El ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos

Silvia Marina Rivas
(El Salvador)

EL CIBERESPACIO COMO ZONA DE CONTROL GEOPOLÍTICO Y PAPEL DE LAS POTENCIAS POR LA SUPREMACÍA CIBERNÉTICA: CHINA Y ESTADOS UNIDOS

Silvia Marina Rivas

RESUMEN

El uso de internet a través de herramientas, aplicaciones y entornos digitales al alcance de millones de usuarios alrededor del mundo, volvió al ciberespacio un área geopolítica. Este artículo pretende hacer una breve descripción sobre los métodos y actores dentro de la llamada cibergeopolítica y la carrera en la que los Estados aseguran un lugar privilegiado en la fabricación de dispositivos y la creación de software. La competencia por lograr el control de la información y la distribución de datos entre las potencias es de interés no solo de empresas privadas, sino de los propios gobiernos en aras de tomar ventaja con otros Estados, utilizando diversos medios que incluyen nuevas modalidades, como: espionaje por medio de hackeos a oficinas gubernamentales, figuras políticas, manipulación de elecciones y ataques a infraestructuras críticas. Las intrusiones en los sistemas de datos con información privada, han llegado a trastocar los derechos de los propios ciudadanos con la justificación del mantenimiento de la seguridad nacional. Así, a través de una investigación bibliográfica se identifican los conceptos fundamentales para entender cómo se configuran las amenazas cibernéticas entre los Estados y usuarios, y cuáles son los puntos claves del por qué el ciberespacio es ahora un área de competencia entre dos de las principales potencias tecnológicas, como Estados Unidos y China; cuestión que en el mediano plazo configurará el mercado de dispositivos y la transmisión de datos entre los usuarios a nivel planetario dentro de una carrera tecnológica y cibernética en pleno desarrollo.

PALABRAS CLAVE: ataques - cibergeopolítica - ciber agentes - ciber amenazas - ciberseguridad - ciberdefensa - espionaje - geopolítica.

CYBERSPACE AS A ZONE OF GEOPOLITICAL CONTROL AND THE ROLE OF THE GREAT POWERS FOR THE CYBER SUPREMACY: CHINA AND THE UNITED STATES

Silvia Marina Rivas

ABSTRACT

The use of Internet through tools, applications, and digital environments available to millions of users around the world, turned cyberspace into a geopolitical area. This article aims to make a brief description about methods and actors within the so-call cybergeopolitics and the race in where States are in a privileged place in the manufacture of devices and creation of software. The competition to achieve control of the information and the data distribution between the great powers is of the interest not only of privates companies, but rather the governments themselves to take advantage of other States, using various means that include new modalities, such as: espionage by hacking government offices, political figures, manipulation of elections and attacks on critical infrastructures. Intrusions in data systems with private information, they have to come to disrupt the rights of citizens themselves with justification of maintaining national security. Thus, through a bibliographic research, the fundamental concepts to understand how cyber threats are configured between States and users are identified, and what are the key points of why cyberspace is now an area of competition between two of the main technological powers, such as the United States and China; an issue that, in the medium term, will shape the device market and the transmission of data between users on a planetary level, within a technological and cybernetic race in full development.

KEYWORDS: attacks - cyber politics - cyber agents - cyber-attacks - cybersecurity - cyber defense - espionage - geopolitics.

El ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos

Silvia Marina Rivas[1]
(El Salvador)

Introducción

Con los movimientos de las potencias en diferentes ámbitos, incluyendo el sanitario por la búsqueda de una cura para el virus COVID-19, el tema de la geopolítica y el neorrealismo ha ocupado buena parte del análisis en las relaciones internacionales actuales. Así, la geopolítica entendida como el estudio de los efectos de la política en la geografía física y humana consta de cuatro ámbitos de aplicación tradicional: tierra, mar, aire y espacio exterior; han sido aprovechados por los Estados para generar dominio y extensión, no solo de su territorio, sino sobre otros a través de instrumentos tanto de poder duro como blando.[2] Sin embargo, desde finales del siglo XX y plenamente en el siglo XXI, la geopolítica como estudio ha experimentado una ampliación de sus ámbitos de acción con la masificación del uso de internet en la vida cotidiana de las poblaciones. El entorno digital se volvió un área de interés para obtener ventajas

1 Licenciada en Relaciones Internacionales por la Universidad de El Salvador, Master en Paz, Seguridad y Conflictos Internacionales, Docente del área Política Internacional de la Escuela de Relaciones Internacionales de la Universidad de el Salvador.

2 Miguel Barrios, "La Geopolítica Digital: un campo de lucha por la supremacía mundial", *América Latina en movimiento*, 30 de septiembre de 2019, https://www.alainet.org/es/articulo/202386.

sobre los demás Estados dentro del sistema. Así, una serie de oportunidades y amenazas como el espionaje en la modalidad cibernética y la exposición de datos confidenciales a través de la vulneración de estos ha colocado retos en la seguridad y defensa tanto estatal como privada debido a una acelerada dinámica de desarrollo e innovación en los entornos virtuales.

El lugar que juegan los actores estatales en el ciberespacio es elemental, puesto que el manejo y desarrollo de las tecnologías de conectividad y dispositivos en términos amplios, así como las redes de distribución de internet, supone una influencia directa en otros junto con una potencial oportunidad/amenaza de espiar el tráfico de datos estatal y poblacional. En ese sentido, las potencias tecnológicas "mueven sus piezas" en el tablero mundial, a fin de posicionarse con hegemonía en la distribución y desarrollo de las tecnologías cibernéticas, lo que supone entonces una modalidad reciente de conflicto geopolítico, tema que se tratará de desarrollar a continuación.

I. Contexto

El ciberespacio se traduce en un conjunto compuesto por redes de información, dispositivos con capacidad de conectarse, protocolos y entornos para el flujo de datos en bytes; es un espacio creado completamente por el ser humano que carece de territorialidad definida y de alguna forma, por no poseer territorio, el ejercicio de la regulación de uno o varios Estados no es posible a nivel planetario.[3] El uso cotidiano del internet por la población mundial y la dependencia de ésta en sus diferentes ámbitos: formación, comunicaciones, ocio, empleo, entre otros; es constante y creciente, caracterizándose en ser rápido y de fácil acceso en información a quienes lo poseen.[4] La interacción social y laboral ha cambiado la forma en que las personas se comunican, ya que, se

3 Ángel Gómez de Ágreda, "Ciberseguridad en ciudades", *Cuaderno de Estrategia 206: Instituto Español de Estudios Estratégicos* (2020): 175-211, http://www.ieee.es/Galerias/fichero/cuadernos/CE_206_LasCiudades_AgentesCriticosParaUnaTransformacionSostenibleDelMundo.pdf.

4 Ángel Gómez de Ágreda, "CIBERESPACIO: de ratones y hombres", n.o 51 (2015): 1-9, http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO51-2015_Ciberespacio_AGdeAgreda.pdf.

establecen relaciones más allá de las fronteras territoriales, permitiendo a su vez, la transmisión de datos en tiempo real.

El internet también ha abierto el espacio como vector principal de voces de protesta sobre situaciones puntuales como derechos humanos, desigualdades, actos de negligencia estatal, entre otros; cuestiones que dan como resultado la exigencia de políticas de intervención, a través de la recolección de firmas electrónicas y el uso de redes sociales, "viralizando" estas situaciones con el fin de generar reacciones de apoyo que ejerzan presión sobre las autoridades competentes y por qué no decirlo, la comunidad internacional.[5] No obstante, así como el internet ha ofrecido un entorno de comunicación más amplio y ha visibilizado problemas que no tenían atención; también, ha engrosado la brecha social, económica y técnica de poblaciones enteras, con menos acceso a recursos, oportunidades de educación y empleabilidad mejores en sectores formales.

El entorno web no está exento de amenazas y de manejos con fines ilícitos, puesto que la existencia del ciberespacio amplió la diversidad de negocios y movimiento de capitales ilegales a través de diferentes bancos alrededor del mundo en lo que se denominó como: "efecto ventilador", barriendo el rastro de las transacciones por las que se había blanqueado el capital;[6] tiempo después, la diversificación de delitos en el ciberespacio llevado a cabo por estructuras organizadas o por habilidosos hackers a personas y después a corporaciones, incluyendo carteras de Estado, fueron en aumento; la existencia de los denominados virus y programas intrusivos como los llamados "troyanos" causaron varios problemas a los usuarios que cayeron en este tipo de malware.

Con la pandemia de COVID-19, la cantidad de usuarios de internet ha aumentado exponencialmente, en parte por la necesidad de la transformación de los empleos y sistemas de enseñanza bajo modalidad virtual como medida contingencial en el manejo de la prevención de contagios. De los 7,750 millones

5 Miguel Barrios y Norberto Emmerit, "Geopolítica de la seguridad: las disputas geopolíticas del ciberespacio (III)", *América Latina en movimiento,* 22 de marzo de 2017, https://www.alainet.org/es/articulo/184284.

6 Francisco Veiga, *El Desequilibrio como Orden, Segunda edición* (Madrid: Allianza, 2015).

de habitantes a nivel mundial, 4,131 millones poseen dispositivos con acceso a internet, de los cuales 3,800 millones poseen redes sociales.[7] Con estas cifras, es claro que al igual que el número de personas con acceso al ciberespacio ha crecido con respecto a 2019 en el que se registraron 3,924 millones de usuarios,[8] así las cosas, las amenazas en el entorno serían directamente proporcionales a éste.

II. Existencia de ciberagentes y ciberamenazas

Según el Centro Criptológico Nacional de España, los ciberataques y las ciber amenazas, constituyen uno de los riesgos globales de mayor impacto y probabilidad de ocurrencia ubicándose con mayores posibilidades en comparación a las crisis alimentarias y los conflictos interestatales.[9] En ese mismo orden de ideas, las amenazas a la seguridad en el tráfico de datos y archivos son cada vez mayores, más complejas y amplias de forma que es indispensable actualizar estrategias de contención para superar vulnerabilidades, tanto por agentes privados como por públicos y salvaguardar datos de posibles intervenciones.

En cuanto a las amenazas y ataques en el ciberespacio pueden encontrarse de varios tipos y fines, los cuales muchas veces van un paso adelante de las estrategias de defensa y protección de datos, por lo que una respuesta efectiva y pronta es necesaria en el resguardo de documentos, archivos y programas sensibles o vulnerables.

7 Centro Criptológico Nacional, *Ciberamenzas y Tendencias 2020* (Ministerio de Defensa Español, septiembre de 2020), https://www.ospi.es/export/sites/ospi/documents/documentos/Informe-Ciberamenazas-Tendencias_2020.pdf.

8 *Ibíd.*

9 Centro Criptológico Nacional, *Ciberamenazas y tendencia 2018* (Ministerio de Defensa Español, 2018), https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html.

El ciberespionaje está centrado en su mayoría hacia los Estados, aunque no descarta otros blancos como la industria y organizaciones privadas, siendo esta una nueva forma de espionaje e intervención en las comunicaciones y datos a fin de obtener información confidencial y sensible a partir de la sustracción de documentos y su posterior publicación o utilización. La ciberdelincuencia, como su nombre lo indica, puede definirse como acciones llevadas a cabo por estructuras criminales que se dedican a sustraer, secuestrar y manipular información a fin de cobrar por su recuperación o si fuera el caso, retiro de los datos manipulados de internet; este tipo de ataques puede afectar tanto a agentes estatales como a privados, incluyendo ciudadanos comunes. El ciberterrorismo tiene objetivos políticos y de reivindicación de su lucha atacando a través de disrupción del servicio, publicación de propaganda y secuestro de datos; estas actividades le permiten publicitarse y de alguna forma obtener un mayor reclutamiento y financiación.[10]

A diferencia de los anteriores, el ciberactivismo cuyo *modus operandi* tiene mayor relación con la toma de control de los sistemas y manipulación de actores estatales como organizaciones privadas; tiene como fin, manifestarse en contra de medidas o acciones específicas por parte de los atacados, su objetivo no es necesariamente monetario, sino que lleva implícito el componente político a través de la visibilización de la causa con estas actividades;[11] con ello buscan que mayor número de personas se unan presionando para la obtención de sus metas.

III. Tipos de ciberataques

Si bien, los ciberagentes que amenazan la seguridad de los datos que fluyen en el ciberespacio tienen objetivos diferentes, las estrategias para vulnerar la seguridad de dispositivos y servidores son bastante parecidas, algunas de las más utilizadas son las siguientes: *ransomware* o secuestro de datos, *phishing*

10 *Ibíd.*

11 *Ibíd.*

o suplantación de identidad, códigos dañinos, entre otras modalidades como el ataque a páginas web, con el objetivo de reivindicar luchas y pensamientos utilizados por activistas y grupos terroristas, creando así, estos últimos una idea de omnipresencia a través del ciberespacio,[12] magnificando la capacidad real de la organización.

Las acciones delictivas emprendidas contra usuarios ya sean particulares, corporativos o estatales, no siempre están determinados por los mismas causas y fines, a pesar de que sean tácticas o ataques comunes tal como se presenta en la ilustración 1, estos se diferencian entre sí dependiendo de quién o quiénes lo patrocinan o realizan.

Ilustración 1: Clasificación de ciberataques y su origen.

Fuente: Centro Criptológico Nacional, España 2020.

12 TIC Negocios, "Qué es un ciberataque y para qué sirve | TicNegocios.es", *Tecnología para los negocios*, accedido el 12 de marzo de 2021, https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/.

Independientemente de lo anterior, el ciberespionaje llevado a cabo entre Estados con finalidades de posicionamiento estratégico, ha repercutido en diversos campos. De acuerdo con Pedro Baños,[13] varios ciberataques fueron utilizados para vulnerar procesos democráticos, es decir, cabe la posibilidad que algunas elecciones estuvieran "arregladas" a través de agresiones cibernéticas con modificación de resultados electrónicos, tal como se supuso en la investigación llevada a cabo por el FBI[14] estadounidense y la posible intervención rusa en las elecciones entre Hillary Clinton y Donald Trump, en la que este último resultó ganador.[15]

Ilustración 2: Sistema de espionaje utilizado por Estados.

Fuente: Iñaki Jiménez, Pinterest 2020.

Uno de los escándalos que más impactó a nivel mundial por la cantidad de información divulgada, se refiere a la publicación de cables de diferentes gobiernos bajo el portal de Wikileaks, que dejaron al descubierto el alcance del ciberespionaje por parte de los Estados Unidos hacia personas, instituciones y países; inclusive a aquellos considerados aliados del gobierno estadounidense, lo que causó incomodidad y tensión en las relaciones diplomáticas entre los Estados y desconfianza de los ciudadanos.

13 Pedro Baños, "Ciberespionaje, influencia política y desinformación (I)", *El Orden Mundial - EOM,* 20 de diciembre de 2017, https://elordenmundial.com/ciberespionaje-influencia-politica-y-desinformacion-i/.

14 Buró Federal de Investigaciones, FBI, por sus siglas en inglés.

15 Redacción, "La investigación de la injerencia rusa en las elecciones de EE.UU. en las que venció Trump en 300 palabras", *BBC News Mundo,* accedido 11 de marzo de 2021, https://www.bbc.com/mundo/noticias-internacional-46400948.

Sin embargo, entre algunos de los estadounidenses se consideró que las filtraciones constituían una amenaza a la seguridad nacional al haber hecho públicos una cantidad de información entre las que se incluía toda una serie de operaciones dentro las guerras libradas por los Estados Unidos en Oriente Medio y las estrategias de interrogación utilizadas ante potenciales terroristas.[16]

Aunque el escándalo de ciberespionaje se dio en torno a la NSA[17] de los Estados Unidos, no es el único país que potencialmente estaría espiando a sus ciudadanos y vecinos. Según Amnistía Internacional, varios países entre los que se encuentran China, Francia, Reino Unido y Rusia espían los mensajes de texto y actividades de sus ciudadanos en el ciberespacio con la justificación de la prevención del terrorismo y así mejorar la seguridad interna.[18] Aunque a simple vista pareciera que se trata de una estrategia de protección, en realidad se convierte en un espacio donde el Estado obtiene, con la información recabada, datos de líderes opositores, políticos o personas que son incómodas al aparato de gobierno.

En 2015, el diario digital *Nation Vanguard* informó sobre algunas de las estrategias utilizadas por el FBI en contra de sospechosos o agentes incómodos al gobierno estadounidense, la cual, consistía en plantar pornografía infantil de forma remota en los dispositivos de los objetivos encargados a *Hacking Team*, una empresa italiana especializada en software de vigilancia. Según los datos publicados en forma de filtración en la revista *Wired*, el Buró habría pagado a la empresa italiana cerca de $800,000 en concepto de espionaje.[19] Aunque estas

16 Redacción, "Qué es WikiLeaks, la web de filtraciones con que Assange reveló los secretos de EE.UU.", *BBC News Mundo,* 11 de abril de 2019, https://www.bbc.com/mundo/noticias-internacional-47901012.

17 *National Security Agency.*

18 Amnistía Internacional España, "Infórmate sobre vigilancia masiva", *Amnistía Internacional,* accedido 12 de marzo de 2021, https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/.

19 Rosemary W. Pennington, "Leak: FBI Is Major Customer of "Hacking Team" Which Produces Malware That Can Remotely Plant Child Porn", *National Vanguard*, (2015). https://nationalvanguard.org/2015/07/leak-fbi-is-major-customer-of-hacking-team-which-produces-malware-that-can-remotely-plant-child-porn/.

cifras podrían parecer escandalosas en realidad es solo "la punta del iceberg", al parecer, la empresa habría filtrado los nombres de otros gobiernos que pagan por sus servicios de vigilancia haciendo que la desconfianza sea creciente entre los usuarios del ciberespacio.

En ese orden de ideas, existen acciones estatales cuestionables con el fin de intervenir en la opinión pública en momentos considerados estratégicos como las campañas electorales; que, a través de estrategias engañosas con el fin de extraer material políticamente sensible, desprestigiando al partido/candidato de oposición y así cambiar la intención de voto entre los votantes.[20] Los ciberataques lanzados a partidos políticos e instituciones estatales se caracterizan por utilizar el *phishing* en diferentes variantes de manera que hace más sencilla la extracción de información necesaria, sin generar mayores sospechas; así este tipo de ataque se vuelve más constante hacia los asistentes y mandos medios a través del *spear phishing*, por medio de la suplantación de identidad se extraen datos confidenciales de un tercero.[21]

De acuerdo con la Cámara de Comercio de Valencia, España, basándose en los datos de IHS *Markit*, una empresa especializada en información crítica para inversionistas, en el 2016 el 77 % de los ataques a usuarios fue a través de la implantación de software malicioso o malware; y, en segundo lugar, el *phishing* con un 57 %, este último utilizado como esquema tradicional de estafas y robos financieros en las plataformas bancarias de internet.[22] La situación ha ido en aumento tomando en cuenta los incrementos de usuarios de la red y las capacidades de generar ataques más sofisticados y difíciles de detectar.

20 Baños, «Ciberespionaje, influencia política y desinformación (I)».

21 Karpersky, "¿Qué es el spear phishing?", *latam.kaspersky.com,* 13 de enero de 2021, https://latam.kaspersky.com/resource-center/definitions/spear-phishing.

22 Centro Criptológico Nacional, *Ciberamenzas y Tendencias 2020.*

IV. Ciberseguridad y Ciberdefensa

Anterior a la era digital, las amenazas percibidas por los Estados giraban prácticamente alrededor de la posibilidad de ataque armado, como el inicio de una guerra o invasión hacia algún territorio. Durante la guerra fría, la seguridad se ampliaba a la protección de documentos con respecto a operaciones en el extranjero, desarrollo de armamentos y cualquier otro tipo de estrategia destinada a contener o sacar ventaja al enemigo a través de mensajes cifrados u ocultos; con el tiempo, las amenazas se han ido ampliando y no necesariamente se relacionan con violencia o con uso de armas convencionales. Muchas de las acciones que se encuentran hoy en los nuevos conflictos geopolíticos se traducen en operaciones políticas, económicas, psicológicas y cibernéticas.

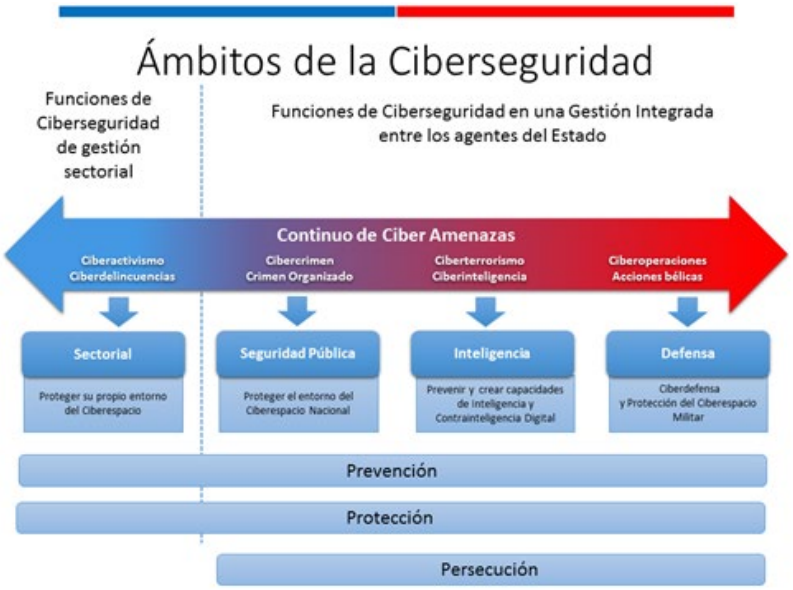
Los factores precedentes pueden poner en peligro la integridad territorial, la seguridad de sus ciudadanos y de las infraestructuras críticas como las fuentes de energía, oleoductos, conexiones telefónicas y cibernéticas, entre otras; creando un complejo entramado de ámbitos comprendidos en la seguridad nacional. Lo anterior, lleva a su vez, hacia una necesaria diferenciación entre la ciberseguridad y la ciberdefensa: cuando se refiere a ciberseguridad se habla del objetivo o finalidad de preservar el ciberespacio libre de amenazas y ataques exitosos, mientras que la ciberdefensa plantea las distintas estrategias para lograr el estado de seguridad.[23]

Así las cosas, la ciberseguridad transitaría desde evitar los daños que un usuario podría experimentar en su dispositivo, debido a descarga de malware, hasta los daños causados por un agente malicioso a infraestructuras industriales. No obstante, estas acciones de protección se transforman en ciberdefensa, cuando ese mismo ataque se dirige a espacios gubernamentales o a infraestructuras críticas de un Estado con el fin de hacerle daño. La ilustración

23 Ramón Casar Corredera, *El Ciberespacio Nuevo Escenario de Confrontación* (Ministerio de Defensa Español: 2012). https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf.

3 habla sobre la ciberseguridad ampliando las competencias y límites entre ciberseguridad y ciberdefensa para tener en cuenta en el análisis de situaciones.

Ilustración 3: Ámbitos de la Ciberseguridad.



Fuente: Ministerio del Interior y Seguridad Pública, República de Chile.

En suma, al ampliar el espectro de ámbitos vulnerables se requiere de un entramado eficiente de respuesta y comunicación entre las instituciones de gobierno y privadas, según el caso; siendo de vital importancia que el Estado genere las capacidades técnicas y financieras tanto para la ciberdefensa como la ciberseguridad de datos y comunicaciones en sus distintos niveles: prevención, protección y persecución.

V. El ciberespionaje y la cibergeopolítica

Siendo que, las actividades de ciberespionaje por parte de los Estados se han exacerbado, no solamente por la situación de las sospechas sobre las operaciones rusas en las elecciones estadounidenses, sino porque más de 100 países tienen la capacidad de emprender operaciones de ciberespionaje a través de sus servicios de inteligencia o encargar este tipo de trabajos a hackers privados por medio de terceros, por medio de contratos en lo que se conoce como *crime as a service*.[24] El ciberespionaje resulta también más barato en costo y menos arriesgado que el espionaje tradicional, por lo que, no es descabellado que este tipo de actividades y ciberataques a estructuras críticas de Estados enemigos sea más frecuente.

La idea central de este tipo de actividades es el dominio del flujo y contenido de la información almacenada en el ciberespacio, por lo que existe en este campo una "carrera" entre los países, sobre todo potencias con capacidad de I+D en éste. El manejo y desarrollo de internet, no fue incluyente, de hecho, la invención misma de estas conexiones por parte de los Estados Unidos, se remonta al tráfico de datos de uso militar con el objetivo de limitar las posibilidades de interceptación por parte de los soviéticos en la guerra fría, uso que después se extendió a los ámbitos académicos y terminó siendo de uso cotidiano.[25] Razones por las que, este conocimiento y desarrollo logrado desde su origen ha permitido al país norteamericano estrategias de ciberespionaje más amplias e innovadoras, inclusive ha concedido violentar *hardware* audiovisual para espiar a potenciales sospechosos y aliados como se ha comentado supra.

El desarrollo de internet es extenso y actualmente diferentes países cuentan con industrias de desarrollo tecnológico importante y más competidores van incursionando al mercado de desarrollo, distribución y procesamiento de

24 Gómez de Ágreda, "Ciberseguridad en ciudades".

25 Gustavo Buzai, "Fronteras en el ciberespacio. El nuevo mapa mundial visto desde Buenos Aires (Argentina)", *Cuadernos de Geografía: Revista Colombiana de Geografía* 23, n.o 2 (2014): 85-92, doi:10.15446/rcdg.v23n2.38088.

información; sobre todo con dispositivos móviles, y actualmente con el manejo de tecnología 5G que permitiría conectividad en robótica avanzada y manejo de *Big Data*, esto involucra mayormente a empresas chinas y estadounidenses entre ellas *Huawei y Google*, respectivamente, que van a la cabeza del desarrollo de una conectividad más amplia y más rápida, lo que a su vez representaría un espacio estratégico de dominio tecnológico y geopolítico.[26]

En décadas anteriores, la innovación y dominio aeroespacial era determinante durante la carrera armamentista en la guerra fría entre Estados Unidos y la URSS, actualmente, esto se traslada al desarrollo y manejo de tecnologías cibernéticas, dando ventaja a un Estado sobre los demás, lo que, al mismo tiempo representa una amenaza en cuanto a la capacidad y oportunidad de ciberespionaje.

En ese sentido puede inferirse una auténtica guerra entre Estados de las principales empresas fabricantes de dispositivos 5G, al grado que el gobierno del ex presidente Trump prohibió a empresas tecnológicas estadounidenses vender partes a empresas chinas, en específico *Huawei y ZTE*, al igual que la Comisión de Inteligencia del Congreso de los Estados Unidos consideró que tales empresas podrían ser una amenaza a la seguridad nacional y ha sugerido crear una red de última generación propia cumpliendo con estándares de ciberseguridad necesarios para salvaguardar al país de posibles filtraciones de datos y revelación de documentos sensibles.[27] Por su parte, el Congreso no avaló la sugerencia de la Comisión por resultar onerosa y se decantó porque empresas privadas lleven a cabo esta actualización.

Las políticas restrictivas de los Estados Unidos sobre Google, el principal proveedor de servicios cibernéticos a nivel mundial,[28] ha afectado

26 Vicente Moret, *El despliegue de las redes 5G, o la geopolítica digital - Elcano,* 12 de marzo de 2019, http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari31-2019-moret-despliegue-de-redes-5g-geopolitica-digital.

27 *Ibíd.*

28 Lucy Hooker, *¿Cómo se convirtió Google en la empresa más valiosa del mundo?,* BBC News, 2 de febrero de 2016. https://www.bbc.com/mundo/noticias/2016/02/160202_google_mas_valiosa_

la relación de la empresa con *Huawei* y viceversa; esto, porque los teléfonos *Huawei* lanzados al mercado desde 2019 no cuentan con los servicios de Google que se incorporan por defecto en los entornos Android. Sin embargo, China ha logrado presencia de estos programas a través de acceso abierto aunque Google teme no sea lo más seguro con respecto a la protección de *malware*. Al igual que Microsoft, la empresa norteamericana solicitó a inicios del año 2020 operar bajo una licencia del gobierno y colaborar con *Huawei*.[29]

La petición no ha sido concedida por el gobierno durante la presidencia de Trump y tampoco en la actual administración del presidente Biden ya que no levantará el veto comercial y de colaboración que mantiene Estados Unidos con la compañía tecnológica por encontrarse dentro de la lista negra de empresas consideradas de riesgo para la seguridad nacional estadounidense; tal como lo expresó Gina Raimondo, Secretaria de Comercio en febrero del presente año.[30] De seguir la situación, lo más probable es que *Huawei* genere sus propias aplicaciones en los espacios que no tienen soporte de Google como: Play Store, navegación por mapa y protección de datos, cuestión que podría tornarse inclusive más ventajosa para la empresa, tornándose más competitivo en mercados extranjeros como Europa.

En esa búsqueda de opciones para superar la situación, *Huawei* ha decidido impulsar servicios más allá del *hardware* para no depender de software estadounidense como *App Gallery*, *Huawei Mobile Services* y el sistema *HarmonyOS* que se plantea de acceso libre.[31] Esto también aseguraría una alternativa para

men#:~:text=Esto%20la%20convierte%20en%20la,Larry%20Page%20y%20Sergey%20Brin. Google está valorada en $520,000 millones, siendo la empresa más valiosa del mundo.

29 Enrique Pérez, "Google quiere volver a colaborar con Huawei y solicita a los EE. UU una licencia para regresar a los móviles de la marca china", *Xataka,* 26 de febrero de 2020, https://www.xataka.com/empresas-y-economia/google-quiere-volver-a-colaborar-huawei-solicita-a-ee-uu-licencia-su-software-regrese-a-moviles-marca-china.

30 Martin, "Biden Commerce Pick Sees 'No Reason' to Lift Huawei Curbs" *Bloomberg.Com,* 4 de febrero de 2021, https://www.bloomberg.com/news/articles/2021-02-04/biden-commerce-pick-sees-no-reason-to-pull-huawei-from-blacklist.

31 Nicolás Rivera, "¿Se convertirá Huawei en Google para proteger a China de EE.UU.?", *Hipertextual*, 25 de enero de 2021, https://hipertextual.com/2021/01/y-si-futuro-huawei-es-convertirse-google-china-y-proteger-sus-propios-rivales-estados-unidos.

otras compañías de tecnología chinas como *Xiaomi* que está en la lista negra de los Estados Unidos pero que aún no ha sido vetada.

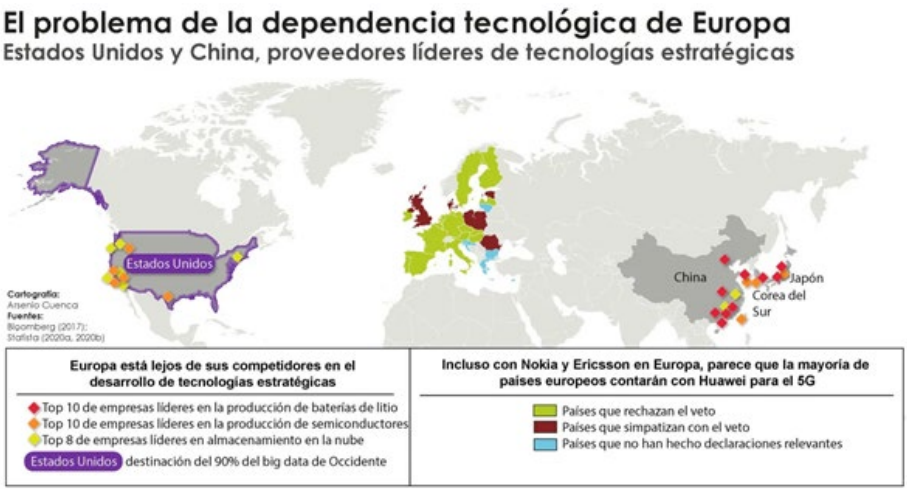
La presión que se está ejerciendo por parte del gobierno de los Estados Unidos y la guerra comercial en la que se ha visto inmersa con China, parte de un contexto en el que se involucra, desde propiedad intelectual, hasta el dominio de la tecnología 5G y su implementación a través de empresas nacionales. Así, la carrera por lograr dominio tecnológico por parte de las potencias y la utilización del ciberespionaje para sacar ventaja y mejor posicionamiento frente a sus contendientes implica desarrollo de mayores conectividades y con mayor rapidez; sin embargo, también significa amenazas a la ciberseguridad, violación a la privacidad y vulneración de datos personales, *hackeos* e intervenciones a burócratas claves que representen un eslabón importante en la cadena de mando que se traduce en conocimiento e información.

¿Qué están haciendo otros actores ante esta situación?

Europa por su parte posee empresas tecnológicas competitivas, pero que no son suficientes para enfrentar la tensión entre Estados Unidos y China en este espectro. La situación para los europeos se torna compleja partiendo de las represalias que podrían recibir al decidirse por uno de estos dos competidores; en términos generales, saben que China ha avanzado mucho en el manejo de redes más amplias como la tecnología 5G que incluye la gestión del internet de las cosas y otros progresos cibernéticos como la inteligencia artificial. Por una parte, Estados Unidos, es un aliado indispensable para Europa en el marco de la OTAN y por otro, aunque China es un socio comercial fuerte, existen roces de tipo económico, político e ideológico. A pesar de ello, varios de los países miembros se han decantado por contratar a *Huawei* para la distribución de redes 5G aun con los casos de espionaje industrial de la empresa china a la francesa Alcatel, lo que llevó a ser absorbido por Nokia en 2016.[32]

32 Arsenio Cuenca, "El problema de Europa: la dependencia tecnológica de Estados Unidos y China", *El Orden Mundial - EOM*, (2020), https://elordenmundial.com/dependencia-tecnologica-union-europea/.

Ilustración 4: Dependencia tecnológica europea.



Fuente: El Orden Mundial, 2020.

Tal como se aprecia en la ilustración 4, la dependencia tecnológica de Europa frente a estos dos rivales les ha hecho quedar desprotegida ante una guerra cibergeopolítica en desarrollo con millones de usuarios de dispositivos chinos con almacenamiento y gestión estadounidenses; así muchos podrían quedar vulnerables a ataques cibernéticos en la medida que se vean obligados a utilizar software de acceso libre, pero sin la protección constante que ofrece Google en sus plataformas.

En ese mismo orden de ideas, la UE se decanta por crear sus propios protocolos de defensa que complementan a los ya existentes por cada Estado miembro; sin embargo, el éxito de la misma residirá en la disposición a mantenerse como un bloque de contención y a la vanguardia en la investigación de estructuras criminales y operaciones de ciberespionaje por Estados adversarios que deseen sacar ventaja aplicando este tipo de técnicas en la sustracción de información con sanciones, denuncias diplomáticas y cualquier otro recurso que pueda implementarse a partir de directivas como NIS,[33]

33 Normativa europea de ciberseguridad.

establecidas directamente a través de la Política Común de Seguridad Europea (PCSE), con regulaciones concretas en cuanto a Operadores de Servicios Esenciales (OSE) y Proveedores de Servicios Digitales (PSD).

Por lo pronto, en cuanto al juego cibergeopolítico entre China y EEUU, la UE como bloque jugará un papel importante en el balance de poder de ambos Estados, así definir en última instancia el margen de influencia de estas potencias tecnológicas al menos en parte de los mercados occidentales, aunque por lo que la historia y la coyuntura ha enseñado es probable que se decante por el apoyo a Estados Unidos en mayor medida que a China. Esto, mientras no se establezcan las bases para dar un impulso a las empresas europeas como Ericksson y Nokia; los que, aunque se colocan en el tercer puesto para el soporte de redes 4G,[34] no representan competencia para la tecnología oriental y que, con la expansión del mercado tecnológico a ritmo acelerado quede con mayores problemas para ofrecer redes de gestión de datos.

Conclusión

La dependencia generalizada del uso de internet y los dispositivos con conexión a ésta han generado un nuevo espacio de confrontación entre los Estados. Al igual que en los ámbitos geopolíticos tradicionales, los posicionamientos ventajosos con respecto a los demás se logran en la medida que se sostiene un mayor dominio del espectro a través de diferentes estrategias, en este caso, la inversión y desarrollo de dispositivos, redes y sistemas informáticos que permitirían conectividad constante y rápida en la vida cotidiana de los gobiernos y poblaciones; generando a su vez acceso a datos e información sensible que puede utilizarse de distintas maneras y con objetivos diferentes, desde la venta de datos sobre el comportamiento y toma de decisiones de los usuarios sin el consentimiento de los mismos, hasta actividades ilícitas con objetivos económicos y/o políticos.

34 Cuenca, «El problema de Europa».

La carrera entre los Estados Unidos y China por generar mayores ventajas cibergeopolíticas ha llevado a tensiones fuertes entre ambos con consecuencias globales, en la medida en que la falta de colaboración entre empresas por sospechas de ciberespionaje deja a millones de usuarios vulnerables en el uso de aplicaciones sin seguridad en el manejo de datos a corto plazo. El desarrollo de dispositivos cada vez más veloces, complejos y accesibles económicamente enfrenta a varias empresas tecnológicas en el mercado; pero que, podrían quedar en mayor desventaja si *Huawei* sigue produciendo dispositivos accesibles y de calidad, aunque no tengan el soporte de Google, a diferencia de otras marcas de países competitivos en términos tecnológicos, pero con precios más altos.

Sobre esa línea, es indispensable mencionar que la ciberseguridad y ciberdefensa de los Estados tendrá éxito en la medida que estos inviertan tiempo y esfuerzo en la contención de ataques cada vez más complejos y frecuentes. Estas acciones ilícitas no serán en lo próximo la excepción para lo que los Estados deben estar preparados tanto ante otros países como células delincuenciales y terroristas. Sin embargo esta capacidad de defensa y contención de amenazas depende a su vez de la fortaleza y tecnificación de las instituciones encargadas; siendo así, que serán entonces los países desarrollados quienes tengan mejores oportunidades para enfrentar las amenazas, mientras que los países en desarrollo tendrán más dificultades para hacerlo partiendo de sus condiciones menos favorables en cuanto al acceso y desarrollo de tecnologías de información y que, en caso de lograrse, son adquiridas por empresas extranjeras de gran capital, acarreando también en muchas ocasiones, fuga importante de cerebros.

Bibliografía

» Ágreda, Ángel Gómez de. "CIBERESPACIO: de ratones y hombres", n.o 51 (2015): 1-9. http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO51-2015_Ciberespacio_AGdeAgreda.pdf

» Ágreda, Ángel Gómez de. *Cuaderno de Estrategia 206: Instituto Español de Estudios Estratégicos* (2020): 175-211, http://www.ieee.es/Galerias/fichero/cuadernos/CE_206_LasCiudades_AgentesCriticosParaUnaTransformacionSostenibleDelMundo.pdf.

» Baños, Pedro. "Ciberespionaje, influencia política y desinformación (I)". *El Orden Mundial - EOM*, (2017). https://elordenmundial.com/ciberespionaje-influencia-politica-y-desinformacion-i/.

» Barrios, Miguel. "La Geopolítica Digital: un campo de lucha por la supremacía mundial". *América Latina en movimiento*, 30 de septiembre de 2019. https://www.alainet.org/es/articulo/202386.

» Barrios, Miguel, y Norberto Emmerit. "Geopolítica de la seguridad: las disputas geopolíticas del ciberespacio (III)". *América Latina en movimiento*, (2017). https://www.alainet.org/es/articulo/184284.

» Buzai, Gustavo. "Fronteras en el ciberespacio. El nuevo mapa mundial visto desde Buenos Aires (Argentina)". *Cuadernos de Geografía: Revista Colombiana de Geografía* 23, n.o 2 (2014): 85-92. doi:10.15446/rcdg.v23n2.38088.

» Casar Corredera, Ramón. *El Ciberespacio Nuevo Escenario de Confrontación.* Ministerio de Defensa Español, 2012. https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf.

» Centro Criptológico Nacional. *Ciberamenazas y tendencia 2018.* Ministerio de Defensa Español, 2018. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html.

» Centro Criptológico Nacional. *Ciberamenzas y Tendencias 2020.* Ministerio de Defensa Español, septiembre de 2020. https://www.ospi.es/export/sites/ospi/documents/documentos/Informe-Ciberamenazas-Tendencias_2020.pdf.

» Cuenca, Arsenio. "El problema de Europa: la dependencia tecnológica de Estados Unidos y China". *El Orden Mundial* (2020). https://elordenmundial.com/dependencia-tecnologica-union-europea/.

» España, Amnistía Internacional. "Infórmate sobre vigilancia masiva". *Amnistía Internacional.* Accedido 12 de marzo de 2021. https://www.es.amnesty.org/en-que-

» Karpersky. "¿Qué es el spear phishing?" *latam.kaspersky.com*, 13 de enero de 2021. https://latam.kaspersky.com/resource-center/definitions/spear-phishing.

» Martin. "Biden Commerce Pick Sees 'No Reason' to Lift Huawei Curbs". *Bloomberg.Com*, 4 de febrero de 2021. https://www.bloomberg.com/news/articles/2021-02-04/biden-commerce-pick-sees-no-reason-to-pull-huawei-from-blacklist.

» Moret, Vicente. *El despliegue de las redes 5G, o la geopolítica digital - Elcano*, 12 (2019). http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari31-2019-moret-despliegue-de-redes-5g-geopolitica-digital.

» Pennington, Rosemary W. "Leak: FBI Is Major Customer of "Hacking Team" Which Produces Malware That Can Remotely Plant Child Porn". *National Vanguard*, 28 (2015). https://nationalvanguard.org/2015/07/leak-fbi-is-major-customer-of-hacking-team-which-produces-malware-that-can-remotely-plant-child-porn/.

» Pérez, Enrique. "Google quiere volver a colaborar con Huawei y solicita a los EE. UU una licencia para regresar a los móviles de la marca china". *Xataka*, (2020). https://www.xataka.com/empresas-y-economia/google-quiere-volver-a-colaborar-huawei-solicita-a-ee-uu-licencia-su-software-regrese-a-moviles-marca-china.

» Redacción. "La investigación de la injerencia rusa en las elecciones de EE.UU. en las que venció Trump en 300 palabras". *BBC News Mundo.* Accedido 11 de marzo de 2021. https://www.bbc.com/mundo/noticias-internacional-46400948.

» Redacción. "Qué es WikiLeaks, la web de filtraciones con que Assange reveló los secretos de EE. UU". *BBC News Mundo*, 11 de abril de 2019. https://www.bbc.com/mundo/noticias-internacional-47901012.

» Rivera, Nicolás. "¿Se convertirá Huawei en Google para proteger a China de EE.UU.?" *Hipertextual*, 25 de enero de 2021. https://hipertextual.com/2021/01/y-si-futuro-huawei-es-convertirse-google-china-y-proteger-sus-propios-rivales-estados-unidos.

» TIC Negocios. "Qué es un ciberataque y para qué sirve | TicNegocios.es". *Tecnología para los negocios.* Accedido 12 de marzo de 2021. https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/.

» Veiga, Francisco. *El Desequilibrio como Orden.* Segunda edición. Madrid: Allianza, 2015.