo coordinarse para trabajar de forma colectiva (González, 2015, párr. 29).

Así las cosas, tanto las campañas de desinformación - noticias falsas- y el ciberactivismo, son herramientas que hoy los actores no estatales han utilizado para alcanzar sus objetivos. Una persona común o una organización puede difundir una noticia falsa con el objetivo de desacreditar a un aspirante a la presidencia, o un grupo hacktivista, por ejemplo, puede promover protestas en contra del dominio de China sobre Hong Kong.

De esta manera, en el presente capítulo se analizará específicamente las noticias falsas y el ciberactivismo como medios usados por los actores no estatales para alcanzar sus intereses, los cuales en ocasiones pueden ser difícil de identificar, no obstante, y según Sigholm (2016) los intereses pueden ser de orden político, social y/o económico. Es por eso, que en los siguientes párrafos profundizaremos sobre estos términos y se expondrán casos en que los actores no estatales se han beneficiado de estos. Igualmente, se utilizarán como referencia los actores no estatales que actúan o tienen repercusión en los Estados mencionados en el primer capítulo.

2.1 Noticias falsas

En 2017, "noticias falsas" o su nombre en inglés "*fake news*" se convirtió en la expresión del año del *Collins Dictionary* y ha permanecido en los titulares desde entonces. Aunque la frase pueda parecer una invención moderna, se pueden encontrar ejemplos a lo largo de la historia. Desde la antigua Roma hasta la actualidad, los relatos que no son ciertos o los hechos tergiversados que buscan desinformar al público, se han utilizado para ganar dinero, cambiar los puntos de vista y las opiniones de las personas y hacerlas cuestionarse sobre en quién pueden confiar. Ahora, con la explosión de la Internet y las redes sociales, las "*fake news*" parecen estar en todas partes y viajar más rápido que en cualquier otro momento de la historia (BBC, s.f.).

Hace más de 2000 años, previo al establecimiento del Imperio Romano en el año 27 antes de Cristo, la antigua Roma enfrentaba una guerra civil por el poder entre Octavio, el hijo adoptivo del general Julio César, y Marco Antonio, uno de los comandantes de mayor confianza de César. Para ganar la guerra, Octavio sabía que tenía que tener al público de su lado. Por eso, con el fin de obtener su respaldo, Octavio lanzó una guerra de noticias falsas contra Marco Antonio. Afirmó que Antonio estaba teniendo una aventura con la reina egipcia Cleopatra y que no respetaba los valores romanos tradicionales como la fidelidad y el respeto; también difundió que Antonio no era apto para ocupar el cargo porque siempre estaba borracho. Hizo llegar sus mensajes al público romano a través de poesías y lemas breves impresos en monedas. La estrategia de Octavio dio resultado, finalmente ganó la guerra y se convirtió en el primer emperador de Roma, pasándose a llamar César Augusto y gobernando durante más de 40 años (BBC, s.f.).

Lo anterior nos hace pensar en la enseñanza que nos dejó Nicolás Maquiavelo en su obra maestra: El Príncipe. “Los hombres son tan simples y de tal manera obedecen a las necesidades del momento, que aquel que engaña encontrará siempre quien se deje engañar”. Adaptando esa sabiduría al tema que nos atañe en este momento, los creadores de noticias falsas siempre tienen en cuenta “las necesidades del momento” y con base en ellas, fabrican la noticia con un fin específico y siempre van a encontrar un público que las cree y además las difunde.

Después de la invención de la imprenta en el siglo XV, las noticias lograron difundirse más fácilmente, los libros y otros documentos se podían producir mucho más rápido que cualquier escritura a mano. A mediados del siglo XVIII esa tecnología fue aprovechada para difundir noticias falsas sobre George II, quien era el rey de Gran Bretaña e Irlanda en ese momento. El rey se enfrentaba a una rebelión y confiaba en ser visto como un líder fuerte; en vista de la situación, los rebeldes empezaron a imprimir noticias falsas sobre una supuesta enfermedad grave del rey y no pasó mucho tiempo antes de que estas historias fueran vistas por otros impresores que luego las volvieron a publicar. Esto dañó la imagen pública del Rey y, aunque la rebelión fue un fracaso, demostró cómo se pueden utilizar las “*fake news*” para intentar cambiar la opinión de las

personas y de cómo una información falsa puede ser reproducida por otros sujetos u organizaciones que piensan que es cierta (BBC, s.f.).

En el siglo XIX, los periódicos eran una forma eficaz y barata de hacer llegar las noticias al público. En Estados Unidos, la impresión se volvió tan barata que algunos diarios se podían comprar por un centavo de dólar. El periódico *The New York Sun* publicó una serie de artículos en 1835 sobre la vida en la luna, afirmaron que había animales fantásticos como unicornios, castores de dos patas e incluso hombres murciélago voladores. Además, aseguraron erróneamente que los descubrimientos fueron hechos por un astrónomo conocido en ese momento, lo que ayudó a las personas a creer que la historia era cierta. (BBC, s.f.). Según afirma Carlos Salas Abad (2019) en su artículo "*La primera fake news de la historia*" publicado por la Universidad Complutense de Madrid, esta fue la primera noticia falsa de la historia contemporánea "porque fue la primera mentira difundida en gran escala gracias a la combinación de los nuevos medios de comunicación y transporte de masas: desde trenes, hasta barcos de vapor y, por supuesto, las rotativas de alta velocidad (que redujeron los precios por copia) y los niños voceadores".

Todo lo anterior sirvió para fortalecer el término "*fake news*". El paso del tiempo y la aparición de nuevos avances tecnológicos hicieron mucho más fácil y barata la reproducción de información falsa. Tal como lo expresa Salas (2019):

> Los contenidos de las plataformas son baratos (radio, televisión, y ahora internet con las redes sociales), y el avance de la tecnología reduce los precios de acceso: los teléfonos móviles y las tarifas de conexión son baratas. A principios del siglo XIX no existían móviles ni redes sociales, pero sí tuvo lugar un salto histórico en los medios de comunicación cuando arrancaron las inmensas rotativas de alta velocidad, que bajaron el precio de los periódicos a un nivel nunca visto (Salas, 2019, p. 424).

Ahora, en la segunda década del siglo XXI, cualquier individuo con acceso a la Internet y redes sociales puede fabricar y difundir sus propias noticias falsas en el ciberespacio.

Lo que es innegable es que las noticias falsas amenazan a la libertad de prensa y al periodismo y tienen el poder de distorsionar la realidad y de impactar en la vida de las personas, como quedó demostrado tras las elecciones de Estados Unidos y el referendo del Brexit, ambos en 2016 (La Voz de Galicia, 2017). Las campañas para esas votaciones estuvieron llenas de información falsa en las redes sociales. En Estados Unidos se difundió, entre otras "*fake news*", que la candidata Hillary Clinton estaba asociada a una red de prostitución infantil, cuya sede era una pizzería en Washington. La noticia falsa trascendió tanto que un hombre llamado Edgar Maddison Welch abrió fuego contra la pizzería para "acabar por cuenta propia" con la presunta red de prostitución infantil vinculada a Clinton (DW, 2016).

Las '*fake news'* también formaron parte del debate sobre el Brexit todo el tiempo. Una de ellas fue sobre un tema tan sensible como la migración; los argumentos recurrían al miedo y a asegurar que la gente se quedaría sin trabajo si no se detenía el flujo de migrantes, sin aportar cifras ni explicar que su cotización como trabajadores aporta riqueza al país (La Vanguardia, 2020). Finalmente, Donald Trump resultó elegido presidente de Estados Unidos y el Reino Unido votó por abandonar la Unión Europea.

El término *"fake news*" se popularizó precisamente gracias a Donald Trump, quien lo utilizaba para referirse a cualquier noticia o publicación en la que era criticado y así restarle importancia. Durante una entrevista a la cadena CNN posterior a su victoria en las elecciones expresó lo siguiente sobre las noticias falsas: "No he inventado el término, porque creo que otras personas lo han usado a lo largo de los años, pero nunca lo había notado. Lo que sí he hecho es darle visibilidad, porque lamentablemente nuestro país está plagado de ellas y es una pena" (La Voz de Galicia, 2017).

La propagación de noticias falsas aumenta día a día. Por esa razón, redes sociales como *Facebook, Twitter* e *Instagram* trabajan constantemente con iniciativas para

combatir las *fake news* con la ayuda de denuncias y reportes de los usuarios. Un estudio realizado por la ONG Avaaz reveló que las 100 noticias falsas más populares que circularon en *Facebook*, entre enero y octubre de 2019, fueron vistas 159 millones de veces en total. Obtuvieron 8,9 millones de interacciones entre comentarios, me gusta o compartir. Además, fueron publicadas 2,3 millones de veces por parte de los mismos usuarios de *Facebook* (Avast Security, 2019).

Facebook anunció en 2019 una nueva herramienta para combatir la desinformación y propagación de noticias falsas. Se trata de una nueva pestaña que muestra a los usuarios de la red social noticias revisadas por periodistas de medios creíbles, entre los que se encuentran: *The Washington Post*, *Bloomberg*, *BuzzFeed News*, *Business Insider*, y *Los Angeles Times*. Sin embargo, a pesar de los esfuerzos de *Facebook* para combatir las noticias falsas, el Laboratorio de Periodismo Nieman de la Universidad de Harvard asegura que es fácil para los usuarios compartir las publicaciones que la red social ya ha marcado como "*fake news*". Un investigador del Laboratorio intentó buscar y compartir las 20 noticias falsas más vistas en 2019 en *Facebook*, lo cual pudo hacer con éxito (Avast Security, 2019).

Por otro lado, desde el 22 de noviembre de 2019 entró en vigor una nueva política en *Twitter* para detener las "*fake news*" y evitar la influencia de terceros en las decisiones de los usuarios en futuras elecciones. La medida fue anunciada por su director ejecutivo, Jack Dorsey, quien informó que quedaba prohibida la publicidad política dentro de la red social a nivel mundial. Asimismo, *Instagram* también trabaja para combatir las noticias falsas dentro de su plataforma con etiquetas para clasificar el contenido y evitar la propagación del mismo. La aplicación muestra etiquetas que advierten a los usuarios sobre el contenido con información falsa; no obstante, "los usuarios tendrán la opción de visualizar el contenido si así lo desean. Si el usuario quiere compartir contenido falso, también será advertido sobre la publicación, esto no impedirá que sea compartida, pero tendrá la misma etiqueta para otros usuarios" (Avast Security, 2019).

Es tanta la repercusión que ha tenido el fenómeno de las noticias falsas que se ha convertido en un problema global. Una muestra de ello está en que el organismo

multilateral más importante del planeta, la Organización de Naciones unidas, a través de la UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura) encargó en 2017 a un grupo de expertos la elaboración de un manual que ayudara a los periodistas y al público en general, a identificar las noticias falsas y combatir la desinformación.

En septiembre de 2018, finalmente fue publicado el libro "Periodismo, Noticias Falsas y Desinformación", que se considera como el primer acto mundial de investigación colaborativa e intercambio de conocimientos que involucra a destacados expertos internacionales en materia de lucha contra la desinformación y las noticias falsas. La ONU lanzó el manual con el objetivo de ayudar a equipar al periodismo para abordar el problema de lo que denominan "desorden de la información". El libro fue editado por la periodista australiana Julie Posetti, investigadora principal del Instituto *Reuters* para el Estudio del Periodismo de la Universidad de Oxford, y la sudafricana Cherilyn Ireton, directora ejecutiva del Foro Mundial de Editores (Nieman Lab, Harvard University, 2018)

En los siguientes subtítulos estaremos analizando cómo los actores no estatales usan la Internet como herramienta para alcanzar sus intereses, valiéndose de la difusión de noticias falsas en el ciberespacio, con las que pueden resultar perjudicados actores estatales o tener algún tipo de incidencia en ellos. Estudiaremos este fenómeno desde la perspectiva de cuatro países: Corea del Norte, China, Rusia e Irán.

2.1.1 Noticias falsas sobre Corea del Norte

El régimen norcoreano maneja todos los aspectos de la vida de sus ciudadanos, quienes tienen un acceso restringido a internet, con la prohibición de ver contenido extranjero. Por esa razón y las posibles consecuencias de despertar la furia de la familia Kim, probablemente el fenómeno de las noticias falsas no sea muy común al interior del país. Sin embargo, si no ha sido por internet, es posible que alguna vez se hayan presentado *fake news* difundidas por otros medios al interior de la sociedad norcoreana; pero resulta difícil saberlo por lo hermético del régimen liderado por Kim Jong-un.

El servicio de internet en Corea del Norte está dividido en dos redes. Los estudiantes más brillantes reciben formación sobre el uso de internet en instituciones cuyas conexiones están monitoreadas. El resto de los ciudadanos se tiene que conformar con una intranet norcoreana llamada *Kwangmyong*, que provee una versión limitada de la información. De todas formas, ambas redes son controladas y vigiladas por el Estado (BBC, 2014).

Lo que sí es una realidad, como veremos en los siguientes casos, es que el régimen de la República Popular Democrática de Corea ha sido víctima de diversas noticias falsas, provenientes principalmente de un medio de comunicación de Corea del Sur. Estas *fake news* podrían ser difundidas con fines políticos, como aumentar aún más la imagen negativa del régimen a nivel internacional; o con fines económicos, como el de generar *rating*.

Caso 1: *Chosun Ilbo* contra Corea del Norte

Fundado en 1920, el *Chosun Ilbo*, de corte conservador nacionalista, es uno de los principales medios de comunicación de Corea del Sur. Con la evolución de la Internet, el diario no solamente sigue circulando en su versión física en todo el territorio surcoreano, sino que también cuenta con un portal web de noticias, con versiones en coreano, inglés, chino y japonés; lo que da cuenta del enorme público al que puede llegar.

En su página web oficial, el *Chosun Ilbo* expresa su punto de vista corporativo sobre las noticias falsas:

> El panorama de los medios está cambiando rápidamente e internet está repleto de información inexacta y rumores no confirmados. Pero incluso en estos tiempos tumultuosos, hemos seguido manteniendo la precisión para estar a la altura de las expectativas de nuestros lectores. Creemos que nuestros esfuerzos para proporcionar relatos justos y precisos de los eventos, así como un análisis en profundidad y comentarios de expertos sobre los problemas que afectan a la

sociedad, y los editoriales lúcidos que eliminan los prejuicios son las piedras angulares de nuestro distinguido contenido (Chosun Ilbo s.f.).

No obstante, este medio informativo se ha visto envuelto en polémicas por la publicación de noticias falsas que, por el prestigio que ha gozado a través de los años a nivel nacional e internacional, son reproducidas por medios de comunicación de todos los continentes y replicadas sin control en las redes sociales; particularmente sobre Corea del Norte y su líder Kim Kong-un.

Una noticia publicada por *Chosun Ilbo* a finales de mayo de 2019 dio la vuelta al planeta. En ella se afirmaba que Kim Jong-un había ejecutado a su enviado especial para los Estados Unidos, Kim Hyok-chol, cuando regresaba de la fallida cumbre con Estados Unidos en Hanoi en febrero de 2019. En el diario también se afirmó que otros ejecutivos de alto rango del partido fueron enviados a campamentos de "reeducación", incluido Kim Yong-chol, quien era considerado la mano derecha del líder norcoreano. Unos minutos después de la publicación de la noticia, la agencia *Reuters* replicó la historia, seguida por el *New York Times*. La historia se difundió en las redes sociales y aterrizó en innumerables periódicos locales y nacionales en todo el mundo a través de varias agencias de noticias, todos citando la fuente surcoreana (DW, 2019).

Gráfico 14

*Tomado de *Chosun Ilbo*, 2019.

Sin embargo, a los pocos días de publicada la noticia, Kim Yong-chol, reapareció en un programa de televisión de la agencia estatal de noticias de Corea del Norte (KCNA), no en un campo de trabajo, sino en un concierto de ópera junto a otros funcionarios de alto rango del partido; y según Chad O'Carroll, editor en jefe de *NK News*, un portal especializado en noticias e información sobre Corea del Norte, Kim Hyok-chol también fue visto posteriormente en el Ministerio de Relaciones Exteriores en Pyongyang. Lo que hacía constatar la falsedad de la noticia del *Chosun Ilbo* y que los medios internacionales más importantes tuvieran que retractarse de lo publicado (DW, 2019).

Pero la historia de la falsa ejecución en 2019 no ha sido la única "fake news" publicada por el medio surcoreano en internet. Otras noticias tuvieron similar desenlace; como aquella en la que informaron en 2013 que Kim Jong-un había ejecutado a su exnovia, la cantante Hyon Song-wol, por violar la ley de pornografía. Poco tiempo después, la cantante, también miembro del Comité Central del Partido de los Trabajadores, apareció en televisión dejando al descubierto la mentira del *Chosun Ilbo*. Asimismo, en 2014 publicaron la noticia de que el Líder Supremo hizo que 120 perros hambrientos se comieran a su tío, Jang Song-thaek; lo cual resultó ser un engaño. De lo único que hay certeza es de que Jang Song-thaek fue asesinado, pero no de esa forma (DW, 2019).

Lo anterior nos permite deducir la "guerra" de este medio de comunicación contra el régimen norcoreano, y también su pérdida de credibilidad como fuente para buscar información sobre Corea del Norte, país al que, como se puede observar en el gráfico 14, dedica una sección exclusiva en su página web. Ahora los medios informativos internacionales más importantes lo pensarán más de una vez para citar al *Chosun Ilbo*.

Caso 2: La enfermedad y muerte de Kim Jong-un

Otras noticias que involucran a Corea del Norte, y que tuvieron gran trascendencia a nivel mundial en abril de 2020, fueron las de la enfermedad y posterior muerte de su líder supremo, Kim Jong-un. El primer medio en publicar la noticia sobre la enfermedad de Kim fue el diario digital especializado en noticias sobre Corea del Norte, *Daily NK,*

con sede en Seúl. La noticia se fue regando como una bola de nieve y a los pocos días la televisora HKSTV de Hong Kong anunció la muerte del líder norcoreano. Las noticias se reprodujeron sin control en medios de todo el mundo y en las redes sociales.

Según *Daily NK*, integrado por varios desertores del régimen norcoreano, Kim Jong-un estaba recibiendo tratamiento después de someterse a un procedimiento cardiovascular el 12 de abril de 2020. El diario digital afirmó que la salud de Kim se había deteriorado en los últimos meses debido al tabaquismo, la obesidad y el exceso del trabajo. La ausencia de Kim Jong-un durante el cumpleaños de su padre y abuelo el 15 de abril, día establecido como celebración nacional, generó especulaciones sobre su estado de salud (Forbes, 2017).

En noticia publicada en el portal web de CNN y sus cuentas oficiales en redes sociales como *Facebook*, *Twitter* e *Instagram,* el 21 de abril de 2020, se refuerza la información de *Daily NK* con fuentes supuestamente cercanas al Gobierno de Estados Unidos.

> Estados Unidos está monitoreando inteligencia que sugiere que el líder de Corea del Norte, Kim Jong Un, está en grave peligro después de someterse a una cirugía previa, según un funcionario estadounidense con conocimiento directo. Una segunda fuente familiarizada con la inteligencia dijo a CNN que Estados Unidos ha estado monitoreando de cerca los informes sobre la salud de Kim (CNN, 2020).

Corea del Sur se pronunció al respecto, a través de su ministro de unificación, Kim Yeon-chul, cuya cartera se encarga de las relaciones intercoreanas, calificando de *fake news* las informaciones que apuntaban que el líder norcoreano sufría graves problemas de salud, y haciendo mención directa a *Daily NK* y CNN. Según afirmó el ministro durante una sesión de la comisión parlamentaria de Exteriores: “esto se puede ver como un fenómeno de infodemia. Tenemos medios de inteligencia que nos permiten decir con confianza que no hay señales inusuales (en el Norte)” (Agencia EFE, 2020).

Gráfico 15

*Tomado de la cuenta oficial de Instagram de CNN, 2020.

El entonces presidente de Estados Unidos, Donald Trump, también expresó su opinión sobre las noticias, a las que tildó de falsas y aprovechó para criticar a CNN por difundir esa información. Trump afirmó en una rueda de prensa en la Casa Blanca: "Tenemos una buena relación con Corea del Norte, tan buena como puede tenerse. Tengo una buena relación con Kim y espero que esté bien" (DW, 2020).

Corea del Norte respondió, a través del sitio web de *Meari*, un medio de propaganda del régimen, el cual tildó de *fake news* las noticias procedentes de Corea del Sur sobre el estado del líder supremo. Las noticias sobre la salud y posible muerte de Kim Jong-un se quedaron sin piso cuando reapareció en público el 1 de mayo de 2020 en una ceremonia de finalización de la construcción de una fábrica de fertilizantes en Pyongyang (Agencia de Noticias Yonhap, 2020).

Conclusión de los casos

Ahora la pregunta que nos hacemos es ¿qué interés tienen estos medios de comunicación en publicar *fake news* sobre Corea del Norte? Y hay dos posibles respuestas no excluyentes entre sí: un interés político; en el caso del *Daily NK* está totalmente clara su posición, al estar conformado por varios desertores del régimen. En similar línea, el *Chosun Ilbo* es conocido por su postura ampliamente crítica hacia el régimen de Kim; pero con una tendencia nacionalista, por lo que suele publicar como cierta cualquier información, no confirmada, que muestre al régimen de una forma brutal, para así dejar en claro la diferencia que hay entre la vida en Corea del Sur y la vida en su vecino del norte.

El otro posible interés que tendrían estos actores no estatales es el económico; hablar sobre la República Popular Democrática de Corea vende en todo el mundo. Para Kretschmer (2019), periodista del medio alemán DW, "Las historias del Estado secreto cautivan a los medios y al público por igual. Pero a menudo las historias son solo una verdad a medias, a veces completamente falsas, especialmente las que provienen de una fuente particular de Corea del Sur", haciendo referencia al *Chosun Ilbo.* También afirma sobre la publicación de la falsa ejecución de Kim Hyok-chol que "no solo fue una primicia mundial sino también publicidad gratuita. Prácticamente todos los medios internacionales citaron el nombre del periódico". (DW, 2019).

Finalmente, el régimen se pronunció, a través de *Meari*, apuntando las *fakes news* originadas en Corea del Sur como un "acto de manipulación de la opinión pública, al inventar, de forma intencionada, hechos falsos sobre un sujeto o grupo específico, con el fin de perseguir ciertos objetivos políticos y económicos". Asimismo, se burlaron de los medios de comunicación conservadores de Seúl, de quienes aseguran, siempre publican noticias falsas como si fueran ciertas, y que "los surcoreanos tienen dificultades para discernir la verdad de los informes falsos" (Agencia de Noticias Yonhap, 2020).

Para Corea del Norte no hay la menor duda de que todas las noticias falsas sobre ellos se originan en medios de Corea del Sur y son posteriormente difundidas en todo el

planeta con ayuda de la Internet. Sin embargo, como pudimos ver, actores con sede en otros países como CNN de Estados Unidos y HKSTV de Hong Kong también han puesto su grano de arena.

Lo anterior nos hace recordar el postulado del escritor y politólogo francés Dominique Moïsi sobre lo que denomina "Geopolítica de las Emociones". Ya que las *fake news* sobre Corea del Norte, probablemente buscan generar "emociones" -como miedo o esperanza- en la audiencia a la que son dirigidas. Para Moïsi (2009), mientras la geopolítica se encarga de elementos racionales y datos objetivos como fronteras, recursos económicos, poder militar y el cálculo político de los intereses; las emociones son esencialmente subjetivas, si no puramente irracionales. Sin embargo, para el escritor francés la mezcla de emociones y geopolítica puede ser un ejercicio fútil y peligroso que puede llevar a la sinrazón, como pasó en Alemania durante la era Hitler.

2.1.2 China y las *fake news*

Al igual que en Corea del Norte, los habitantes de la República Popular China sufren de grandes restricciones al momento de navegar por la Internet. Aunque no al nivel de su vecino; en China encontramos, por ejemplo, que el buscador *Google* y redes sociales como *Facebook*, *YouTube*, *Instagram* o *Twitter* están prohibidos. Mientras las redes sociales locales están vigiladas por el Gobierno, que tiene la potestad de censurar cualquier comportamiento que considere que va en contra de sus intereses (BBC, 2019).

China, en su lucha contra lo que consideran *fake news* sobre el Gobierno, expidió a principios de 2020 una nueva ley que prohíbe a las personas publicar contenido negativo en línea. La administración de Xi Jinping aseguró que la ley está diseñada para "crear un ecosistema en línea positivo" y "preservar la seguridad nacional y el interés público" (Business Insider, 2020). La ley divide el contenido en tres grandes grupos:

- Contenido ilegal: incluye la "difusión de rumores", "alterar el orden económico o social", "subvertir el régimen nacional" y "destruir la unidad nacional".

- Contenido negativo: incluye “titulares sensacionalistas” y cualquier “otro contenido con un impacto negativo en el ecosistema de información en línea”.
- Contenido recomendado: incluye “difundir y explicar la doctrina del Partido”, “difundir los logros económicos y sociales” y “otro contenido positivo y saludable” (Business Insider, 2020).

Palabras más, palabras menos, el mismo Gobierno alienta a las personas del común y a grupos nacionalistas a publicar información favorable a ellos; por lo que las noticias falsas, publicadas por actores no estatales, sobre Estados Unidos, Taiwán o cualquier otro adversario político, podrían ser bien recibidas. En tanto que, cualquier noticia, sea cierta o falsa, que haga ver mal al Partido Comunista de China será censurada y de ser posible, su autor castigado. A fin de cuentas, el Gobierno es el que define a qué categoría pertenece cada contenido.

Caso 1: Elecciones Presidenciales de 2020 en Taiwán

Taiwán, China Taipei, o como se denomina oficialmente: República de China, es autoproclamado como un Estado independiente. Es una isla que se encuentra ubicada justo al frente de la provincia china de Fujian, como se puede observar en el gráfico 5. Sin embargo, la República Popular China considera a Taiwán como parte de su territorio bajo la política de una sola China que ha logrado imponer en la escena internacional. Una muestra de ello es que solamente 15 Estados han reconocido oficialmente a Taiwán como un Estado soberano (El Orden Mundial, 2020).

Taiwán funciona como una república, que elige presidente cada cuatro años con posibilidad de reelección. Las elecciones del 11 enero de 2020 enfrentaban a Tsai-Ing-Wen; quien buscaba ser reelegida y partía como favorita, se presentaba bajo el lema “Resiste a China, defiende a Taiwán”; y Han Kuo-Yu, del Partido Nacionalista Chino, que defendía una relación más cercana a Beijing. En el marco de las campañas electorales, asociaciones de ciudadanos de Taiwán denunciaron la existencia de grupos en China que se aprovechan de la apertura de la isla, considerada una de las sociedades más libres de Asia, para lanzar campañas de desinformación en la Internet. Esta estrategia resultaba

altamente efectiva porque ambos lugares comparten el idioma chino mandarín; y según un estudio de 2019 del Instituto V-Dem, de la Universidad de Gotemburgo, en Suecia, Taiwán es el lugar más expuesto a campañas de desinformación orquestadas desde el extranjero (El Diario, 2019).

Entre las noticias falsas, se publicaban historias como que el doctorado de Tsai era falso o que el activista pro democracia de Hong Kong, Joshua Wong, en su visita a Taiwán de octubre de 2019, le dio una patada a un anciano. Según Jarvis Chiu, responsable del *Institute for Information Industry*, que asiste al Gobierno taiwanés en su lucha contra la desinformación, "China tiene múltiples maneras de fomentar la desinformación. Hemos descubierto que los creadores de contenidos ya no se limitan a generar noticias falsas, sino que cada vez manipulan más la opinión pública". Chiu también afirma que los ejércitos de *trolls* intentan cambiar el foco del debate publicando miles de comentarios cada vez que un candidato sube una publicación o cada vez que se publica una noticia. "Cuentas falsas de redes sociales comparten contenidos favorables a Pekín e inflan el número de *likes* de dichos contenidos" (El Diario, 2019).

Estas campañas de noticias falsas presuntamente provenientes de territorio chino comenzaron poco tiempo después de que Tsai-Ing-Wen ganara las presidenciales de 2016 y se hicieron más frecuentes a medida que se acercaban las nuevas elecciones de 2020. En 2017, la Oficina de Seguridad Nacional de Taiwán reveló que un volumen significativo de desinformación que había circulado en las redes sociales de Taiwán provenía de "granjas de contenido" asociadas al Partido Comunista de China. Muchos de estos rumores y noticias falsas apuntaban a la vida personal de Tsai. Tal vez la *"fake news"* que tuvo más repercusión en la Internet fue una historia que afirmaba falsamente que, cuando le preguntaron a Tsai por qué nunca se casó, ella respondió: "No compraría un cerdo entero solo para poder comer una salchicha" (Advox, Global Voices, 2018).

De todas formas, Tsai resultó reelegida. Lo que desató la furia del Gobierno chino y fue celebrado por la administración del entonces presidente de Estados Unidos, Donald Trump.

Gráfico 16

*Tomado de Gizmodo, 2016.

> El ministro de Exteriores chino, Wang Yi, antiguo responsable de la Oficina de Asuntos Taiwaneses en su Gobierno, ha insistido desde Zimbabue, en una gira por África, en que, pese a los resultados electorales, China no cambiará de actitud hacia la isla, que considera parte inalienable de su territorio y que no renuncia a anexionar por la fuerza. "Este consenso no cambiará ni un ápice por unas elecciones locales en Taiwán, y no se verá alterado por los actos y palabras erróneos de ciertos políticos occidentales", ha subrayado, en una aparente alusión al secretario de Estado de EE UU, Mike Pompeo, que el fin de semana felicitó a Tsai y criticó la "presión sin descanso" de Pekín (El Mundo, 2020).

Así las cosas, los expertos taiwaneses, como Jarvis Chiu, señala a los creadores de contenido chinos como los responsables de estas noticias falsas. Por otro lado, la Oficina de Seguridad Nacional de Taiwán sugiere una incidencia del Estado chino en la difusión de *fake news* en Taiwán. Sin embargo, no es posible establecer con certeza que las noticias falsas hayan sido originadas en China o que su elaboración haya sido ordenada por el Estado chino.

Otros actores que podrían estar interesados en difundir noticias falsas sobre la presidenta Tsai, aparte del Estado chino o de individuos o grupos nacionalistas chinos, serían los taiwaneses pro-China que apoyaban al candidato Han Kuo-Yu. Existe la posibilidad de que todos estos actores tengan algún grado de participación en las campañas de noticias falsas.

Caso 2: China contra la BBC

A comienzos de febrero de 2021, las autoridades chinas pidieron a la cadena de televisión británica BBC que se disculpara y retirara una serie de lo que consideran son noticias falsas sobre el país asiático y la pandemia de Covid-19. En un comunicado, el Ministerio de Relaciones Exteriores chino señaló que dichas informaciones "vinculan la pandemia a la política" y respaldan "teorías de la conspiración" al tiempo que sitúan la responsabilidad del origen del virus en China. Asimismo, ha instado a la cadena a eliminar esas noticias que "tienen un impacto negativo sobre el país" y emitir una "disculpa públicamente" por las *fake news*. El Gobierno chino "llama a una actuación profesional y objetiva que lleve a informar de forma justa sobre el país" (Europa Press, 2021).

Sin embargo, la queja no tuvo impacto en el medio británico, que por esos días emitió un reporte en el que revelaba denuncias sobre violaciones sistemáticas, abuso sexual y trabajo forzoso sufrido por integrantes de la etnia uigur, y otras etnias predominantemente musulmanas -minorías asentadas en territorio chino- en los llamados "campos de reeducación" de la región de Xinjiang (France 24).

El comunicado de la Cancillería china se produjo justo después de que una agencia del Gobierno británico anunciara la retirada de la licencia a la cadena estatal china CGTN por estar vinculada con el Partido Comunista Chino. Según la legislación vigente en el Reino Unido, las licencias deben estar bajo control de las cadenas de televisión y no pueden estar sujetas a gobiernos (Europa Press, 2021).

Finalmente, el 12 de febrero, la Administración Nacional de Radio y Televisión de China prohibió la emisión de la BBC en su territorio, bajo el argumento de que los

informes y noticias presentadas habían violado sus regulaciones (France 24, 2021). China consideró que las noticias sobre el origen del Covid-19 y la violación de derechos humanos a los integrantes de las minorías, que fueron rápidamente difundidas en la Internet, eran noticias falsas que afectaban gravemente la imagen del Estado.

Según el medio *Global Times* (2021), controlado por el Partido Comunista, China envió al mundo exterior una clara señal de que tiene cero tolerancia con las noticias falsas. Aseguran que la BBC está llevando a cabo una campaña de desinformación contra China y que se ha convertido en una herramienta de propaganda para las fuerzas secesionistas y separatistas de China, que amenaza la seguridad nacional. El diario afirma que la BBC se ha degradado a una fábrica de rumores que ve casi todo lo relacionado con China con un doble rasero. El medio expresa lo siguiente:

> Veamos cómo la BBC distorsiona los hechos y fabrica historias sobre China. Retrató la violencia callejera de Hong Kong como un movimiento "a favor de la democracia" y, hasta cierto punto, incluso glorificó a los alborotadores y su violencia. Después de que los partidarios del presidente de los Estados Unidos, Donald Trump, irrumpieran en el Capitolio el 6 de enero, los reporteros de la BBC, incluida Grace Tsoi, que defendió a los alborotadores de Hong Kong, se apresuraron a criticar a los alborotadores estadounidenses, mostrando vívidamente lo que es un doble rasero (Global Times, 2021).

Desde mediados de febrero se han escrito artículos en contra de la BBC casi a diario en los medios estatales chinos. La BBC de cierta forma respondió a la prohibición a través de un documental sobre campañas de desinformación y campañas de noticias falsas provenientes de China, que fue ampliamente repudiado por la embajada china en Londres. Según la BBC, cuando China se enfrentó a una reacción violenta por su manejo de las primeras etapas de la pandemia en el 2020, y algunos funcionarios estadounidenses plantearon la teoría de que el virus podría haber escapado de un laboratorio de Wuhan, el canal CGTN comenzó a impulsar su propia teoría de la conspiración. La estación sugirió, sin aportar pruebas, que el virus se originó en una base militar en Estados Unidos y fue

llevado a China por soldados estadounidenses durante una competencia de atletismo (BBC, 2021).

Asimismo, la BBC también denuncia que, expertos chinos han notado docenas de cuentas de redes sociales oficiales nuevas y muy activas que representan a las embajadas y los principales diplomáticos chinos. El ejemplo más conocido pertenece a Zhao Lijian, funcionario del Ministerio de Relaciones Exteriores de China; quien causó controversia en marzo de 2021, después de tuitear artículos que sugerían que el coronavirus se originó en Estados Unidos; y en diciembre de 2020, había compartido una imagen falsa de un soldado australiano matando a un niño afgano, por la que China se negó a disculparse (BBC, 2021).

La BBC asegura que China posee un "Ejército de teclado", ya que recurre a millones de ciudadanos para monitorear Internet e influir en la opinión pública a gran escala en línea. Afirma que a esos "reclutas" se le conocen como el "ejército de 50 centavos", llamado así debido a los informes de que se les pagaba 0,5 yuanes por puesto para defender y proteger agresivamente la imagen de China en el exterior; y que, al publicar en inglés, los mensajes están dirigidos a una audiencia occidental (BBC, 2021).

La más reciente manifestación de esta "guerra" entre China y la BBC se dio a finales de marzo cuando el corresponsal de la BBC en China, John Sudworth, quien había denunciado amenazas contra su vida por los reportajes publicados por la cadena británica, tuvo que abandonar territorio chino. Según *Global Times* "el Ministerio de Relaciones Exteriores dice que no sabe que Sudworth estaba bajo alguna amenaza, excepto que puede ser demandado por personas en Xinjiang por sus reportajes difamatorios". El periodista partió rumbo a Taiwán (BBC, 2021).

Así las cosas, vemos cómo esta acusación mutua de crear *fake news* involucra a dos actores, uno estatal: China y uno no estatal: BBC, que se mueven por sus respectivos intereses. ¿Quién tendrá la razón?

Conclusión de los casos

Pudimos ver cómo las noticias falsas alrededor de las elecciones en Taiwán, dirigidas principalmente contra la presidenta Tsai, tienen un fin claramente político. Si aceptáramos que China tiene algún grado de participación en esas campañas de *fake news*, es muy claro que tenía interés en que ganara el candidato cercano a ellos. Si consideramos que el Gobierno chino no tuvo participación; y los individuos o grupos nacionalistas chinos y los taiwaneses pro China, fueron quienes crearon las noticias falsas, observamos que también tienen intereses políticos similares a los que tendría la República Popular China.

Si aceptáramos la versión de China sobre la BBC, encontraríamos que el medio británico tiene una línea editorial bien definida crítica del Gobierno chino, por lo que podría tener interés en dañar su imagen y hacerlo ver como un régimen autoritario a nivel internacional. También podría tener un interés económico en vender historias sobre China, que resulten impactantes para el público como el caso de falsas violaciones sexuales. Si aceptamos la versión de la BBC sobre China, podríamos observar cómo el Gobierno usa la Internet como una herramienta para lavar su imagen, a través del llamado "Ejercito de Teclado" principalmente ante occidente, y publica noticias falsas sobre sus enemigos, todo con un interés político.

Una investigación de la BBC en mayo de 2020 encontró cientos de cuentas de redes sociales falsas o secuestradas que promocionan mensajes a favor de China en *Facebook, Twitter* y *YouTube*. Unas 1.200 cuentas estaban dirigidas contra personas que criticaban cómo Beijing estaba manejando la pandemia; aunque no hubo evidencia definitiva que vincule estas cuentas con el gobierno chino. También se conoció que *Twitter* había eliminado más de 23.000 cuentas vinculadas a China, involucradas en una variedad de "actividades manipuladoras y coordinadas" (BBC, 2021).

Sin embargo, es difícil establecer si las noticias falsas que defienden los intereses del Estado chino, son creadas por ese Estado -o con su auspicio- o si sus creadores son actores no estatales que actúan de forma independiente movidos por motivos patriotas.

2.1.3 Rusia y la desinformación

Controlar la creación y propagación de una noticia falsa es casi imposible, por lo que para la mayoría de los Estados se ha vuelto un gran reto mitigar sus daños, tratando de investigar el origen y reaccionar de manera rápida ante la posible propagación de alguna *fake news.* Rusia no es la excepción; en marzo de 2019, el presidente Vladímir Putin firmó una ley contra noticias falsas, la cual prevé multas de hasta US $23.000 (Euronews, 2019).

Sin embargo, lo particular de la ley contra noticias falsas en la Federación Rusa, es que está orientada a castigar a aquellos que generen contenido que atente contra el Estado y hablen mal del Gobierno. Estas leyes, actualmente vigentes, generaron controversias, pues para la mayoría es un acto de represión contra la libertad en Internet. No obstante, para simpatizantes del Kremlin, estas leyes "garantizan la protección contra los llamados terroristas en la web" y permiten "disciplinar a los ciudadanos" promoviendo una mayor responsabilidad (BBC, 2019).

Lo cuestionable de lo anterior, no pasa por los intentos del Gobierno ruso de regular las *fake news,* sino por la falta de cobertura de estas leyes, las cuales no investigan ni castigan a aquellos actores que desde su territorio difunden falso contenido que perjudica a otros Estados, como lo puede ser la injerencia en un proceso electoral o la desinformación sobre una problemática global como la pandemia de Covid-19; casos que trataremos a continuación.

Caso 1: Elecciones Presidenciales en Estados Unidos- 2016

Las elecciones a la presidencia de los Estados Unidos en el año 2016, la cual enfrentaba a la demócrata Hillary Clinton y al Republicano Donald Trump; este último terminaría llegando a la Casa Blanca, estuvo marcada por una polémica campaña de desinformación que afectó en gran parte a la candidata demócrata. La mayoría de críticos apuntan a que esta campaña de desinformación provino de territorio ruso, algo que ya se había vivido en tiempos de la guerra fría, cuando en la década de los 80 bajo la llamada

"*Operation Infektion*" se difundió desde Rusia, la noticia que el virus del VIH/SIDA había sido creado por el gobierno de Estados Unidos para eliminar a su población afroamericana y homosexual (CCN-CERT, 2019).

Durante las elecciones de ese año en Estados Unidos, se difundieron noticias como las que menciona Sarabia (2016); entre ellas, el apoyo del Papa Francisco a Donald Trump o el pago de 400 millones de dólares de Hillary Clinton al Estado Islámico. También, a finales de octubre 2016, una de las noticias más vistas fue la que cuentas anónimas de *Facebook* y medios de comunicación comenzaron a difundir sobre una red de explotación sexual de menores de la que hacía parte la candidata demócrata (CCN-CERT, 2019).

Para Mars (2018), esta campaña de desinformación se realizó desde territorio ruso. Mars, describe que *Facebook* ha reconocido que, hasta 126 millones de sus usuarios, los cuales representan aproximadamente una tercera parte de la población de Estados Unidos, se vieron expuestos a publicaciones de una compañía llamada *Internet Research Agency* durante las elecciones de 2016. Igualmente, se acusa directamente a esta compañía de hackear los correos de los demócratas, como parte de una estrategia para favorecer a Donald Trump. No obstante, no se ha podido comprobar desde donde eran dirigidas las órdenes para la compañía involucrada.

De manera similar, Cembrero (2020), en su artículo *Desinformación "made in Russia": Un desafío para las democracias europeas,* concuerda en que al menos 126 millones de estadounidenses se vieron expuestos a material generado desde San Petersburgo, lugar donde operaba la *Internet Research Agency*. No obstante, la compañía anterior, no actuaba sola, pues hacía parte de un grupo de tres empresas que completaban *Concord Management* y *Concord Catering*.

> Su mecánica era sencilla. Ochenta personas se dedicaban día y noche desde Rusia a sembrar la cizaña. No había muchos disimulos. El operativo, siempre según la versión del FBI, apoyaba al entonces candidato Trump y atacaba a sus rivales Ted Cruz y Marco Rubio. Al mismo tiempo, denigraba a Clinton y ensalzaba a su adversario Bernie Sanders. "La orden era usar cualquier oportunidad para criticar

a la candidata demócrata y a todo el resto, excepto a Trump y Sanders", resume el escrito de la fiscalía (Martínez, 2018, párr. 10).

Así las cosas, aún las investigaciones continúan sobre diferentes compañías rusas involucradas y se trata de determinar la injerencia rusa en las elecciones; no obstante, desde el Kremlin no hubo pronunciamiento ni se brindó cooperación para la investigación que iniciaron las autoridades estadounidenses. Marck Zuckemberg, creador de *Facebook*, admitió ante el Senado de Estados Unidos que millones de usuarios vieron publicidad procedente de Rusia publicada en *Facebook* e *Instagram*. *Twitter* declaró que encontró 2.752 cuentas controladas por rusos y que *bots* rusos tuitearon 1,4 millones de veces durante la elección. (Cortés & Isaza, 2017).

Caso 2: Fake News y la Covid-19

¿Se aprovecha Rusia del miedo al Coronavirus con noticias falsas y teorías de conspiración? Esta pregunta planteada por Roa (2020) sirve para inquietarnos sobre recientes hechos de noticias falsas promovidas desde la Federación Rusa, en el marco de la problemática global actual como lo es la pandemia de Covid-19. Rusia estaría detrás de miles de cuentas en redes sociales que difunden noticias falsas sobre el Coronavirus. Según estas noticias difundidas, se promueven teorías de que Estados Unidos estaría involucrado en la creación del brote del Covid-19. Según el autor, estas noticias difundidas a través de redes sociales, buscaban distraer a la población sobre la respuesta sanitaria mundial que se necesitaba para afrontar la pandemia. No obstante, desde Rusia, María Zajárova, portavoz del Ministerio de Asuntos Exteriores, asegura que esta historia es falsa y que no ha salido desde el Kremlin (Roa, 2020).

Urreiztieta (2020) se refiere a un informe de la empresa de ciberseguridad *Cyrity,* en el cual se señala a Rusia, junto con China, como los principales generadores de *fake news* en el mundo sobre la Covid-19. Sin embargo, estas noticias falsas provenientes de Rusia buscan generar más que solo controversia sobre teorías del origen de la pandemia, también tiene tintes propagandísticos, como si se tratase de un instrumento para promover una buena imagen de Rusia en el mundo frente al manejo del Covid-19.

> Esta operativa abarca "desde teorías no probadas sobre el origen" de la Covid-19, pasando por "falsos consejos sobre la salud o la minimización del impacto en sus estados". Pero también "actividades propagandísticas relativas a resaltar la preparación y gestión de sus gobiernos para enfrentar el brote, la ayuda que están prestando y la consecuente gratitud de algunos gobiernos extranjeros (Urreiztieta, 2020, párr. 2).

Los señalamientos a Rusia, también provienen desde la Unión Europea. Josep Borrell, Alto representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, señaló en junio de 2020, que este país estaba "involucrado en campañas de influencia y desinformación buscando socavar el debate democrático, exacerbar la división y mejorar su propia imagen en el contexto de la Covid-19". Durante los primeros meses de la pandemia, se detectaron alrededor de 550 noticias falsas provenientes de territorio ruso, las cuales estaban dirigidas a los países de la Unión Europea. No obstante, las acciones diplomáticas para evitar que desde Rusia salgan estas noticias, han fracasado. El Kremlin se desentiende de esta actividad pues argumenta que estas noticias se generan desde empresas privadas (Sánchez, 2020).

Los informes de la Unión Europea resaltaban que "la significativa campaña de desinformación" contra Occidente buscaba generar pánico, sembrar la desconfianza y agravar la crisis de salud pública en los países occidentales. Así las cosas, los medios vinculados a Rusia divulgaron información en lenguas oficiales de la UE, como francés, inglés, español, alemán e italiano (El País, 2020).

Por otra parte, las acusaciones a Rusia sobre *fake news* en tiempos de Covid-19, no se limitan solo a desinformación sobre el origen de la pandemia o generar confusión sobre el tema, también con la acelerada carrera de las principales farmacéuticas para crear una vacuna eficaz para inmunizar a la población, se empezaron a realizar señalamientos sobre posible injerencia rusa, desacreditando otras vacunas y priorizando la *Sputnik V*, creada en territorio ruso. Cladera (2020), toma de Josep Borrell, las siguientes palabras:

> Se burlan abiertamente de las investigaciones de vacunas occidentales en medios de comunicación estatales rusos en varios idiomas y en algunos casos ha llevado a afirmaciones absurdas como que estas vacunas podrían convertir a la gente en monos (Cladera, 2020, Párr. 1).

De esta manera, las noticias falsas alrededor de la pandemia y las cuales han tenido origen en territorio ruso y acusadas principalmente, por la Unión Europea, pone otro caso, en el que este país se ve involucrado como origen de *fake news*.

Conclusión de los casos

Con lo expuesto anteriormente se puede evidenciar cómo desde territorio ruso se han generado campañas de desinformación que han afectado a otros Estados, teniendo inclusive injerencia en un proceso democrático de otro país. Ahora bien, en distintas fuentes encontradas se sugería una responsabilidad directa del gobierno en ambos casos. No obstante, en ninguno de los casos se ha comprobado participación directa del Kremlin, por lo que se encuentran otros actores no estatales involucrados. En el primer caso, se señaló a un grupo de empresas que operaban desde San Petersburgo, los cuales contaban con personas dedicadas a la propagación de noticias falsas e incluso con *hackers,* que permitieron interceptar correos del partido demócrata. En el segundo caso, se señalan a agencias de noticias e incluso no se puede determinar si personas del común son quienes estarían detrás de las noticias falsas.

Dicho lo anterior, podríamos relacionar por lo menos 3 actores no estatales detrás de estos casos. Las personas del común, *hackers* y corporaciones. Los 3 tal vez motivados por un sentido de nacionalismo, viendo a occidente como un adversario de su propio Estado; también posiblemente motivados por fines económicos y políticos como podría ser el favorecer a un candidato a la presidencia de Estados Unidos.

No obstante, para autores como Urreiztieta (2020), las *fake news* generadas desde Rusia, hacen parte de “una estrategia militar de desinformación cuyo objetivo es crear división en todos los países en los que pueda tener algún interés”. Claro está, que son

muchos otros los casos donde se asocia a la Federación Rusa de estar involucrado en esta generación de noticias falsas, ocurrió en el Brexit o con los movimientos independentistas en Cataluña; sin embargo, los dos casos expuestos son una referencia de las dudas que siempre quedan sobre estas campañas y los actores involucrados, pues si bien se pueden identificar actores no estatales que participaron directamente, quedará la duda si estos no trabajan para otro actor con objetivos más claros y como parte de una estrategia más amplia.

2.1.4 Irán creador y víctima de las noticias falsas

Las noticias falsas abundan y cada vez son más compartidas, lo que hace que sea más difícil identificar que noticia es real y cual es una *fake news.* De esta ola de campañas de desinformación no escapa la República Islámica de Irán. Según Mackenzie (2019), son cuatro los países desde donde provienen la mayor cantidad de noticias falsas que llegan a la Unión Europea, entre los mencionados, se encuentra Irán.

Igualmente, en el año 2018, la agencia de ciberseguridad *Clearsky* realizó un informe sobre lo que consideran una operación de desinformación global creada desde el país Islámico. En ese informe se detalla, por ejemplo, que la infraestructura desde la cual se crean noticias falsas desde Irán corresponde al menos a 98 medios de comunicación falsos, los cuales cuentan con sus propias páginas web y redes sociales. Esa máquina de *fake news* se centraba en 28 países objetivo, y empezó a operar desde el año 2012. El principal método utilizado era copiar artículos de medios de comunicación legítimos de todo el mundo, en los que se encontraban medios de comunicación de Estados Unidos, Europa, África y Asia. Se identificó también que, en la etapa inicial, muchos de los esfuerzos estaban orientados a divulgar noticias falsas en diferentes países que interesaban a Irán, principalmente en Turquía, Egipto y Afganistán, por considerarlos lugares estratégicos para la revolución islámica (ClearSky Security Ltd, 2018).

Gráfico 17

Región	Propósito
	Propagar desinformación, principalmente, acerca de la actual situación de Estados Unidos y Europa – Presentarlos como fallidos- depravados e indeseables. Nosotros consideramos que los actores iraníes están

Estados Unidos y Europa	tratando manipular los pensamientos de las personas y ponerlos en contra de los gobiernos que no apoyan a Irán o al régimen iraní. Por ejemplo, actualmente los principales métodos utilizados en contra del presidente Trump es promover la colaboración con Irán, independientemente de la secesión de Estados Unidos del acuerdo nuclear, y promover a Jeremy Corbin como el legítimo líder del Reino Unido.
Medio Oriente y Norte de África	Propagar desinformación, principalmente, acerca de problemas de Medio Oriente que son relevantes para Irán y sus aliados. La prensa fraudulenta tiene como objetico los enemigos de Irán (Israel y Arabia Saudita) publican información disuasiva. Nosotros consideramos que esto tiene como objetico presentar a Irán como un poder positivo de balance, mientras se presenta a Israel y Arabia Saudita como poderes que violan la paz y el orden global.
Países musulmanes en África y Asia	Propagar desinformación acerca del papel positivo de Irán en el mundo islámico. Nosotros consideramos que este acto es parte de los esfuerzos iraníes de ser vistos como un líder en el mundo islámico. Nótese que muchos de los objeticos son países con minoría de grupos Chiitas como Nigeria, Pakistán y Afganistán
Aliados de Irán (Como Turquía, Siria y Rusia)	Propagar desinformación, principalmente, en contra de oponentes en común de Irán y sus aliados políticos. Nosotros consideramos que este acto es parte de los esfuerzos de posicionar a Irán como un aliado político valioso

*Traducido de ClearSky Security Ltd, 2018.

La tabla anterior, resume las áreas geográficas de interés de Irán y como a través de campañas de desinformación que salieron desde ese territorio, se buscaba generar contenido que se alineara con sus propósitos. Así las cosas, para Estados Unidos y Europa, se presentaba información que buscara generar resentimientos con sus gobiernos. Para sus rivales en la región como Israel y Arabia Saudita, se publicaba información disuasiva con el fin de elevar a Irán como un poder político positivo en la región y por el contrario mostrar a sus adversarios como países que vulneran el orden global y la paz.

Sin embargo, más allá de una posible coincidencia entre los intereses geopolíticos de la República Islámica, el informe de *Clearsky* no puede determinar si estas acciones de desinformación están orquestadas directamente por el actor Estatal. Para la agencia de ciberseguridad, la infraestructura de generación de noticias falsas desde territorio iraní está coordinado por un grupo organizado que agrupa a varios operadores, como editores, escritores, diseñadores gráficos y especialistas de medios audiovisuales.

Teniendo en cuenta lo anterior, en los siguientes párrafos se detallarán casos de como Irán ha puesto en marcha su infraestructura para crear *fake news,* haciendo uso también de las redes sociales como la plataforma *Facebook,* la cual ha deshabilitado miles de cuentas falsas gestionadas desde territorio iraní. Por otra parte, hablaremos también de la otra cara de la moneda, en la cual la República Islámica ha sido víctima de las noticias falsas.

Caso 1: Redes sociales*: Fake News* "*made* in Iran"

Una de las plataformas a través de las cuales se han viralizado las noticias falsas, son las redes sociales. Con millones de usuarios conectados a plataformas como *Facebook*, *Twitter* o *Instagram*, una noticia sin importar su veracidad puede convertirse viral en pocos minutos e impactar a millones de personas. En el año 2019, se encontró una campaña de desinformación de origen iraní dirigida a influir en los usuarios de internet de todo el mundo; para esta se utilizaban, entre otros recursos, cuentas de redes sociales en 11 idiomas diferentes. La denominada Unión Internacional de Medios Virtuales (IUVM, por sus siglas en inglés) era una red de sitios y cuentas de redes sociales que promovía el contenido de medios de comunicación iraníes, ocultando las verdaderas fuentes de información de las cuales se presume algunas de las noticias estaban dirigidas por chiíes respaldados por *Hezbolá*. Así las cosas, *Facebook* y *Twitter* suspendieron alrededor de 770 cuentas de IUVM, aunque reconocen que alrededor de 100 de estas cuentas estaban ubicadas en los Estados Unidos (Stubbs y Bing, 2019).

Ahora bien, el bloqueo de cuentas de redes sociales con contenido falso que se origina desde Irán, no es un hecho nuevo, ya en el 2018, *Twitter* había suspendido 284 cuentas, argumentando una campaña de manipulación coordinada.

Gráfico 18

*Tomado de AN Noticias (2018)

Según el informe de Clearsky, hay dos tipos de perfiles en redes sociales usados en la campaña de desinformación proveniente de Irán. El primero, son cuentas que se hacen pasar como cuentas oficiales de los medios de comunicación falsos. El segundo tipo de perfiles son cuentas de "personas reales" usualmente mujeres atractivas del país que están usando como objetivo. Desde estos perfiles se divulga a través de historias, artículos con contenido falso. En la siguiente imagen, se observa uno de los ejemplos. Maria López, una mujer de origen francés que desde su cuenta se divulgaban artículos de prensa con *fake news* de Europa.

Gráfico 19

Image 16 – fake social account of "Maria Lopez"

*Tomado de ClearSky Security Ltd, 2018.

Ahora bien, también a través de redes sociales, se descubrió el año pasado, durante las elecciones de 2020 en Estados Unidos, un intento de injerencia con *fake news* dirigidas desde Irán. El Departamento del Tesoro de Estados Unidos sancionó en octubre de 2020 a cinco entidades iraníes, entre las que se señala a los Guardianes de la Revolución, un ejército ideológico de Teherán formado en 1979, cuyo fin era "sembrar discordia entre la población votante al difundir desinformación en línea y ejecutar operaciones de influencia maligna con el objetivo de confundir a los votantes estadounidenses". También se

sancionó al *Bayan Rasaneh Gostar Institute*, una herramienta de propaganda de los Guardianes de la Revolución, así como la Unión iraní de radios y televisoras islámicas y la Unión Internacional de Medios Virtuales, IUVM (DW, 2020).

Caso 2: "Cura" contra el Covid en Irán

En tiempos de pandemia de Covid-19, las noticias falsas se han propagado. Se han difundido diferentes noticias falsas sobre el origen del virus o incluso sobre la eficacia de las vacunas. Sin embargo, una noticia que causó curiosidad y que tuvo una amplia repercusión negativa en Irán fue la de una supuesta cura contra el coronavirus.

Por redes sociales, se difundió la *fake news* que el alcohol mataba al coronavirus. De esta manera, los contrabandistas empezaron a vender alcohol industrial y metanol, lo que causó en el 2020, alrededor de unas 700 muertes por intoxicación y miles de personas resultaron con pérdida de la vista. Y es que "el metanol no puede olerse ni degustarse en bebidas, causa daño cerebral y en órganos. Entre los síntomas se incluyen dolor de pecho, náuseas, hiperventilación, ceguera e incluso coma" (AP News, 2020).

> Según explicó a la agencia iraní IRNA un portavoz de la Universidad de Ciencias Médicas de Ahwaz, Ali Ehsanpour, un bulo difundido a través de las redes sociales, asegurando que el alcohol previene el contagio del coronavirus, ha jugado un rol importante en las muertes locales. Ahvaz es la capital de Juzestán, donde casi medio centenar de personas han muerto por esta razón. Entre los supervivientes se han registrado casos de ceguera y daños hepáticos graves (Hurtado, 2020, párr. 2).

La noticia falsa sobre el uso del alcohol como cura contra el Covid-19, se difundió a través de redes sociales; también se multiplicaron los videos de remedios caseros falsos, como por ejemplo en el que se aseguraba que un médico británico sugería el uso de whisky y miel para combatir el coronavirus. De esta manera, en Irán durante los primeros meses de la pandemia, cuando las cifras de muertos crecían, también tuvieron que

enfrentar la situación de atender la población intoxicada, con un sistema de salud colapsado (El Periódico, 2020).

Dado a esa situación en Irán, la Organización Mundial de la Salud (OMS), debió pronunciarse sobre el tema, desmintiendo la información sobre el uso de alcohol como remedio para el coronavirus. Lo anterior, demuestra el poder de una noticia falsa, la cual se aprovecha de una situación problemática y logra persuadir, debido a la desesperación y falta de conocimiento de las personas.

Conclusión de los casos

Con lo expuesto en Irán y las *Fake News,* se puede observar como el uso de las redes sociales, ha sido un elemento importante para la divulgación de noticias falsas. Se utilizan perfiles con el objetivo de divulgar información según sea el interés, enfocándose en las principales áreas geográficas que necesita atacar la República Islámica, como si se tratase de una acción coordinada de desestabilización política o simplemente de propaganda en favor de Irán.

Desde Irán se ha desarrollado una campaña de desinformación a gran escala, con una infraestructura que ha operado desde el año 2012. Como resultado, se ha logrado influenciar a miles de personas y posiblemente a millones de lectores que no sabían que estaban expuestos a información falsa. (ClearSky Security Ltd, 2018).

Igualmente, se han identificado actores involucrados en las campañas de desinformación, es por eso que se señalan actores como la Unión Internacional de Medios Virtuales, e incluso el gobierno estadounidense sancionó al Bayan Rasaneh Gostar Institute y la Unión iraní de radios y televisoras islámicas. También, se involucra a otro actor no estatal como los Guardianes de la Revolución. Sobre esto, se podría llegar a pensar que el interés de estos actores no estatales es expandir la revolución islámica, divulgando noticias falsas contra gobiernos opuestos a Irán y buscando generar propaganda para su propio país. En una sociedad con grupos tan radicales y con objetivos

trazados en el marco de la revolución islámica, se podría inferir que los intereses de estos actores son de tipo patriota.

2.2 Ciberactivismo

Gracias a la rápida y eficaz comunicación, la capacidad de difusión de información a grandes audiencias, así como la facilidad de coordinación; el ciberactivismo está basado en el uso de las tecnologías de la comunicación y la información. No podemos entender el ciberactivismo sin el desarrollo de la internet y sus diversas aplicaciones, especialmente las redes sociales; las cuales son mucho más que puntos de encuentro, son nuevas vías de expresión que permiten la movilización y dinamización de la opinión pública, por lo que se han convertido en el escenario ideal para defender o promover una causa específica. Para García-Estévez (2018), la libertad de expresión encuentra su mejor aliado en la Internet.

> Los ciudadanos comienzan a estar más informados e involucrados en los procesos sociales y políticos. Encuentran nuevos espacios ciudadanos donde acceder a una gran cantidad y diversidad de información, no ya exclusivamente canalizada por discursos mediáticos, políticos o institucionales. Son, o pretender ser, redes de comunicación alternativas al poder (García-Estévez, 2018).

Las redes sociales ayudan a formar las 4 áreas sobre las que se sustenta el ciberactivismo.

> 1). Organización: las redes sociales son un canal amplio y directo para dar a conocer la información que se necesita circular.
> 2). Construcción de la comunidad: después de trasladar la información se crean espacios de debate que llevan a crear comunidad que les darán seguimiento y nutrirán el tema.
> 3). Recaudación de fondos: aunque es la parte que no siempre se ve, en una parte del proceso se reúnen fondos para que la información llegue de manera más precisa, ya sea por viralización o por medios de publicidad de pago.

4). Acciones de incidencia: cuando la comunidad se forma y cuenta con recursos llega a acciones concretas las cuales fomentan aún más la participación y desembocan en resultados (Democracy Speaks ORG, 2016).

Sin embargo, el origen del activismo digital se encuentra antes de la aparición de la primera red social en 1995, como observábamos en el gráfico 13, las primeras acciones se remontan al año 1989. Sin embargo, adicional a este caso, podemos hacer referencia a otro suceso que tuvo lugar a principios de la década de los noventa. El 10 de abril de 1990 la compañía *Lotus* anunció la comercialización de un programa de bases de datos de correos electrónicos, denominado *Lotus Marketplace*, que contendría el nombre, dirección e información sobre los hábitos de consumo de 120 millones de ciudadanos de Estados Unidos. En respuesta, ciudadanos defensores de la privacidad realizaron una campaña mediante el envío masivo de correos electrónicos y la publicación de información en foros en la red, que incluían datos para ponerse en contacto con *Lotus*, así como plantillas de cartas ya elaboradas y listas para enviar. Más de 30.000 personas se pusieron en contacto con *Lotus* y pidieron que sus nombres fueran retirados de la base de datos. Debido a la presión, el 23 de enero de 1991, *Lotus* anunció que había cancelado el *Marketplace* (García-Estévez, 2018).

Desde entonces, se han presentado diversos momentos de protesta y reivindicación por causas políticas o sociales, en los que internet y los dispositivos tecnológicos han jugado un papel protagónico. Los movimientos antiglobalización en Seattle (1999), las protestas tras los atentados del 11 de marzo en España (2004), las revueltas estudiantiles contra la ley de contrato de primer empleo (*contrat première embauche*) en Francia (2005), las revueltas ocurridas en el Medio Oriente y el Norte de África, que dieron origen a la llamada "Primavera Árabe" (2010-2013), el "*Occupy Wall Street*" contra la desigualdad social en Estados Unidos (2011), son solo algunos ejemplos de movimientos sociales originados en la Internet (García-Estévez, 2018).

Una forma de ciberactivismo muy popular en estos tiempos es el "hacktivismo", realizado por aficionados o profesionales de la seguridad informática con fines

reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general, tal cual como ya lo vimos anteriormente.

Actualmente, también se habla de otra forma de ciberactivismo conocida como "slacktivismo", que no es más que un "activismo de sillón" con un bajo nivel de compromiso de los individuos o grupos en determinada causa y escasa capacidad de transformación en el mundo real. El slacktivismo es un neologismo compuesto de las palabras en inglés: *slacker*, que traduce "holgazán" y *activism* que traduce "activismo" y se utiliza para denominar un tipo de activismo *online* en el que el ciudadano continúa con sus actividades habituales y su implicación se limita a acciones mínimas como dar un "me gusta", publicar algún estado o compartir algún contenido a través de sus redes sociales. Según Morozov (2009), muchos critican esta forma de ciberactivismo al considerar que quien lo practica busca "sentirse bien" haciendo público su apoyo a un tema o causa, pero con poco o nulo impacto político o social; también considera que el slacktivismo no consigue generar efectos importantes en el tejido social y normalmente solo beneficia los egos de los individuos que lo realizan (Morozov, 2009).

Un tema que ha logrado ser más visible ahora antes que en cualquier otra época, gracias al ciberactivismo, es el de los derechos humanos. Muchos defensores de derechos humanos utilizan las redes sociales para denunciar, documentar, escribir o llamar la atención sobre situaciones violatorias de estos que serían ignoradas por los medios de comunicación tradicionales o serían censuradas por las autoridades de determinados gobiernos. La utilización de la Internet sirve para exponer injusticias, difundir información a la que de otra manera sería difícil acceder o estaría bloqueada. En la llamada era de la información, los ciberactivistas han logrado un nuevo espacio en el movimiento de derechos humanos y la tecnología ha permitido que aquellos que antes no eran escuchados tengan una plataforma desde la cual hacer oír sus voces (Frontline Defenders, s.f.).

No obstante, las redes sociales, no en su calidad de plataformas digitales sino en su calidad de corporaciones, también juegan otro papel diferente en el tema del activismo digital. Según afirma Morozov (2017), actualmente resulta obvio que gran parte del

ciberactivismo, especialmente acciones dirigidas a movilizar multitudes con algún objetivo, depende de la "benevolencia" de redes sociales como *Facebook* y *Twitter.*

> El activismo digital nunca se ha visto tan intermediado por estas empresas; sus algoritmos crean o ponen fin a ciertas causas, ayudando a desviar la atención de la audiencia global que controlan. Hay muy poca transparencia en este proceso y poco se puede dar por sentado: algunas causas y campañas pueden tener un éxito fenomenal, mientras que otras pueden fracasar o incluso desaparecer por completo si van contra las reglas, explícitas o implícitas, adoptadas por la plataforma (Morozov, 2017).

Así las cosas, vemos como las redes sociales como corporaciones que son, también tienen sus propios intereses y analizan muy bien qué información les conviene que se haga viral y cuál merece ser olvidada.

En los siguientes párrafos estaremos analizando cómo los actores no estatales usan la Internet para hacer activismo y así alcanzar sus intereses, que en este caso es la defensa de una causa política o social. Tal como vimos en los ejemplos enunciados, la lucha puede ser contra actores estatales como el Gobierno de Francia o actores no estatales como la compañía *Lotus*. Al igual que hicimos con el tema de las "*fake news*", también estudiaremos el fenómeno del ciberactivismo desde su incidencia en cuatro países: Corea del Norte, China, Rusia e Irán.

2.2.1 Desafiando al régimen norcoreano

Al estar la navegación en la Internet totalmente controlada por el Estado, los ciudadanos norcoreanos del común no tienen la posibilidad de hacer campañas de ciberactivismo en pro de sus derechos o en reclamo por la consolidación de una democracia, so pena de los castigos a los que se podrían hacer acreedores. Su voz tampoco podría ser escuchada fuera de las fronteras de Corea del Norte, al tener prohibido el acceso a sitios web extranjeros.

Por las anteriores razones, el fenómeno del ciberactivismo relacionado con Corea del Norte es originado por actores no estatales ubicados fuera de sus fronteras, que luchan por un cambio de sistema político y una mejor calidad de vida para los norcoreanos; generalmente es llevado a cabo por ciudadanos desertores que pudieron escapar del régimen, aunque también grupos hacktivistas, que en principio no tendrían ninguna relación con la República Popular Democrática de Corea.

Caso 1. Operación Corea Libre

En abril de 2013, el grupo hacktivista *Anonymous* anunció que logró tener acceso a información sensible y a cuentas de redes sociales ligadas al régimen de Corea del Norte. La acción fue denominada por el grupo como "Operación Corea Libre"; y se dio como respuesta al discurso de Kim Jong-un, que declaraba el estado de guerra entre las dos Coreas (ABC, 2013).

Según *Anonymous*, sus *hackers* consiguieron forzar el cierre de la página web de noticias *Uriminzokkiri,* pudieron manipular cuentas de *Twitter* y *Flickr* y obtuvieron 15.000 nombres de usuario y sus contraseñas de la base de datos de una universidad norcoreana. Con esta "operación", *Anonymous* hizo un llamamiento al líder del régimen para que abandone su cargo, instaure la democracia en el país y permita el libre acceso a la Internet a todos los ciudadanos (ABC, 2013). Asimismo, el grupo aprovechó para publicar en las cuentas hackeadas imágenes en las que se ridiculizaba al Líder Supremo, como la que se observa en el siguiente gráfico.

Otra web oficial presuntamente atacada por *Anonymous* fue la de reservas en línea de la aerolínea nacional *Air Koryo*. En este caso, la página habría sido vulnerada mediante un ataque de denegación de servicio o ataque DDoS, que consiste en inundar una web con demasiado tráfico (BBC, 2013).

Gráfico 20

*Tomado de New York Magazine, 2013.

Anonymous intentó atacar nuevamente a Corea del Norte en el aniversario de la Guerra de Corea, el 25 de junio de 2013. El grupo apuntaba a infiltrarse en sus sistemas internos y obtener documentos sobre las armas del país y los funcionarios gubernamentales; para conectar la intranet altamente regulada de Corea del Norte a la Internet en general y así permitir que sus ciudadanos finalmente se conecten al mundo exterior. Sin embargo, *Anonymous* -que también esperaba acceder a sitios de armas nucleares- fracasó en su objetivo de vulnerar los sistemas norcoreanos (The Washington Post, 2013).

Según se lee en el *Washington Post* (2013), el ataque autoatribuido por el grupo a la base de datos de una universidad norcoreana es extremadamente improbable, esto debido a que la intranet de Corea del Norte está físicamente separada del resto de la Internet; y la evidencia de *Anonymous* de que una serie de nombres y direcciones de correo electrónico que supuestamente pertenecían a propagandistas norcoreanos, era en realidad una lista de nombres chinos.

Así las cosas, si bien *Anonymous* alcanzó a hackear efectivamente algunas cuentas de redes sociales occidentales manejadas por el régimen; le fue imposible acceder a la

aislada red interna de Corea del Norte, en la que se maneja toda la información sensible. Probablemente sus ataques molestaron de cierta forma al régimen, pero no lograron causar un daño real. Podríamos decir que fue una victoria de la República Popular Democrática de Corea sobre *Anonymous*.

Caso 2: Luchadores por una Corea Libre

"Luchadores por una Corea Libre" (FFNK por sus siglas en inglés) es un grupo de ciberactivistas compuesto principalmente por desertores norcoreanos. Esta organización opera desde Corea del Sur y cuenta con una página web oficial y cuentas en redes sociales, que le sirven para recoger fondos y así sostener su funcionamiento y para denunciar las presuntas violaciones de derechos humanos por parte del régimen. A finales de abril de 2021, FFNK, encabezado por el famoso desertor Park Sang-hak, anunció a través de su página web que había enviado 500.000 panfletos, 500 libretos y 5.000 billetes de 1 dólar a Corea del Norte usando 10 globos. Estos globos, llenos de hidrógeno o helio, normalmente son soltados cerca de la frontera para que el viento los arrastre hacia el norte, donde se espera que revienten y el material sea esparcido. Los panfletos son impresos en polietileno y denuncian los presuntos crímenes de la familia Kim (Swiss Info, 2021).

El grupo no precisó la fecha exacta del envío, pero Park había anunciado que el envío de los globos se daría entre el 25 de abril y el 1 de mayo. Hay varios grupos que operan de forma similar a FFNK radicados en Corea del Sur, pero esta sería la primera vez que uno de ellos decide efectuar esta actividad desde que en marzo entró en vigor una ley que castiga con una multa de hasta 30 millones de wones (aproximadamente 27.000 dólares) o una pena de hasta 3 años de prisión, a quien envíe material a Corea del Norte atacando al régimen de Kim. FFNK expresó que, aunque sus integrantes tengan que pasar en prisión "30 años en vez de 3, seguirán adelante con sus envíos hasta el día de la liberación de los norcoreanos" (Swiss Info, 2021).

La ley fue aprobada por iniciativa del Gobierno del presidente Moon Jae-in después de que Corea del Norte hiciera explotar la oficina de enlace intercoreana en su territorio en aparente protesta por envíos similares a este. Muchos críticos de la norma

consideran que el Gobierno surcoreano ha cedido a las presiones de un régimen autoritario. La administración de Moon argumenta que la ley busca proteger a los residentes en las zonas fronterizas, ya que en el pasado los norcoreanos respondieron con disparos a estas sueltas de globos (Swiss Info, 2021).

La reacción del régimen norcoreano no se haría esperar. Justo al empezar mayo, la subdirectora del Comité Central del Partido de los Trabajadores de Corea Norte, Kim Yo-jong, hermana del líder norcoreano Kim Jong-un -y quien se rumoraba sería su sucesora después de las noticias falsas sobre su enfermedad y muerte- advirtió a Corea del Sur que tomarán represalias en su contra por la difusión de propaganda por parte de desertores norcoreanos; acusó abiertamente a las autoridades surcoreanas de permitir "los actos imprudentes de los desertores del norte" (Excelsior, 2021).

En respuesta a las amenazas hechas por Corea del Norte, las autoridades surcoreanas están investigando el caso para castigar a los responsables. El 6 de mayo, la policía surcoreana registró la sede de FFNK para encontrar evidencias que los pudieran inculpar en el asunto. Mientras tanto las investigaciones continúan (Agencia EFE, 2021).

FFNK es un ejemplo de cómo varias personas con una causa en común se unen para formar una organización que lucha por un interés particular: la libertad de los norcoreanos. La Internet le sirve a su activismo de dos maneras: para que el planeta se entere de lo que consideran atropellos del régimen de Corea del Norte y para recolectar dinero y así llevar a cabos sus acciones en el mundo real.

Conclusión de los casos

En lo expuesto observamos la forma de hacer ciberactivismo de dos actores no estatales diferentes. *Anonymous,* grupo hacktivista, trató luchar por el fin de la dictadura a través de hackeo a cuentas de la Internet manejadas por el régimen y de intentos por acceder a los sistemas controlados por el Estado; en tanto que FFNK, grupo formado principalmente por desertores, utilizó la Internet para denunciar al régimen y como plataforma para conseguir recursos y así ejecutar acciones materiales que, como vimos,

generaron un gran malestar. El punto en común de *Anonymous* y FFNK son sus intereses, ambos son movidos por intereses políticos: acabar con el régimen y devolver la libertad a los norcoreanos.

Por otro lado, los intentos fallidos de hackeo de *Anonymous* son un recordatorio de la notable capacidad de Corea del Norte para aislarse del mundo. Esto no solo incluye a los colectivos de *hackers*, sino también a agencias estatales de inteligencia. Funcionarios de inteligencia de Estados Unidos han admitido que tienen muy poca información sólida sobre su funcionamiento interno y que el régimen posee mejores capacidades tecnológicas de lo que se podría pensar (The Washington Post, 2013).

Ese aislamiento no solo es aplicable al ámbito virtual, sino también al plano físico. Por ejemplo, se supo que la acción de FFKN tuvo consecuencias porque hubo pronunciamiento de parte de Corea del Norte. Sin embargo, resulta casi imposible saber si la propaganda lanzada desde territorio surcoreano llegó a ciudadanos norcoreanos del común y si estos pudieron leer lo que ahí se escribió.

2.2.2 Derechos humanos y democracia en China

El ciberactivismo relacionado con China suele tener una causa común: la lucha por más libertades individuales y colectivas. Los ciberactivistas, tanto los que se encuentran dentro de China continental como los que se encuentran fuera de ella, generalmente tiene el mismo enemigo en común: el Gobierno de la República Popular China, como veremos en los casos que estudiaremos a continuación.

Caso 1: El "Supercarnicero Vulgar"

La Justicia china condenó en diciembre de 2017 a Wu Gan, un conocido activista y bloguero, a ocho años de cárcel tras ser declarado culpable de "subversión al poder del Estado". El ciberactivista, más conocido por su alias de "Supercarnicero Vulgar", denunció varios casos de corrupción y abuso de poder por parte de funcionarios del Partido Comunista chino. "Además de ser un azote en las redes, sus métodos de protesta

poco convencionales lograron que algunas de sus causas trascendieran a la opinión pública china, pese al fuerte control que el Gobierno ejerce sobre los medios de comunicación e Internet". (El País, 2017).

El tribunal consideró, tras un proceso a puerta cerrada, que Wu "llevó a cabo una serie de acciones criminales para subvertir el poder estatal y derrocar el sistema socialista, además de dañar la seguridad del Estado y la estabilidad social". El bloguero recibió una de las condenas más severas sobre activistas políticos de los últimos años. Las organizaciones de derechos humanos estiman que su detención y sentencia están relacionadas con la llamada campaña 709, que se dio en el 2015 y consistió una redada masiva contra decenas de disidentes en todo el país (El País, 2017).

Wu, quien había sido soldado y guardia de seguridad, saltó a la fama con su activismo en internet en 2009 al denunciar el caso de Deng Yujiao, una joven acusada de matar a un funcionario local en la provincia de Hubei, cuando el hombre presuntamente intentó abusar sexualmente de ella. El caso despertó muestras de simpatía hacia la mujer entre la opinión pública china y admiración hacia Wu. El "Supercarnicero vulgar" siguió con su ciberactivismo y denunció el caso de cuatro individuos que habían sido torturados con el fin de que confesaran haber participado en un crimen, a raíz de eso participó en una protesta en mayo de 2015 por la libertad de esas personas en Nanchang, una ciudad al sureste de China; y fue arrestado mientras protestaba, acusado de provocar disturbios. Un año después, los implicados fueron declarados inocentes (France 24, 2017).

En agosto de 2016, el ciberactivista fue detenido nuevamente y denunció haber sido torturado y que su familia estaba siendo amenazada para que él confesara la comisión de varios delitos. Ese mismo año, su padre, Xu Xiaoshun, fue condenado por fraude; presuntamente como castigo a las actividades de su hijo (France 24, 2017).

En ambas oportunidades, Wu estuvo detenido por poco tiempo, pero ya estaba en la mira de las autoridades. En otra ocasión publicó en sus redes sociales una imagen de tres cerdos con las caras de tres altos funcionarios públicos a los que consideraba corruptos, pero lo que más enfureció al Gobierno fue el hecho de que cuestionara la

versión oficial sobre la muerte de un protestante que fue abatido por la policía (El País, 2017). El "Supercarnicero Vulgar" volvió a ser detenido en 2017, ya de forma definitiva, acusado de "difundir información falsa en internet, exagerar casos controvertidos y atacar al régimen", según afirmaron los medios oficiales chinos (DW, 2017).

Sobre la detención de Wu Gan, en el diario El País (2017) se puede leer lo siguiente:

> Patrick Poon, investigador de Amnistía Internacional, asegura que el bloguero "nunca debería haber sido detenido por ejercer su derecho a la libertad de expresión" y señala "lo vergonzoso" de haber hecho pública la sentencia un día después de Navidad, cuando la atención de diplomáticos, periodistas y observadores es menor. "Al tratar de evitar el escrutinio de la prensa y la comunidad internacional, el Gobierno chino revela el hecho de que sabe bien que estos falsos juicios no pueden sostener este escrutinio", dice Poon (El País, 2017, párr. 2).

El caso del ciberactivista, más conocido en el mundo virtual como el "Supercarnicero Vulgar" y quien aún se encuentra detenido, representa solo un ejemplo de los muchos casos de individuos críticos del Partido Comunista Chino, que usan la Internet para alzar su voz contra lo que consideran violaciones de derechos humanos por parte del Gobierno.

Caso 2: "*Occupy Central with Love and Peace*"

"*Occupy Central with Love and Peace*" (OCLP), conocido también como "*Occupy Central*", es un movimiento de desobediencia civil que comenzó en 2014, impulsado por ciberactivistas que luchan por más libertades en Hong Kong. La descripción de su perfil en Twitter señala que "OCLP es un movimiento no violento de acción directa que demanda un Gobierno verdaderamente democrático en Hong Kong". El movimiento propende por una reforma política y unas elecciones democráticas acordes con el cumplimiento de las normas internacionales (García-Estévez, 2015).

La Ley Fundamental de Hong Kong establece que tanto el líder de Hong Kong como su legislatura serán elegidos por sufragio universal. No obstante, el Congreso Nacional del Pueblo de China declaró el 31 de agosto de 2014 que cualquier candidato a liderar Hong Kong tendría que obtener el respaldo mayoritario de un comité electoral compuesto por funcionarios cercanos al Partido Comunista, además de imponer otras condiciones que algunos críticos consideraron "falsa democracia al estilo de China". Este hecho fue el detonante de las protestas de 2014 (Reuters, 2019).

Es preciso recordar que, desde 1997, tras 155 años de ocupación británica, China recuperó la administración de Hong Kong. Desde entonces, se vive una compleja situación en el territorio, por la fórmula "un país, dos sistemas". De acuerdo con este planteamiento, Hong Kong gozaría de ciertos privilegios, como libertad de prensa, derecho a realizar manifestaciones y elección del jefe ejecutivo de la ciudad, cosas que no ocurren en el resto de China. Sin embargo, para los habitantes de Hong Kong, tales privilegios se han quedado cortos para una sociedad que exigen más derechos y más democracia (García-Estévez, 2015).

El movimiento, que comenzó como una réplica del *Occupy Wall Street* que ocupó las calles del distrito financiero neoyorquino en 2011, fue cobrando fuerza y popularidad a medida que sirvió para mostrar el malestar creciente en muchos sectores de la antigua colonia británica hacia el Gobierno chino y su cada vez mayor influencia en un territorio que todavía cuenta con tribunales independientes, libertad de expresión y estatus como centro financiero internacional (Vidal, 2014).

OCLP es un claro ejemplo del papel movilizador de las redes sociales. El movimiento creció específicamente en *Twitter*, que sirvió como medio para impulsar y coordinar las manifestaciones y revueltas callejeras. "Díganle al mundo entero: esta NO es una revolución de color, este es un movimiento de la gente de *#HongKong* para ganar la democracia que les pertenece", dice un tuit de la cuenta de OCLP, publicado el 4 de octubre de 2014. También se observaron otros tuits en apoyo a las movilizaciones como "No necesitamos héroes. Nosotros determinamos nuestro propio destino. *#occupyhk*

#umbrellamovement", publicado en la cuenta de otro influyente grupo, la Federación de Estudiantes de Hong Kong. La explosión de *hashtag* o etiquetas que se convirtieron en tendencias en *Twitter* fue una constante desde el inicio de las protestas (García-Estévez, 2015). Los más populares se pueden ver en el siguiente gráfico.

Gráfico 21

HASHTAG	COMENTARIO
#HKClassBoycott	Con este hashtag comenzó la huelga de las clases de los estudiantes universitarios de Hong Kong el lunes 22 de septiembre.
#OccupyCentral	Tras la perseverancia que mostraron los jóvenes de Hong Kong, el movimiento OCPL adelanta la fecha en que tenía prevista lanzar su campaña de protesta.
#UmbrellaRevolution	El domingo, 28 de septiembre el mundo es testigo de unas imágenes las que los oficiales de policía estaban disparando gases lacrimógenos contra la multitud de manifestantes desarmados, cuyo único escudo son los paraguas. El hashtag #UmbrellaRevolution fue un tema de debate entre los usuarios de medios sociales, muchos de los cuales preferían el de #UmbrellaMovement, pues entendían que revolución implicaba cierta violencia la cual no se había dado en las manifestaciones hongkonesas.
#OccupyHK	Las manifestaciones desbordan la mera ocupación del centro de negocios de Hong Kong, convirtiéndose en una fenómeno global. Esto llevó a muchos manifestantes a concluir que #OccupyCentral ya no reflejaba la verdadera magnitud del movimiento y, por lo tanto, el hashtag #OccupyHK se convirtió en su mantra.

*Tomado de García-Estévez (2015)

A las manifestaciones que se originaron con el movimiento OCLP se les conoció como la Revolución de los Paraguas, después de que los manifestantes usaran los paraguas para defenderse del gas pimienta, los gases lacrimógenos y ataques de la policía. Sin embargo, las protestas terminaron en diciembre de 2014, con el desalojo a la fuerza de los manifestantes por parte de la policía. Por otro lado, las autoridades centrales chinas no otorgaron concesiones democráticas (Reuters, 2019).

El movimiento OCLP constituye un ejemplo de cómo un grupo de personas con una causa en común crean o impulsan iniciativas en la Internet y con las constantes interacciones en las redes sociales van ganando adeptos a su movimiento o logrando que grupos con causas similares se adhieran a la suya, para después llevar a cabo acciones en el mundo real.

Conclusión de los casos

La situación de Wu Gan, quien tenía como interés la lucha por el respeto de los derechos humanos en su país, es la misma de muchos disidentes del Gobierno chino que son detenidos y se ven enfrentados a juicios con dudosas garantías procesales o son presuntamente obligados a declararse culpables. El constante monitoreo que hace el Gobierno a la Internet hace más fácil la labor de identificar a sus "enemigos". Según afirma la escritora y periodista china, Karoline Kan, en una entrevista dada a la BBC: "Pueden venir funcionarios del gobierno y tocarte la puerta de casa para averiguar los motivos por los que publicas en la web tantas palabras delicadas" (BBC,2019).

Por otro lado, el caso de OCLP, cuyo interés era el establecimiento de una democracia real en Hong Kong, nos demuestra el poder de convocatoria que tienen las redes sociales, pero al igual que el caso del "Supercarnicero Vulgar", nos deja en claro el enorme poder de China como actor estatal. La policía de Hong Kong, que actuaba bajo las órdenes de Beijing, logró repeler las protestas y minimizar el movimiento; y China no cedió a ninguna de las pretensiones de los manifestantes. Al final, en ambos casos, como en muchos otros, China logró imponerse sobre los actores no estatales, que parecían minúsculos a su lado.

2.2.3 Lucha social y política en Rusia

Las protestas sociales manifestadas a través de movilizaciones que buscan resaltar la inconformidad del pueblo ante una situación particular, es una forma tradicional de expresar a los gobernantes que algo anda mal. Sin embargo, Rusia es un país donde cada vez se buscan más mecanismos para regular las protestas. Desde el año 2012 existe una ley que restringe la libertad de reunión, estableciendo multas de hasta 23.800 euros o hasta 200 horas de trabajo comunitario (DW, 2012).

De esta manera, el ciberactivismo se convierte en una forma pacífica, pero a la vez eficaz de manifestar alguna protesta. Así, haciendo uso de las plataformas digitales, como redes sociales y páginas web las personas protestan ante sus gobiernos o expresan

su posición frente a algún tema. En el caso de Rusia, veremos cómo estas acciones de ciberactivismo han ganado terreno. Desde acciones globales lideradas por organizaciones como Avaaz, hasta acciones más recientes como la exigencia de liberar al líder opositor Alekséi Navalny, son algunos de los casos en que las personas en Rusia pasaron de protestar en las calles a hacerlo en la Internet.

Caso 1: Avaaz.org y los casos rusos

Avaaz, "la comunidad activista que acerca el poder y la voz de la gente a los centros políticos de decisión a nivel mundial". "Avaaz es una comunidad global de movilización *online* que integra acción política impulsada por la ciudadanía dentro de los procesos de toma de decisiones globales". Estas son algunas de las frases que podemos encontrar en la página *Avaaz.org;* de esta manera se presentan y manifiestan tener alrededor de 68 millones de miembros en 194 países. Avaaz, que significa voz en varios idiomas europeos, asiáticos y de medio oriente fue fundada en 2007, con lo que manifiestan, una misión simple y democrática "movilizar a los ciudadanos del mundo para cerrar la brecha entre el mundo que tenemos y el mundo que la mayoría de la gente quiere" (Avaaz.org, 2021).

Para Paz (2018), quien escribe una crítica sobre Avaaz, la presenta como una organización "aparentemente" caritativa y que aprovecha las nuevas tecnologías para realizar sus campañas a través de redes sociales. Recoge fondos a través de iniciativas como el respeto por el medio ambiente, la lucha contra la pobreza, la protección de los derechos humanos, entre otros. Para Paz estas "Son causas bien asimilables y compartidas por la mayoría de la población, entre las personas con una visión altruista, que creen que un mundo mejor es posible y que están dispuestas a donar parte de su dinero para su consecución". No obstante, para el autor, las luchas que decide emprender esta ONG son "selectivas" pues asegura, que entre sus proyectos nunca se verán iniciativas para boicotear eventos en territorio estadounidense o acciones contra este país.

Sin embargo, más allá de la polémica sobre esta organización, lo que es claro es que *Avaaz.org* dedica gran parte de su actividad al ciberactivismo. Dentro de sus acciones

se destacan la firma de peticiones o*nline* o el envío de correos de protesta de manera masiva. Por esto en los siguientes párrafos veremos algunos casos de ciberactivismo en las que esta organización se ha manifestado frente a la Federación Rusa.

En 2012, mediante el título "Combatan la trata sexual", la ONG creó una página que buscaba recolectar firmas para pedirle a Vladímir Putin que protegieran las mujeres y niñas rusas de la trata de personas. Para esto, se solicitaba a Rusia que firmara la Convención Europea contra el Tráfico de Personas. Igualmente, en el mismo año y ante el asesinato de manifestantes pro democracia en Siria, se solicitaba a Turquía, Alemania y a la Liga Árabe para que ejercieran presión internacional sobre Rusia con el objetivo de que dejara de suministrar armamento al gobierno de Bashar al-Ásad. Esta petición, aunque no logró llegar a su objetivo, fue firmada por 353.724 de los miembros de la ONG.

Gráfico 22

*Tomado de Avaaz.org

Igualmente, dentro de las victorias de Avaaz, se encuentra la petición de 1,3 millones de usuarios que solicitaba al presidente Vladimir Putin de firmar un acuerdo, ya que Rusia era el único país que faltaba por firmar, de un tratado de 24 países, que buscaba proteger el mar de Ross. Esta zona de la Antártida se convirtió en el año 2016 en la reserva marina más grande del mundo. Así las cosas, lograron, junto con otros ambientalistas que se liberara de pesca a esta zona durante 35 años (BBC, 2016).

Caso 2: *#LoveIsStrongerThanFear*

Alekséi Navalny, un abogado y político opositor ruso y catalogado como "el crítico más ferviente de Vladímir Putin en Rusia", es el centro de la campaña ciber activista *#loveisstrongerthanfear.* El opositor ruso reúne millones de seguidores en redes sociales y es conocido por criticar abiertamente al gobierno de Putin. Navalny asegura que el partido de Gobierno, Rusia Unida, está lleno de criminales y ha denunciado diferentes acciones de corrupción del Kremlin. En el año 2018, intentó desafiar a Vladimir Putin en las elecciones presidenciales, pero su candidatura fue vetada. En agosto del 2020, este líder opositor fue envenenado; "el gobierno alemán reveló que las pruebas realizadas mostraban "signos inequívocos" de envenenamiento por agente nervioso *Novichok".* El 17 de enero de 2021 regresó a Rusia y fue encarcelado por violación de las condiciones de una condena previa. Actualmente está condenado a más de dos años de prisión (BBC, 2021).

Desde su encarcelamiento, diferentes acciones de protestas llevadas por simpatizantes del líder opositor se han desarrollado en Rusia. Los manifestantes convocaron multitudinarias marchas para exigir la liberación de Navalny; no obstante, muchas de estas manifestaciones fueron reprimidas y terminaron con miles de detenidos como ocurrió en la realizada el 31 de enero de 2021 en Moscú (France24, 2021).

Dado lo anterior, los manifestantes y simpatizantes de Navalny, tuvieron que recurrir a otra forma de protesta para evitar ser arrestados. Con el *hashtag: #LoveIsStrongerThanFear* los organizadores realizaron una campaña la cual describieron que era una respuesta a la ola de violencia y represión sin precedentes que iniciaron las fuerzas de seguridad en contra de las protestas. Así las cosas, esta forma de manifestación pacífica y descentralizada, es una forma que los simpatizantes de Navalny en Rusia han empezado a utilizar para evitar la represión policial y seguir luchando por la libertad del líder opositor (DW, 2021).

> "Putin es el miedo. Navalny es el amor. Por eso ganaremos", escribió en *Twitter* Leonid Volkov, uno de los estrechos aliados de Navalny, al llamar a la gente a

> reunirse. Instó a la gente a inundar las redes sociales con fotos de las reuniones del domingo -una nueva aventura para la oposición que se asemeja a las acciones políticas en la vecina Bielorrusia- utilizando el hashtag #loveisstrongerthanfear en ruso (Tétrault-Farber y Soldatkin, 2021).

La campaña *#LoveIsStrongerThanFear,* también ha servido como plataforma para solidarizarse con las mujeres que sufren persecución policial en Rusia. Más de 100 mujeres han sufrido de persecución policial en las protestas de enero, por lo tanto, con esta forma de manifestarse, expresan que es una manera pacífica de mostrar lo que está pasando. "es más efectiva que la agresión y la violencia, permite el dialogo con la sociedad" (DW, 2021).

El *hashtag #LoveIsStrongerThanFear,* llegó rápidamente el 14 de febrero de 2021, a 20.000 publicaciones en *Twitter.* En *Instagram* el número de publicaciones fue de 8.000 ese día. Con esta campaña, liderada principalmente por los jóvenes, quienes apoyan en gran medida a Navalny, se manifiesta el descontento de la población joven con la administración de Putin, pero también se refleja como los jóvenes utilizan este medio para manifestarse ante una causa política. Igualmente, las redes sociales, *Youtube* y las publicaciones en línea son vistas por los jóvenes en Rusia como un medio de información alternativo ya que los medios de información tradicionales están influenciados por el Gobierno y tienen como objetivo la población mayor y la población rural (Dupré, 2021).

Conclusión de los casos

Por lo visto anteriormente, se evidencia cómo los ciberactivistas han empezado a presionar al gobierno ruso sobre diferentes temas de interés. Por un lado, acciones de interés global como puede ser la conservación de un mar en la Antártida o solicitar a otros gobiernos para que ejerzan presión diplomática para que cese el suministro de armas por parte de Rusia a una zona de conflicto. Por otro lado, acciones más particulares como la trata de mujeres en Rusia o las protestas en favor de la liberación de un opositor al gobierno.

Las redes sociales y los avances tecnológicos permiten que las personas puedan tener otras maneras de manifestar su inconformidad. En el caso de Avaaz, por ejemplo, se encuentra como una ONG puede hacer que las personas se unan a una causa, a través de envío de correos, creación de páginas web y peticiones en línea. En el caso de las protestas en favor del opositor Navalny, es un ejemplo de cómo las personas pueden organizarse a través de las redes sociales para manifestar su inconformidad contra el gobierno. Haciendo tendencia un *hashtag*, en redes tan populares como *Twitter* o *Instagram*, logrando no solo encontrar una manera pacífica de manifestarse y evitar la represión, sino también de ser más visibles ante el mundo.

Así las cosas, los actores no estatales, como una ONG, un grupo político o una persona del común, pueden a través del ciberactivismo mostrar sus intereses de orden político o social como el caso de Navalny, Siria y la trata de mujeres, o de orden ambiental como el caso del mar de Ross.

2.2.4 Más libertades en Irán

Al pasar los años, las redes sociales y la Internet, se vuelven más importantes para todos. Es así, que se han empezado a desarrollar diferentes debates sobre el papel de las redes en las manifestaciones sociales. Para algunos expertos, como asegura Carlini (2018), las redes sociales como *Twitter* y *Facebook* desempeñaron una función vital en diferentes eventos de protestas; en Irán, no es la excepción, tal y como veremos a continuación, en la Revolución *Twitter* de 2009 las redes sociales fueron la plataforma para plasmar la inconformidad de la población.

No obstante, hoy en día, Irán es un país altamente restrictivo con el uso de la Internet. Durante época de elecciones o diferentes conflictos, el Gobierno ha regulado la conexión con el fin de hacer más difícil la comunicación y evitar acciones de organización que puedan desencadenar en protestas sociales. “No es ninguna sorpresa que las únicas VPN legales, las cuales informan a las autoridades, son las que cuentan con la aprobación del gobierno” (National Geographic, 2019).

En los siguientes casos, abordaremos en primer lugar, la revolución *Twitter* y, en segundo lugar, la lucha de las mujeres en la República Islámica para reivindicar sus derechos; para ellas el ciberactivismo ha sido un medio fundamental en su proceso de protesta contra la rigidez del régimen.

Caso 1: La Revolución *Twitter*

Transcurría el año 2009 y en la República Islámica se presentaron elecciones Presidenciales. Por un lado, se encontraban los conservadores y radicales que apoyaban al presidente Mahmud Ahmadineyad, por otro lado, se encontraba el partido reformista que había tenido la presidencia desde 1997 hasta el 2005. Así las cosas, para los reformistas era la oportunidad de volver al poder y para ello tenían dos candidatos, el exprimer ministro Mir-Hussein Mousavi y el exportavoz del Parlamento Mehdi Karroubi. Al final del día de las elecciones, Mousavi se perfilaba como ganador, pero al día siguiente los resultados fueron diferentes. De esta manera, en la mañana del 13 de julio empezaron las protestas, las cuales se extendieron por 9 meses. Estas protestas se iniciaron principalmente por el papel de las redes sociales, por eso para muchos se le conoce como la Revolución *Twitter* (Gómez, 2019).

> En esta ocasión miles de jóvenes, que contaban con móviles de última generación, invadieron las calles de Teherán para protestar en contra de la que consideraban haber sido una elección ilegítima. La sociedad iraní se estaba enfrentando a la crisis política más difícil después de la de 1979 cuando cayó el régimen del Sha Reza Pahlavi. (Carlini, 2018, pág. 5).

Para Betancour (2017), las protestas no se hubieran podido llevar sin la ayuda de las redes sociales. A través de *Twitter,* se exacerbó el descontento de miles de iraníes, en su mayoría, población joven, que salió a protestar a las calles. Para el mismo autor, existen pruebas de que en la revuelta participaron también hacktivistas que realizaron ataques DDoS contra los proveedores de servicios web de Irán. Este ataque consistió en saturar el ancho de banda del servicio de internet para que este fuera denegado a sus usuarios habituales.

Así las cosas, *Twitter* sirvió como plataforma para incentivar las protestas, pero también, para informar al mundo lo que ocurría en territorio iraní, en unas elecciones que para muchos fueron amañadas. No obstante, esta revolución *Twitter* no funcionó para más allá de movilizar las masas, pues los resultados de las elecciones no cambiaron y, por el contrario, se reprimió el uso de la Internet a partir de este suceso. Como expresa Carlini (2018) "para las autoridades iranís Internet no era nada más que una herramienta en manos de las potencias enemigas cuyo interés era la desestabilización del país". La Internet en Irán pasó de ser una herramienta para el crecimiento económico a ser una amenaza para el régimen, es por eso que, tras las protestas, el gobierno formó un equipo de expertos para contrarrestar el cibercrimen y detectar cualquier información que pudiese atacarlos.

Caso 2: La lucha de las mujeres ciberactivistas

"La vida de una mujer vale la mitad que la de un hombre". Estas palabras, mencionadas por Shirin Ebadi, la primera mujer iraní en recibir el Premio Nobel de la Paz en 2003, es el reflejo de lo que viven las mujeres en la República Islámica. No obstante, estas palabras que parecen ser una analogía a como son tratadas las mujeres en Irán, era una regla establecida en la Sharia, el código de derecho islámico que regula las leyes, la moral y la conducta de los ciudadanos (Membrado, 2016).

Así las cosas, en Irán la Internet ha surgido como un medio para romper las estructuras patriarcales en las que se basa el pueblo iraní. La Internet se ha convertido en un instrumento utilizado por las mujeres para generar una consciencia feminista que pretende hacer cambiar la percepción sobre la sociedad y el papel de la mujer en las nuevas generaciones. Esto a partir de mayores espacios para expresarse, aunque como afirman las autoras, así estos se encuentren en el universo virtual (Medina y Sepeda, 2019).

De esta manera, estos espacios ganados en la red, se representan en *blogs*. Como expresa Velasco de Castro (2012), no es casual que Irán sea el segundo país del mundo

con mayor cantidad de *blogs*, los cuales en su gran mayoría están escritos por mujeres "para quienes la posibilidad de poder expresarse libremente a través de la Red, ha permitido que muestren al mundo la infatigable lucha que continúan llevando a cabo por la consecución de sus reivindicaciones".

> Actualmente se editan en Farsi (Persa) alrededor de 700.000 *blogs* y de ellos la mitad son gestionados y escritos por mujeres. Bloguistán es el nuevo refugio de los activistas pro Derechos Humanos. Así llaman en Farsi los internautas a este espacio para la protesta que escapa con más facilidad a las redadas policiales (Sisco, 2018).

Gráfico 23

LA REPÚBLICA ISLÁMICA Y LAS MUJERES / *La oposición a Ahmadineyad*

Las políticas de Mahmud Ahmadineyad están suscitando una ola de oposición interna que hace que el régimen se tambalee. Sus expresiones más visibles son las protestas por la campaña para que las mujeres cumplan rigurosamente con el código de vestimenta islámico. Pero el movimiento feminista se ha hecho fuerte en internet, un medio que utiliza para eludir la férrea censura. Entre bastidores, la política iraní vive una época convulsa. Una gran coalición antigubernamental intenta generar una segunda revolución por la vía de las urnas para impedir que el ultraconservador dirigente acceda a un segundo mandato. Los progresistas leales a Jatami y los conservadores pragmáticos que siguen a Rafsanyani se preparan para derribar el régimen.

'Bloguistán', el último reducto de las iraníes

El movimiento feminista en Irán atemoriza al Gobierno de Mahmud Ahmadineyad desde internet, el campo de lucha de 'ciberactivistas' que reivindican la igualdad de derechos con el hombre y protestan contra la rigidez del régimen

ROSA MENESES

La moda y la tecnología se han convertido en los dos látigos del régimen de los ayatolás. Y es que desde que el actual presidente, el ultraconservador Mahmud Ahmadineyad, llegó al poder en 2005, vestir a lo occidental, llevar un corte de pelo a la última o defender en un *blog* de internet que se deje de discriminar a las mujeres son valientes actos de resistencia política contra el paternalismo y el involucionismo del actual Gobierno. Los iraníes ven las decisiones del Ejecutivo como un paso atrás en los avances sociales y políticos conseguidos durante la época de Mohamad Jatami. Ahora, imperan el rigor, la moral puritana y los formalismos.

La *blogsfera* se ha convertido en un manifiesto virtual en contra de las injusticias del régimen y son sobre todo las mujeres las que se valen de la tecnología para eludir la censura. Actualmente se editan en farsi alrededor de 700.000 blogs y de ellos la mitad son gestionados y escritos por mujeres. Bloguistán es el nuevo refugio de los activistas pro Derechos Humanos. Así llaman en farsi los internautas a este espacio para la protesta que escapa con más facilidad a las redadas policiales.

Aunque sólo aparentemente. El resquicio de libertad de bloguistán se ve frecuentemente acosado por las autoridades iraníes y las detenciones

Tres mujeres iraníes cubiertas con el tradicional 'chador' se toman un descanso en la plaza Nagsh-e Jahan mientras visitan la ciudad de Isfahan. / MORTEZA NIKOUBAZL / REUTERS

nal» por enarbolar eslóganes como: «Los derechos de las mujeres son los derechos del hombre». Se enfrentan teniendo un régimen tan rígido», manifiesta RSF. Cuando un sitio se cierra o se bloquea, sus creadores edad a los 9 años; los hombres lo son a los 15) y en cuestiones de derecho familiar, las margina.

iraníes, es un medio de decir: 'Resistimos y continuaremos movilizándonos, sin importar a qué precio', pese a las detenciones, ante a las presio-

*Tomado de *20 Minutos* (2007)

Así las cosas, Bloguistán es un espacio donde se congregaban no solo mujeres sino también diferentes actores que buscaban manifestar su inconformidad con la rigidez del régimen. Esta era vista como una herramienta para evitar represiones.

No obstante, a pesar de intentar escapar de las represiones, el ciberespacio tampoco es seguro para las feministas en Irán. Como se describe en el libro *Así pasó en Irán* del año 2018, 4 ciberfeministas fueron enviadas a la cárcel por sus publicaciones en la web que reclamaban una mejor condición para la mujer en la República Islámica. Algunas de sus publicaciones se realizaban bajo el slogan "los derechos de las mujeres son los derechos del hombre" por esto se les acusó de atentar contra la seguridad nacional.

De esta manera, como establecen Medina y Sepeda (2019), la resistencia en la Internet le ha permitido a la mujer iraní manifestarse frente a sus derechos, buscando la igualdad en una sociedad con una gran inequidad de género. Al mismo tiempo, estas acciones de ciberactivismo, les han permitido a los movimientos feministas en Irán tener apoyo transfronterizo y "posicionar no solo a la mujer iraní sino a la musulmana en un proceso de reconstrucción acorde con sus necesidades".

Conclusión de los casos

El ciberactivismo en Irán ha generado movimientos como la revolución *Twitter* que permitió a la población de Irán inconforme por las elecciones, coordinarse para revelarse frente al gobierno que para ellos manipuló los resultados. Igualmente, ha permitido que grupos amenazados por las leyes iraníes, como las mujeres, puedan expresar su voz de protesta. Así las cosas, los actores no estatales en Irán, vieron en el ciberactivismo la manera de defender sus intereses, de tipo político y social, como los que se relacionan en ambos casos.

Sin embargo, se hace evidente también el poder del actor estatal, el cual reprime las acciones ciberactivistas mediante el control de la Internet. En este caso se demuestra, que otros actores no estatales como las personas del común o hacktivistas luchan contra un adversario de mayores recursos, capaz de emitir leyes que minimizan sus posibilidades o simplemente, como sucedió en el año 2019, dejar a un país completo, de casi 80 millones de personas, sin acceso a la red (BBC, 2019).

Cierre del segundo capítulo

La Internet ha cambiado las maneras en que diferentes actores no estatales pueden manifestar sus intereses. Al mismo tiempo, ha modificado las formas de participación política permitiendo a través de una publicación, una imagen o una opinión en un *blog* difundir discursos y acciones. También ha permitido que estos puedan comunicarse e informarse más allá de los medios tradicionales de comunicación. Así las cosas, el uso efectivo de las tecnologías de la información ha dado la posibilidad a los actores no estatales de plantear su posición política y/o social sobre un tema particular, como se evidenciaba en los casos señalados (Perales, 2008).

Así las cosas, al analizar los casos expuestos de noticias falsas y ciberactivismo relacionados con Corea del Norte, China, Rusia e Irán, observamos cómo los actores no estatales persiguen sus propios intereses, que muchas veces están alineados con los de un actor estatal, como el de los grupos de taiwaneses pro-China con los intereses del Estado chino o el de los hackers patriotas rusos con el Kremlin.

Asimismo, pudimos ver otros casos en los que los intereses del actor no estatal van abiertamente en contra de los intereses del actor estatal. Como el caso de FFNK, el grupo compuesto principalmente por desertores del régimen norcoreano que lucha por el fin de la dictadura y la República Democrática Popular de Corea; o el grupo de mujeres ciberactivistas que luchan por la reivindicación de sus derechos ante el Estado iraní.

Los actores no estatales mencionados en los casos analizados van desde individuos, ONG, corporaciones -como son los medios de comunicación-, *hackers,* hasta grupos de personas con un objetivo en común. Todos usaron la Internet como un medio para conseguir o al menos tratar de alcanzar sus intereses. Ahora, para tratar de resolver el interrogante del título del segundo capítulo *Actores no estatales en el ciberespacio ¿Cuáles son sus intereses?*; podemos decir que, de acuerdo con los casos estudiados, son intereses políticos, sociales y/o económicos. Lo anterior coincide con la afirmación de Sigholm (2016), quien analiza los intereses de diferentes actores no estatales y determina

que los intereses políticos, sociales y económicos son los más recurrentes entre este tipo de actor.

En el caso, por ejemplo, de un ciberactivista, es alguien que utiliza la Internet como herramienta para difundir un discurso y buscar acciones que les de poder y visibilidad frente a una causa específica, las cuales pueden ser de orden social o político. "Como se puede denotar, en su aproximación a lo que se concibe como ciberactivista se pone mayor énfasis en la posibilidad de constituirse en un agente de cambio social". No obstante, a través de la Internet, un actor no estatal puede buscar ir más allá de un interés social, también puede realizar acciones que impliquen una estrategia con fines políticos y electorales (Burgos, 2020).

De esta manera, los casos estudiados nos dan a entender que los actores no estatales señalados en cada uno de ellos buscaban generar consecuencias en el mundo fáctico. Esto se evidencia tanto en los casos de noticias falsas como en los de ciberactivismo, pues buscaban influir en la opinión y las emociones del público. Citando nuevamente a Moïsi (2009) "no es posible entender el mundo en el que vivimos sin integrar y comprender sus emociones". En ese sentido, "las emociones son como el colesterol, es decir, buenas y malas. El problema es hallar el balance correcto entre ellas". Con esas "emociones" los grupos ciberactivistas pueden ganar adeptos a su causa o un político víctima de una noticia falsa puede ganarse el repudio de los votantes.

Conclusiones

Después de revisar algunos casos que constituyen una pequeña muestra del actuar de los actores tanto estatales y no estatales en el ciberespacio, pero que nos permite hacernos una idea de la realidad que estamos viviendo con el constante desarrollo de la Internet, podemos concluir que:

Primero, los actores estatales cuentan con intereses más claros de orden político y económico. Sin embargo, lo difícil es atribuir un ciberataque o alguna acción en el ciberespacio a un Estado. En los casos de los 4 países revisados, se presume que ya sea directa o indirectamente, cada uno de estos pudo encontrar en la Internet una herramienta para alcanzar un interés ya sea como parte de una aparente estrategia a largo plazo o de una situación circunstancial. Por ejemplo. En el caso de Corea del Norte, la consecución de réditos económicos para la supervivencia del régimen o en el caso de China la posibilidad de posicionarse como una potencia económica y política mundial en seguimiento de una estrategia global del gigante asiático.

Aunado a lo anterior, en los casos de Rusia, se evidencia como este actor estatal pudo alcanzar sus intereses geopolíticos con respecto a dos conflictos en el año 2007 y 2008, como fueron los que sostuvo en Estonia y Georgia respectivamente. De manera similar, en el caso de la República Islámica de Irán, se observa cómo pudo beneficiarse de ataques que salieron desde su territorio y que afectaron a uno de sus adversarios en Oriente Medio como Israel.

En segundo lugar, en el caso de los actores no estatales, al ser más diversos sus intereses también son más amplios. No obstante, lo revisado permite determinar que estos se pueden agrupar en tres principalmente: políticos, sociales y económicos. Las acciones realizadas en la Internet por este tipo de actores también son heterogéneas. Desde acciones aparentemente más sencillas como replicar una noticia hasta acciones con un grado de especialización tal como el hackeo de una página web gubernamental o financiera. Lo que es claro, es que una persona del común, una corporación, una ONG o

un grupo de individuos que comparten un objetivo en común; se benefician de la Internet como una herramienta para alcanzar el interés que persigue.

En tercer lugar, la Internet es una herramienta amplia y accesible a casi todos, donde tanto actores estatales como no estatales conviven. Al mismo tiempo es un espacio con poca regulación a la expresión, donde muchos pueden ocultarse sin ser fácilmente identificados. Estos elementos hacen de la red una herramienta con pocos límites a la expresión social, donde se puede manifestar la posición de alguna persona o grupo ante una situación específica. Pero al mismo tiempo, una herramienta de información manipulable por cualquiera de nosotros, que puede generar, por ejemplo, a través de una noticia falsa el descontento infundado hacia alguien en particular. Igualmente, y según la información de Swiss info (2019) en la que se menciona el provecho económico en criptomonedas de Corea del Norte a través de ciberataques, se refleja como la comisión de un ilícito puede incluso ser legitimada por un Estado.

De manera similar, debido al carácter trasnacional de la Internet, se evidencia también como esta ha sido, y seguramente seguirá siendo usada, para interferir en asuntos de orden soberano de un actor estatal como unas elecciones políticas. Así las cosas, se puede evidenciar una delgada línea de la Internet, como herramienta usada por actores estatales y no estatales para alcanzar sus intereses, puede incluso ser el instrumento para un ilícito o la violación de la soberanía de un Estado debido a los intereses económicos o políticos de un actor del sistema internacional.

Finalmente, y como expresa De Turiso y Sánchez (2016), la Internet ha pasado de ser una mera herramienta que facilitaba los trabajos burocráticos de las oficinas a constituir por si misma un recurso estratégico para muchas naciones. Si bien, en el ciberespacio habitan tanto actores estatales como no estales, para Quintana (2017) “la mayor amenaza para la ciberseguridad son las acciones de los Estados”. Así y como se tratase de un traslado de la teoría realista de Relaciones Internacionales al ciberespacio, en el que se establece al actor estatal como el actor más preponderante, los actores estatales buscan generar recursos que les permita llevar su poderío del mundo real al mundo virtual. Sin embargo y aunque los ciberataques son cada vez más recurrentes, hasta

la fecha no se ha presentado un ciberconflicto propiamente dicho; y como citábamos de la ciber embajadora de Estonia, Heli Tiirmaa-Klaar, no es aún probable una ciberguerra entre actores estatales.

Referencias

20 Minutos (2007). *Nacer mujer es terrorífico en más de medio mundo*. Disponible en: https://blogs.20minutos.es/martinezsoler/tag/bloguistan/

ABC (2013). *Anonymous «hackea» cuentas de internet de Corea del Norte.* Disponible en: https://www.abc.es/tecnologia/redes/20130405/abci-corea-norte-anonymous-201304051330.html

Advox, Global Voices (2018). *Made-in-China fake news overwhelms Taiwan.* Disponible en: https://advox.globalvoices.org/2018/11/30/made-in-china-fake-news-overwhelms-taiwan/

Agencia de Noticias Yonhap (2020). *Un medio de comunicación norcoreano denuncia las 'noticias falsas' en Corea del Sur.* Disponible en: https://sp.yna.co.kr/view/ASP20200505001000883

Agencia EFE (2020). *Seúl califica de "fake news" las informaciones sobre la salud de Kim Jong-un.* Disponible en: https://www.efe.com/efe/espana/mundo/seul-califica-de-fake-news-las-informaciones-sobre-la-salud-kim-jong-un/10001 4232834

Agencia EFE (2021). *Registran la sede de una asociación en Corea del Sur que envió propaganda al Norte.* Disponible en: https://www.efe.com/efe/america/mundo/registran-la-sede-de-una-asociacion en-corea-del-sur-que-envio-propaganda-al-norte/20000012-4529481

AJN, (2020). *Irán detrás de los ciberataques contra red eléctrica israelí que dejó a oscuras al país, según académico persa.* Disponible en: https://agenciaajn.com/noticia/iran-detras-de-los-ciberataques-contra-red-electrica-israeli-que-dejo-a-oscuras-al-pais-segun-academico-irani-155786

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

AN Noticias (2018). *Facebook elimina cuentas de Irán y Rusia que difunden noticias falsas.* Disponible en: https://aristeguinoticias.com/2308/mundo/facebook-elimina-cuentas-de-iran-y-rusia-que-difunden-noticias-falsas/

AP NEWS (2020). *Irán: Mueren 700 por tomar metanos como "cura" contra virus*. Disponible en: https://apnews.com/article/a50e2dc19402cea694909040a2ee6ba7

Avaaz.org (s.f.). *About us.* Disponible en:

https://secure.avaaz.org/page/es/about/

Avast (2019). *Fake News: La lucha de las redes sociales contra la desinformación.* Disponible en: https://blog.avast.com/es/fake-news-la-lucha-de-la-redes-sociales-contra-la-desinformaci%C3%B3n

Avogadro, M. (2011), *"Hacktivism: entramado invisible del Ciberpoder",* en Revista Razón y Palabra, número 77, año 16, México, Instituto Tecnológico y de Estudios Superiores de Monterrey del Estado de México.

Badie, B. (2008). *Le diplómate et l'intrus. L'e entrée des sociétés dans l´aréne international.* París: Fayard.

Barbé, E. (1993). *El Estado como actor internacional: Crisis y consolidación del sistema de Estados.* Papers. Revista de Sociología**,** p. 33-54. Disponible en: https://papers.uab.cat/article/view/v41-barbe-2

Barbé, E. (2008). *Relaciones Internacionales.* Ed. Tecnos, Madrid.

BBC (2013). *Anonymous 'hacks' North Korea social network accounts.* Disponible en: https://www.bbc.com/news/technology-22025724

BBC (2014). *Corea del Norte: ¿Cómo se usa internet en el país más hermético del mundo?* Disponible en: https://www.bbc.com/mundo/noticias/2014/11/141107_tecnologia_corea_norte_uso_internet_ig

BBC (2016). *El Mar de Ross, la zona de la Antártica que se convirtió la reserva marina más grande del mundo*. Disponible en: https://www.bbc.com/mundo/noticias-37796029

BBC (2019). *"¿Por qué me autocensuro en internet?": el testimonio de una periodista sobre la libertad de información en China.* Disponible en: https://www.bbc.com/mundo/noticias-49611094

BBC (2019). *Los planes de Rusia para castigar las "Fake News" y mandar a la cárcel a quienes hablen mal del gobierno*. Disponible en: https://www.bbc.com/mundo/noticias-internacional-47492208

BBC (2021). *Alexei Navalny: quién es el feroz crítico de Putin arrestado en Rusia 5 meses después de ser envenenado*. Disponible en: https://www.bbc.com/mundo/noticias-internacional-55705243

BBC (2021). BBC *China correspondent John Sudworth moves to Taiwan after threats.* Disponible en: https://www.bbc.com/news/world-asia-china-56586655

BBC (2021). *The disinformation tactics used by China*. Disponible en: https://www.bbc.com/news/56364952

BBC (s.f.). *A brief story of fake news*. Disponible en: https://www.bbc.co.uk/bitesize/articles/zwcgn9q

BBC Mundo (2012). *Las claves sobre como atacaría Israel a Irán.* Disponible en: https://www.bbc.com/mundo/noticias/2012/02/120227_como_israel_atacaria_iran_adz

BBC Mundo (2018). *3 puntos para entender porque Irán e Israel están en su momento más tenso de las últimas décadas*. Disponible en: https://www.bbc.com/mundo/noticias-internacional-44072725

BBC, (2009). *Breve historia de las dos Coreas*. Disponible en: https://www.bbc.com/mundo/internacional/2009/05/090526_historia_dos_coreas_mes

BBC, (2020). *Un "sofisticado hackeo de un agente estatal": Australia denuncia un ataque cibernético contra su gobierno*. Disponible en: https://www.bbc.com/mundo/noticias-internacional-53102950

Bejarano, M. (2011). *Capítulo primero: alcance y ámbito de la seguridad nacional en el ciberespacio.* Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3837251

Berenicefn (2018). *Los actores estatales y no estatales en e entorno digital*. Disponible en:https://berenicefn.wordpress.com/2018/12/13/los-actores-estatales-y-no-estatales-en-el-entorno-digital/

Betancour, E. (2018). *Origen y Evolución del Ciberactivismo*. Disponible en: https://ebentancour.com/02_-origen-evolucion-ciberactivismo/

Burgos, E. (2020). *Ciberactivismo, ejercicio de la ciudadanía y participación política en Internet*. Disponible en: https://elucabista.com/wp-content/uploads/2020/04/LIBRO-CIBER-8-abril.pdf

Burgos, E. (2014). "*El hacktivismo: entre la participación política y las tácticas de subversión digital".* en Razón y Palabra, vol. 18, núm. 88, Estado de México, México, Instituto Tecnológico y de Estudios Superiores de Monterrey.

Business Insider (2020). *China enacted a sweeping new law that bars people from posting negative content online, and it could be used to suppress coronavirus news.* Disponible en: https://www.businessinsider.com/china-internet-ban-criticism-could-suppress-coronavirus-news-2020-3

Calduch, R. (1991). *Relaciones Internacionales.* Ed. Ediciones Ciencias Sociales, Madrid.

Carlini, A. (2018). *Las redes sociales como factor de desestabilización*. ISSN-e 2530-125X, Nº 11, 2018, págs. 216- 230.

Carnegie Endowment for Internacional Peace. (2018). *Russian Election Interference. Europe´s Counter to Fake News and Cyber Attacks*. Disponible en: https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf

CCN-CERT (2019). *Desinformación en el ciberespacio*. Disponible en https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3549-ccn-cert-bp-13-desinformacion-en-el-ciberespacio/file.html

CCN-CERT. (2018). *Ciberamenazas y tendencias 2018.* Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2856-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-2018-resumen-ejecutivo-2018/file.html

Cembrero, I. (2020). *Desinformación "made in Russia": Un desafío para las democracias europeas*. Disponible en: https://blogs.elconfidencial.com/mundo/la-historia-no-acaba-aqui/2020-11-11/desinformacion-rusia-desafio-democracias-europeas_2827024/

Cembrero, I. (2020). *Invierno cibernético: así planeó contaminar Irán el agua de Israel en plena pandemia.* Disponible en: https://www.elconfidencial.com/mundo/2020-06-05/invierno-cibernetico-iran-planeo-contaminar-agua-israel-plena-pandemia_2623160/

Centro Criptológico Nacional de España, (2019). *Ciberamenazas y tendencias 2019.* Disponible en: https://www.ccn-cert.cni.es/en/reports/public/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html

Chosun Ilbo (2019). *Kim Jong-un 'Brutally Purged Officials' After Failed Summit.* Disponible en: http://english.chosun.com/site/data/html_dir/2019/05/31/2019053101126.html

Chosun Ilbo (s.f). *About us.* Disponible en: http://english.chosun.com/dhtm/f_1abtus.html

CIA, (2021). *The World Factbook*. Disponible en: https://www.cia.gov/the-world-factbook/countries/korea-north/#people-and-society

Cladera, C. (2020). *Rusia ataca a las vacunas occidentales y dice que convierten a la gente en monos*. Disponible en: https://www.lavozdegalicia.es/noticia/sociedad/2020/12/28/rusia-ataca-vacunas-occiodentales-dicen-convierten-gente-monos/00031609177703287898982.htm

ClearSky Security Ltd, (2018). *Global Iranian Desinformation Operation*. Disponible en: https://www.clearskysec.com/wp-content/uploads/2018/11/Global-Iranian-Disinformation-Operation-Clearsky-Cyber-Security.pdf

Clotet, J. (2010). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Capítulo III, El ciberespacio y el crimen organizado. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

CNN (2020). *US monitoring intelligence that North Korean leader is in grave danger after surgery.* Disponible en: https://edition.cnn.com/2020/04/20/politics/kim-jong-un-north-korea/index.html

Collins Dictionary, (s.f.). *Diccionario.* Disponible en: https://www.collinsdictionary.com/es/diccionario/ingles/cyberattack

Comité Internacional de la Cruz Roja, (2019). *Derecho internacional humanitario y ciberoperaciones durante conflictos armados, Documento de posición del CICR*. Disponible en: https://www.icrc.org/es/document/derecho-internacional-humanitario-y-ciberoperaciones-durante-conflictos-armados

Comité Internacional de la Cruz Roja, (s.f.). *Guerra y derecho*. Disponible en: https://www.icrc.org/es/guerra-y-derecho

Comité Internacional de la Cruz Roja, (s.f.). *Quiénes somos.* Disponible en https://www.icrc.org/es/quienes-somos

Cortés, C; Isaza, L. (2017). *Noticias falsas en internet: la estrategia para combatir la desinformación*. Disponible en: https://www.palermo.edu/cele/pdf/FakeNews.pdf

Cuaderno de Cultura Científica (2020). *Historia de la primera red social*. Disponible en: https://culturacientifica.com/2020/12/01/historia-de-la-primera-red-social/#:~:text=En%201995%20vio%20la%20luz,trav%C3%A9s%20del%20env%C3%ADo%20de%20mensajes.

De la Cuadra, E. (1996). *Internet: conceptos básicos.* Cuadernos De Documentación *Multimedia*, *5*, 35-56. Disponible en: https://revistas.ucm.es/index.php/CDMU/article/view/59279

De la Hera, C. (2020). *Historia de las Redes Sociales: cómo nacieron y cuál fue su evolución*. Disponible en: https://marketing4ecommerce.co/historia-de-las-redes-sociales-evolucion/

Definicion.co (2015). *Definición de herramientas*. Disponible en: https://www.definicion.co/herramientas/

Democracy Speaks ORG (2016). *¿Qué es Ciberactivismo?* Disponible en: https://www.democracyspeaks.org/blog/%C2%BFqu%C3%A9-es-ciberactivismo

Departamento de Seguridad Nacional, Gobierno de España (2016). *Acuerdo Cyber Pledge de la OTAN.* Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/acuerdo-cyber-pledge-otan

Diccionario de Cambridge (s.f.). *Dictionary*. Disponible en: https://dictionary.cambridge.org/dictionary/english/cyberattack

Diccionario de Cambridge (s.f.). *Dictionary*. Disponible en: https://dictionary.cambridge.org/es/diccionario/ingles/fake-news

Diccionario Panhispánico del Español Jurídico (s.f.). *DEJ Panhispánico*. Disponible en: https://dpej.rae.es/lema/red-social

Dupré, M. (2021). *For Russia , with love: the truth behind Putin´s opossition*. Disponible en: https://sofrep.com/news/for-russians-love-of-country-is-stronger-than-fear/

DW (2012). *Putin firma ley que restringe libertad de reunión en Rusia*. Disponible en: https://p.dw.com/p/15Axr

DW (2016). *EE. UU: tiroteo atribuido a falsa noticia sobre Hillary Clinton.* Disponible en: https://www.dw.com/es/ee-uu-tiroteo-atribuido-a-falsa-noticia-sobre-hillary-clinton/a-36654144

DW (2017). *Activista chino Wu Gan es condenado a 8 años de prisión.* Disponible en: https://www.dw.com/es/activista-chino-wu-gan-es-condenado-a-8-a%C3%B1os-de-prisi%C3%B3n/a-41931567

DW (2019). *North Korea: Fake news on both sides is the norm.* Disponible en: https://www.dw.com/en/north-korea-fake-news-on-both-sides-is-the-norm/a-49042595

DW (2020). *Estados Unidos sanciona entidades iraníes por injerencia en elecciones*. Disponible en: https://www.dw.com/es/estados-unidos-sanciona-entidades-iran%C3%ADes-por-injerencia-en-elecciones/a-55366523

DW (2020). *Trump cree que informaciones sobre salud de Kim son "incorrectas".* Disponible en:

https://www.dw.com/es/trump-cree-que-informaciones-sobre-salud-de-kim-son-incorrectas/a-53227760

DW (2021). *Russia: Navalny Supporters hold Valentine´s day protests.* Disponible en: https://www.dw.com/en/russia-navalny-supporters-hold-valentines-day-protests/a-56565484

DW, (2013). *Acusan a China de estar tras ciberataques contra EE.UU*. Disponible en: https://www.dw.com/es/acusan-a-china-de-estar-tras-ciberataques-contra-eeuu/a-16612502

El Diario (2019). *Una campaña de noticias falsas favorable a China intenta intoxicar las elecciones generales de Taiwán.* Disponible en: https://www.eldiario.es/internacional/theguardian/favorable-china-intoxicar-elecciones-taiwan_1_1169395.html

El Mundo (2020). *Elecciones en Taiwán: entre Hong Kong, China y las fake news.* Disponible en: https://www.elmundo.es/internacional/2020/01/10/5e18534f21efa0e0698b45ad.html

El Mundo, (2012). *Obama ordenó personalmente un ataque cibernético contra Irán.* Disponible en: https://www.elmundo.es/elmundo/2012/06/01/internacional/1338585021.html

El Mundo, (2020). *Australia denuncia ser objetivo de un ciberataque apoyado por un país extranjero.* Disponible en: https://www.elmundo.es/internacional/2020/06/19/5eec5f42fdddffada18b464f.html

El Orden Mundial (2020). *La diplomacia de Taiwán.* Disponible en: https://elordenmundial.com/mapas/diplomacia-taiwan/

El País (2019). *Trump se reúne con Kim y se convierte en el primer presidente de EE UU que pisa suelo norcoreano*. Disponible en: https://elpais.com/internacional/2019/06/30/actualidad/1561872037_039511.html

El País (2020). *La UE acusa a Rusia de campaña de fake news sobre el coronavirus*. Disponible en: https://www.elpais.com.uy/mundo/ue-acusa-rusia-campana-fake-news-coronavirus.html

El País (2021). *El corresponsal de la BBC abandona China por temores sobre su seguridad.* Disponible en: https://elpais.com/internacional/2021-03-31/el-corresponsal-de-la-bbc-abandona-china-por-temores-sobre-su-seguridad.html

El País, (2017). *EE UU culpa a Corea del Norte del ciberataque global del virus WannaCry.* Disponible en: https://elpais.com/internacional/2017/12/19/estados_unidos/1513650640_523812.html

El País, (2019). *La India reconoce un ciberataque contra su principal central nuclear.* Disponible en: https://elpais.com/internacional/2019/10/31/actualidad/1572536132_596927.html

El País, (2020) *No habrá ninguna ciberguerra. Habrá una guerra real con una faceta ciber.* Disponible en: https://elpais.com/tecnologia/2019/12/21/actualidad/1576886357_152918.html

El País, (2020). *Australia denuncia ser objetivo de un ciberataque apoyado por un país extranjero.* Disponible en: https://elpais.com/internacional/2020-06-19/australia-denuncia-ser-objetivo-de-un-ciberataque-apoyado-por-un-pais-extranjero.html

El Periódico, (2020). *Al menos 300 iraníes mueren tras tomar metanol para curar el Covid-19*. Disponible en: https://www.elperiodico.com/es/internacional/20200327/decenas-iranis-mueren-tomar-metanol-curar-covid-19-7907563

Euronews (2019). *Putin Firma leyes polémicas sobre las noticias falsas*. Disponible en: https://es.euronews.com/2019/03/18/putin-firma-leyes-polemicas-sobre-las-noticias-falsas.

Europa Press (2021). *China pide a la BBC que se disculpe por una serie de "noticias falsas" sobre la COVID-19.* Disponible en: https://www.europapress.es/internacional/noticia-china-pide-bbc-disculpe-serie-noticias-falsas-covid-19-20210204160131.html

Excelsior (2021). *Hermana de Kim amenaza a Corea del Sur por 'lluvia' de propaganda.* Disponible en: https://www.excelsior.com.mx/global/hermana-de-kim-amenaza-a-corea-del-sur-por-lluvia-de-propaganda/1446619

Forbes (2020). *Reportan grave a Kim Jong-un, líder de Corea Norte, tras cirugía.* Disponible en: https://www.forbes.com.mx/noticias-reportan-grave-kim-jong-un-corea-norte-tras-cirugia/

France 24 (2017). *Condenan a ocho años de prisión al bloguero chino Wu Gan.* Disponible en: https://www.france24.com/es/20171227-condena-bloguero-chino-wu-gan

France 24 (2021). *China prohíbe la transmisión de la 'BBC'; se abre nueva tensión con Reino Unido.* Disponible en: https://www.france24.com/es/asia pac%C3%ADfico/20210211-china-bbc-etnia-uigur-libertad-de-expresion-reino-unido

France 24, (2017). *Estados Unidos culpa a Corea del Norte de ciberataque 'WannaCry'.* Disponible en: https://www.france24.com/es/20171219-wannacry-trump-virus-corea

France 24, (2021). *Naciones Unidas reportó que Corea del Norte fortaleció su programa nuclear en 2020.* Disponible en: https://www.france24.com/es/asia-pac%C3%ADfico/20210209-onu-corea-norte-misiles-programa-nuclear

France24, (2021). *Rusia: miles de detenidos en protestas a favor del opositor Alexéi Navalny*. Disponible en: https://www.france24.com/es/europa/20210131-rusia-detenidos-protestas-apoyo-alex%C3%A9i-navalny

Frontline Defenders (s.f.). *#Ciberactivismo.* Disponible en: https://www.frontlinedefenders.org/es/right/cyber-activism

Galindo, A; Rivero, G. (2021). *K-pop y paro nacional: Transparencia sí, pero no así.* Disponible en: https://www.elespectador.com/mundo/mas-paises/k-pop-y-paro-nacional-transparencia-si-pero-no-asi-article/

Ganuza, N. (s.f). *La situación de la ciberseguridad en el ámbito internacional y en la OTAN.*

García-Estévez, N. (2015). *La convergencia activista en Hong Kong: del ciberactivismo de "occupy central" al hacktivismo de "operación Hong Kong".* En Move.Net: Actas del I Congreso Internacional Move.Net sobre Movimientos Sociales y TIC (139- 156), Sevilla: Grupo Interdisciplinario de Estudios en Comunicación, Política y Cambio Social de la Universidad de Sevilla (COMPOLÍTICAS). Disponible en: https://idus.us.es/handle/11441/44044

García-Estévez, N. (2018). *Origen, evolución y estado actual del activismo digital y su compromiso social. Ciberactivismo, hacktivismo y slacktivismo.* En II Congreso Internacional Move.net sobre Movimientos Sociales y TIC (139-156), Sevilla: Grupo Interdisciplinario de Estudios en Comunicación, Política y Cambio Social de la Universidad de Sevilla (COMPOLÍTICAS). Disponible en: https://idus.us.es/handle/11441/70636

Gayarre, A. (2012). *EE.UU e Israel salpicados por el virus Flame*. Disponible en: https://p.dw.com/p/15Ijy

Gil, J. (2017). *La integración del ciberespacio en el ámbito militar.* Disponible en: http://www.seguridadinternacional.es/?q=es/content/la-integraci%C3%B3n-del-ciberespacio-en-el-%C3%A1mbito-militar

Gizmodo (2016). *9 More Viral Photos That Are Completely Fake*. Disponible en: https://gizmodo.com/9-more-viral-photos-that-are-completely-fake-1754282672

Global Times (2021). China shows zero tolerance for fake news by banning BBC World News. Disponible en: https://www.globaltimes.cn/page/202102/1215538.shtml

Gómez, C. (2019). *A 10 años de las protestas en Irán que cambiaron la República Islámica de Irán*. Disponible en: https://www.france24.com/es/20190613-protestas-cambios-iran-redes-sociales

Herrero de Castro, R. (s.f). *El concepto de Interés Nacional.* Dialnet- Unirioja. https://www.bbc.com/mundo/noticias-37796029

Hurtado, L. (2020). *El bulo del alcohol que cura el coronavirus mata más de 200 personas en Irán y Turquía*. Disponible en: https://www.elmundo.es/internacional/2020/03/25/5e7b4cb221efa0455c8b45a3.html

INTECO -Instituto Nacional de Tecnologías de la Comunicación (s.f). *¿Qué es (y qué no) un Hacker?* Disponible en: https://egov.ufsc.br/portal/sites/default/files/cdn_hacking_v2.pdf

International Institute for Strategic Studies (2019). *Chapter Five: China's cyber power in a new era.* Disponible en:https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5

Jouve, E. (1992). *Relaciones Internacionales*, PUF, París.

Kirkpatrick, D; Bergman, R. (2020). *Irán ha desarrollado armas más potentes que sus misiles.* Disponible en: https://www.nytimes.com/es/2020/01/09/espanol/mundo/iran-guerra.html

La República (2020). *EE.UU. dice que hackers chinos e iraníes buscan robar investigación de covid-19*. Disponible en: https://www.larepublica.co/globoeconomia/eeuu-dice-que-hackers-chinos-e-iranies-buscan-robar-investigacion-de-covid-19-3005492

La Vanguardia (2020). *El origen del Brexit.* Disponible en: https://www.lavanguardia.com/vida/junior-report/20200124/473098805071/brexit- origen-inmigracion-populismo-fake-news-crisis.html

La Vanguardia, (2017). *Setenta años separados.* Disponible en: https://www.lavanguardia.com/vida/juniorreport/20171127/433146241202/corea-setenta-anos-separados.html

La Voz de Galicia (2017). *¿Cómo nacen las "fake news"?* Disponible en: https://www.lavozdegalicia.es/noticia/internacional/2017/11/15/fake-news/00031510766693688279858.htm

Lexico (s.f.) *Definición de herramienta por Oxford Dictionary*. Disponible en: https://www.lexico.com/es/definicion/herramienta

Linares, N. (2019). *Los Ciberataques en el Derecho Internacional Público*. Disponible en:https://repositori.upf.edu/bitstream/handle/10230/42136/TFGdret1819NataliaLinares.pdf?sequence=1&isAllowed=y

Lukes, S. (1985). *El poder, un enfoque radical.* Ed. Siglo XXI, Madrid.

Mackenzie, M. (2019), *Rusia, China, Irán y Corea del Norte las principales fuentes de las noticias falsas que llegan a Europa*. Disponible en: https://www.20minutos.es/noticia/3586915/0/union-europea-luchar-propaganda-hostil/

Mapas del Mundo, (2013). *Mapa de China*. Disponible en: https://espanol.mapsofworld.com/continentes/asia/mapa-de-china/

Maquiavelo (s.f.). *El Principe*. Disponible en: https://drive.google.com/file/d/0B9_RR11OoXJyNDQ3OTFhYzUtNzdkMC00ODgwLTg2MWYtOTFmMjYzNjY2ZDAz/view?hl=es

Márquez, W. (2011). *Ciberespacio: el nuevo ámbito de la guerra para el Pentágono.* Disponible en: https://www.bbc.com/mundo/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm

Mars, A. (2018). *¿Cómo influyó la desinformación en las elecciones presidenciales?* - Disponible en: https://elpais.com/internacional/2018/02/24/estados_unidos/1519484655_450950.html

Martínez, C. (2015). *El uso de ciberataques como herramienta de relaciones internacionales por parte de los actores estatales: los casos de Estados Unidos y Rusia.* Disponible en: https://repositorio.comillas.edu/rest/bitstreams/2873/retrieve

Martínez, J. (2018). *Así funcionaba la fábrica rusa de las noticias falsas*. Disponible en: https://elpais.com/internacional/2018/02/20/estados_unidos/1519141912_318546.html

Medina, Arely, & Sepeda, María José. (2019). *Feminismo islámico en la web 2.0: el caso de blogistán. PAAKAT: revista de tecnología y sociedad, 9*(17) Epub 10 de diciembre de 2019.Disponible en: https://doi.org/10.32870/pk.a9n17.457.

Membrado, Z. (2016). *En Irán la vida de una mujer ya no vale la mitad que la de un hombre*. Disponible en: https://www.elmundo.es/sociedad/2016/03/27/56f6c430e2704e272d8b4606.html

Merle, M. (1991). *Sociología de las relaciones internacionales*. Alianza, Madrid.

Ministerio de Defensa del Reino de España, (2010). *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Ministerio de Relaciones Exteriores, Unión Europea y Cooperación del Reino de España, (2020). *China*. Disponible en: http://www.exteriores.gob.es/Documents/FichasPais/CHINA_FICHA%20PAIS.pdf

Ministerio de Relaciones Exteriores, Unión Europea y Cooperación del Reino de España (2021). *Rusia.* Disponible en: http://www.exteriores.gob.es/documents/fichaspais/rusia_ficha%20pais.pdf

Ministerio de Relaciones Exteriores, Unión Europea y Cooperación del Reino de España. (2021). *Irán.* Disponible en: http://www.exteriores.gob.es/documents/fichaspais/iran_ficha%20pais.pdf

Moïsi, D. (2009). *La Geopolítica de las Emociones*. Disponible en: https://www.academia.edu/31586529/LA_GEOPOLITICA_DE_LAS_EMOCIONES

Morgenthau, H.J. (1948). *Politics among Nations. A struggle for power and peace*, Nueva York, Aifred A. Knopf.

Morozov, E. (2009). *The brave new world of slacktivism*. Disponible en: https://drive.google.com/file/d/0B_6AAGWfBODkdlI2NE9ybnJYekU/view

Morozov, E. (2017). *El impacto del activismo digital en la política de la Post Guerra Fria. En La Era de la Perplejidad.* Repensar el Mundo que conocíamos, Madrid, BBVA. Disponible en: https://www.bbvaopenmind.com/articulos/el-impacto-del-activismo-digital-en-la-politica-de-la-post-guerra-fria/

Muñoz, P. (2013). *La influencia de los actores no estatales en el sistema internacional.* Disponible en: https://afese.com/img/revistas/revista58/influencia.pdf

National Geographic, (2019). *Estos son los 6 países que tienen más restricciones al acceso de internet.* Disponible en: https://www.ngenespanol.com/lugares/6-paises-tienen-mas-restricciones-al-acceso-de-internet/amp/

Navarrete, F, (2014). *El ciberespacio: Nuevo escenario de confrontación*. *Anu. Mex. Der.* 2014, vol.14, pp.863-868.

Nebreda, R. (2013). *El origen de Internet. El camino hacia la red de redes*. Disponible en: *http://oa.upm.es/22577/1/PFC_IVAN_NEBREDA_RODRIGO.pdf*

New York Magazine (2013). *Hackers Put This Very Unflattering Picture of Kim Jong Unon North Korea's Flickr Page*. Disponible en: https://nymag.com/intelligencer/2013/04/kim-jong-un-pig-photo-hackers-anonymous.html

Nieman Lab, Harvard University (2018). *Fighting back against fake news: A new UN handbook aims to explain (and resist) our current information disorder.* Disponible en: https://www.niemanlab.org/2018/09/fighting-back-against-fake-news-a-new-un-handbook-aims-to-explain-and-resist-our-current-information-disorder/

Paz, D. (2018). *¿Por qué miles de activistas arremeten contra el mundial de Rusia 2018?* Disponible en: https://mundo.sputniknews.com/20180319/george-soros-mundial-futbol-rusia-1077142044.html

Perales, O. (2008). *Esfera pública y medios electrónicos*. En revista electrónica: Razón y Palabra. N° 61.

Petrino, J. (2019). *ARPANET, el "padre" de internet cumple 50 años*. Disponible en: https://www.iri.edu.ar/index.php/2019/10/29/arpanet-el-padre-de-internet-cumple-50-anos/

Quintana, Y. (2017). *Hackers rusos, ciberguerra y el conflicto en Cataluña. Disponible en:* https://ctxt.es/es/20171122/Politica/16256/ciberguerra-hackers-rusos-cni-assange-ataques-informaticos-ctxt-quintana.htm

Reuters (2019). *Explainer: What was Hong Kong's 'Occupy' movement all about?* Disponible en: https://www.reuters.com/article/us-hongkong-politics-occupy-explainer-idUSKCN1S005M

Reventós, L. (2012). *Flame, el código malicioso más complejo para ciberespiar*. Disponible en: https://elpais.com/internacional/2012/05/28/actualidad/1338218887_695257.html

Revista digital INESEM (2016). *Hacktivismo: ¿Qué hay detrás de este movimiento activista?* Disponible en: https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

Riordan, S. (2005). *Adiós a la diplomacia*. Madrid: Siglo Veintiuno Editores.

Roa, M. (2020). *¿Se aprovecha Rusia del miedo al coronavirus con noticias falsas y teorías de la conspiración?* Disponible en: https://cnnespanol.cnn.com/video/coronavirus-noticias-falsas-rusia-campana-desinformacion-conspiracion-pkg-seg-michael-roa/

Rodriguez, A. (2020). *Hacktivismo, lucha y protesta en internet*. Disponible en: https://elordenmundial.com/hacktivismo-lucha-protesta-internet-ciber-geopolitica/

RTVE, (2009). *Internet nació de un proyecto militar de Estados Unidos en la Guerra Fría.* Disponible en: https://www.rtve.es/noticias/20090517/internet-nacio-proyecto-militar-estados-unidos-guerra-fria/276608.shtml

RTVE, (2013). *Un informe desvela que el Ejército chino está detrás de los ciberataques a EE.UU*. Disponible en: https://www.rtve.es/noticias/20130220/ciberataques-estados-unidos-china/609381.shtml

Salas, C. (2019). *La primera 'fake news' de la historia.* Historia Y Comunicación Social, 24(2), 411-431. Disponible en: https://doi.org/10.5209/hics.66268

Salcedo Et. Al. (2011). *Hackers en la sociedad de la información: Análisis de su dinámica desde una perspectiva social.* Visión Electrónica, 2012-06-01 Volumen:6, Año:1 pág: 115–125.

Sánchez, A. (2020). *La UE señala a Rusia y China como instigadoras de campañas de desinformación en plena pandemia*. Disponible en: https://elpais.com/internacional/2020-06-10/la-ue-senala-a-rusia-y-china-como-instigadoras-de-campanas-de-desinformacion-en-plena-pandemia.html

Sarabia, D. (2016). *Las 9 noticias falsas más locas de la campaña electoral en EEUU*. Disponible en: https://www.eldiario.es/tecnologia/noticias-locas-campana-electoral-eeuu_1_3737236.html

Semana, (2013). *China al ataque cibernético.* Disponible en: https://www.semana.com/mundo/articulo/china-ataque-cibernetico/334287-3/

Sigholm, J. (2016). *Non-State Actors in Cyberspace operations*. Disponible en: https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations#:~:text=Employment%20of%20such%20non%2Dstate,will%20likely%20reshape%20future%20warfare.

Sisco (2018) *Así pasó en Irán*. Disponible en: https://books.google.com.co/books?id=zUdvDwAAQBAJ&pg=PT279&lpg=PT279&dq=bloguist%C3%A1n&source=bl&ots=BFb9WGIylc&sig=ACfU3U3-FYaAvdp54MxS44D-3jsNLLmaPQ&hl=es-419&sa=X&ved=2ahUKEwiIk46u7ePwAhXXSzABHWrEBQwQ6AEwEXoECBAQAw#v=onepage&q=bloguist%C3%A1n&f=false

Soler, T. (2020). *Amenazas en el ciberespacio*. Disponible en: https://atalayar.com/blog/amenazas-desde-el-ciberespacio

Stubbs, J; Bing, C. (2019) *La campaña de desinformación de origen iraní más grande, persistente y global*. Disponible en: https://www.reuters.com/article/usa-iran-facebook-idESKCN1LE1EM-OESTP

Swiss Info (2021). G*rupo activista envía propaganda a Corea del Norte pese a nueva prohibición.* Disponible en: https://www.swissinfo.ch/spa/corea-conflicto_grupo-activista-env%C3%ADa-propaganda-a-corea-del-norte-pese-a-nueva prohibici%C3%B3n/46578754

Swiss Info, (2021). *Corea del Norte robó USD 2.000 millones para armas en ciberataques, según informe de ONU.* Disponible en: https://www.swissinfo.ch/spa/corea-del-norte-rob%C3%B3-usd-2.000-millones-para-armas-en-ciberataques--seg%C3%BAn-informe-de-onu/45147122

Televisa News (2017). *Corea del Norte niega responsabilidad en ciberataque con virus Wannacry.* Disponible en: https://noticieros.televisa.com/ultimas-noticias/corea-norte-niega-responsabilidad-ciberataque-virus-wannacry/

Tétrault-Farber, G; Soldatkin, V. (2021). *Rusos comienzan una protesta con velas en solidaridad con el opositor Navalny*. Disponible en: https://www.reuters.com/article/rusia-politica-navalny-idESKBN2AE0HD

The Straits Times, (2020). *US poll: More worry about Chinese cyber attacks than trade gap.* Disponible en: https://www.straitstimes.com/world/united-states/us-poll-more-worry-about-chinese-cyber-attacks-than-trade-gap

The Washington Post (2013*). Hacker group Anonymous is no match for North Korea.* Disponible en: https://www.washingtonpost.com/news/worldviews/wp/2013/06/27/hacker-group-anonymous-is-no-match-for-north-korea/

https://elpais.com/internacional/2017/12/26/actualidad/1514266533_740926.html

The Washington Post (2015). *The 10 things you need to know about cyberconflict.* Disponible en: https://www.washingtonpost.com/news/monkey-cage/wp/2015/09/11/the-10-things-you-need-to-know-about-cyberconflict/

Trejos, L. (2016). *Los actores no estatales en la sociedad internacional: una aproximación a la diplomacia ciudadana en Colombia.* Vol 24. N 1. Disponible en: http://dx.doi.org/10.14482/indes.24.1.8685

Turiso, J; Sánchez (2016). *La Evaluación del Conflicto hacia un nuevo escenario bélico*. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

Universidad Politécnica de Cataluña, (2009). *Historia de internet*. Disponible en: https://www.fib.upc.edu/retro-informatica/historia/internet.html

Urreiztieta, E. (2020) U*n Informe señala a China y Rusia como los principales generadores de Fake News del mundo sobre la Covid-19*. Disponible en: https://www.elmundo.es/espana/2020/05/01/5eac070221efa07e148b45fe.html

Vargas, L. (2014). *Actores no estatales y política exterior: una revisión preliminar del caso colombiano.* Revista Análisis Internacional. Disponible en: https://core.ac.uk/download/pdf/268203067.pdf

Velasco de Castro, R. (2012). *Presencia y participación de las mujeres iraníes en la política y en los medios de comunicación*. Disponible en: https://idus.us.es/bitstream/handle/11441/34630/Pages%20from%20LIBRO%20ACTAS%20I%20CONGRESO%20COMUNICACI%D3N%20Y%20G%C9NERO-3.pdf;jsessionid=F094DF8487ACB472F0DE52400BC29A4D?sequence=1

Verdes-Montenegro, F. (s.f*). La teoría del poder estructural y la securitización: una propuesta teórica para el estudio de las transformaciones del poder y la seguridad.* Disponible en: https://aecpa.es/files/view/pdf/congress-papers/11-0/984/

Vidal, M. (2017). *El Gobierno de Hong Kong recomienda la reforma electoral que desea Pekín*. Disponible en: https://elpais.com/internacional/2014/06/30/actualidad/1404147230_070749.html

Ynet, (2021). *Los ciberataques de Irán contra Israel continuarán.* Disponible en: https://www.ynetespanol.com/tendencias/ciencia-y tecnologia/article/ByW1W6DXu