Capítulo undécimo

Ciberguerra y cibercrimen global, cuando lo virtual transciende a lo real

Javier Fernández Aparicio

Resumen

Los ciberataques ponen en riesgo vidas humanas. El ciberespacio se fue consolidando durante los últimos veinte años como el quinto área del ámbito bélico, un terreno propicio para actos de espionaje, sabotaje y desestabilización entre Estados contendientes. Destacan cuatro actores principales: Estados Unidos, China, Rusia y la Unión Europa, ciberatacantes sofisticados o ciberatacados donde la resiliencia es clave para prevenir las amenazas. A nivel global no es fácil determinar si muchos ciberataques son motivados por una ciberguerra no declarada o son acciones del cibercrimen. La ciberdelincuencia, donde en algunos casos hay sospechas de conexiones con los gobiernos, es un grave problema en un mundo hiperconectado y pone en riesgo la seguridad de los países, corporaciones y ciudadanos, lo que plantea una futura regulación internacional que marque líneas rojas ahora mismo inexistentes.

Palabras clave

Ciberseguridad, ciberdefensa, ciberespacio, cibercrimen, ciberespacio, Estados Unidos, China, Rusia, Unión Europea.

Cyberwar and global cybercrime, when the virtual transcends the real

Abstract

Cyber attacks put human lives at risk. Cyberspace has been consolidating for the last twenty years as the fifth area of the war environment, a propitious terrain for acts of espionage, sabotage and destabilization between contending States. Four main actors stand out: the United States, China, Russia and the European Union, sophisticated cyberattackers or cyberattacked where resilience is key to preventing threats. At a global level, it is not easy to determine if many cyberattacks are motivated by an undeclared cyberwar or are actions of cybercrime. Cybercrime, where in some cases there are suspicions of connections with governments, is a serious problem in a hyperconnected world and puts the security of countries, corporations and citizens at risk, which raises a future international regulation that marks red lines right now nonexistent.

Keywords

Cybersecurity, Cyberdefence, Cyberspace, Cybercrime, Cyberspace, United States, China, Russia, European Union.

1. La ciberguerra nació, creció y se expandió

En septiembre de 2020 las autoridades alemanas calificaron la muerte de una paciente en el hospital de Düsseldorf como la primera víctima real de un ciberataque. Aunque el estado de la paciente era crítico cuando llegó al hospital, no pudo ser intervenida debido al colapso del sistema informático del centro sanitario tras un ataque mediante un virus informático tipo *ransomware*, el cifrado de datos del sistema por parte de los ciberpiratas. Durante horas estuvo bloqueado el sistema de gestión de pacientes de urgencias del hospital e incluso la policía alemana contactó con los ciberatacantes, de origen ruso para restablecer el control del centro[1]. No era la última vez que se producía un ciberataque agresivo contra infraestructuras sanitarias, poniendo en riesgo vidas humanas. En mayo de 2021 todo el servicio de salud pública en Irlanda cerró parte de sus sistemas a raíz de otro importante ataque y en octubre un hospital de Alabama no se apercibió del apagado de un lector de frecuencia cardíaca debido a otro ciberataque, muriendo un recién nacido[2].

El 12 de octubre de 2020, la electricidad se cortó repentinamente en Bombay, la ciudad más grande de la India y su centro financiero. Las autoridades se enfrentaron a un caos de doce horas que sumergió a la población en la incertidumbre sin transporte, telefonía y el apagón de medios para los enfermos de COVID, que por entonces saturaban los hospitales indios con altos niveles de mortalidad. La investigación reveló que corte fue originado por un ciberataque mediante un virus malicioso que infectó los servidores de las compañías eléctricas estatales, apuntando las sospechas hacia piratas informáticos chinos[3]. Todo ello se daba en un momento de tensión entre ambos países y demostró la capacidad china para presionar a su vecino desde el ámbito cibernético, con potenciales víctimas reales.

[1] Pastor, J. (2020). Un ataque ransomware a un hospital en Alemania pudo ser el causante de la muerte de una paciente*.* [Consulta: 25/9/2022]. Disponible en: https://www.xataka.com/seguridad/ataque-ransomware-a-hospital-alemania-pudo-ser-causante-muerte-paciente

[2] *Independent en Español*. (2021). Ciberataque en hospital causó la muerte de bebé por a pagar la pantalla de frecuencia cardíaca, según demanda. [Consulta: 29/9/2022]. Disponible en: Ciberataque en hospital causó la muerte de bebé por apagar la pantalla de frecuencia cardíaca, según demanda (msn.com)

[3] Bay, A. (2021). Apagón eléctrico de Bombay: ¿Guerra china en la zona gris? [Consulta: 25/9/2022]. Disponible en: https://es.theepochtimes.com/apagon-electrico-de-bombay-guerra-china-en-la-zona-gris_803620.html

Como vemos, los ciberataques pueden causar muertes, ya sean como efectos del cibercrimen, un ciberdelincuente o grupo organizado de ellos que realiza sus actos en principio en busca de un beneficio económico, y de la ciberguerra, cuando esos ciberataques entre actores estatales por sí o mediante terceros, son utilizados como arma en esa zona gris y poca definida de los conflictos.

El cibercrimen y la ciberguerra pudieran parecer fenómenos diferentes, pero están relacionados, pues ambos inducen al caos y la parálisis parcial o total de sistemas informáticos de un país, afectando a toda la sociedad y a organismos públicos o privados indistintamente. Un peligro que ya viene de lejos en este mundo cada vez más interconectado.

Introducir la ciberseguridad en una obra como esta dedicada a conflictos geopolíticos y en terreno físico, aunque el ciberespacio también esté presente, puede parecer extraño. No hay ciberguerras declaradas como tales y, sin embargo, nos encontramos en todo el planeta multitud de actores y ataques en el ámbito cibernético de graves consecuencias. La percepción de la ciberguerra varía. En tiempos de paz, aparentemente sus efectos para la población se presentan más alarmantes, mientras que, en guerras abiertas, donde la destrucción mediante armas convencionales copa los medios y, por desgracia, las bajas en vidas humanas, lo cibernético queda relegado a un segundo plano (Calvo Albero, 2022: 73).

Ningún ámbito como la ciberseguridad tiene unas connotaciones geopolíticas tan amplias en esta vida hiperconectada y dependiente de la red. Está en riesgo la existencia de los ciudadanos a través de las cadenas de suministros, cualquier red energética o el sistema financiero, por citar tres de los principales impactos en la ciudadanía en caso de ciberataque. También es relevante su poder expansivo en las campañas de desinformación, así como en el desarrollo y dependencia tecnológica en el ámbito militar[4].

Estamos en una época donde los Estados, en especial aquellos que influyen en el orden mundial, se dotan de medios, en el ámbito civil y el militar, para luchar o defenderse en el ciberespacio y combatir el cibercrimen. En definitiva, los Estados luchan por

[4] Oier, E. & Corchado, J. M. (2022). *Inteligencia Artificial: aplicaciones a la Defensa.* Documento de investigación IEEE, 01/2022, p. 25. [Consulta: 29/9/2022]. Disponible en: https://www.ieee.es/contenido/noticias/2022/04/DIEEEINV01_2022_EDUOLI_Inteligencia.html

proteger la integridad de sus ciudadanos en un espacio virtual y vulnerable, pero cuyos efectos tienen consecuencias reales[5].

Por primera vez desde que el *Panorama geopolítico de conflictos* nació en 2011 se aborda la ciberguerra como un capítulo propio y no solo como un epígrafe dentro de otro conflicto, ya que la ciberseguridad siempre ha constituido un tema capital en los numerosos estudios y documentos publicados desde hace tantos años por el Instituto Español de Estudios Estratégicos[6]. En una obra como esta nos interesa obtener una perspectiva del pasado y una prospectiva del futuro del ciberespacio como campo de batalla transversal, puesto que atañe a múltiples ámbitos públicos y privados, desde los más cotidianos a los tocantes a la seguridad crítica. En un mundo hiperconectado, la ciberguerra es el quinto ámbito de confrontación dentro de los grandes conflictos a escala global en curso y sin duda por venir (IEEE, 2021).

2. Antecedentes de los ciberconflictos: historia de dos décadas

Durante la noche del 5 al 6 de septiembre de 2007 la Fuerza Área de Israel bombardeó un reactor nuclear en Siria cuya construcción era presuntamente secreta. Once años después se supo que era la operación *Orchard* y el sistema de defensa antiaérea sirio, proporcionado por Rusia, no funcionó debido a un ciberataque previo que anuló su capacidad de respuesta[7]. Para Richard Clarke y Robert Knake fue el acto primigenio en lo que se daría en llamar la ciberguerra, concebida como «aquellas acciones realizadas por un Estado nación con el fin de penetrar los ordenadores o las

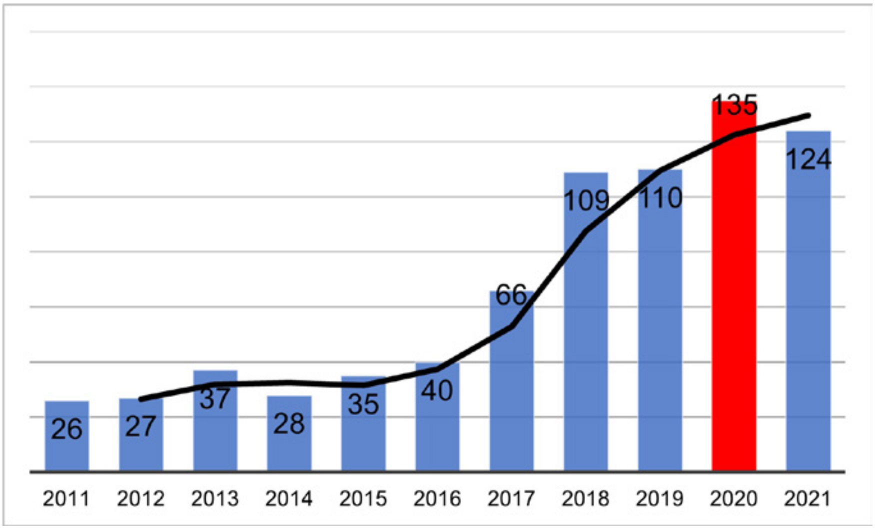
[5] Candau, J. (2021). *Ciberseguridad. Evolución y tendencias*. Documento Marco IEEE, 11/2021, p. 36. [Consulta: 29/9/2022]. Disponible en: https://www.ieee.es/en/contenido/noticias/2021/09/DIEEEM11_2021_JAVCAND_Ciberseguridad.html

[6] Del 2011 es un monográfico dedicado a la ciberseguridad, que no ha perdido vigencia: *Ciberseguridad: retos y amenazas a la seguridad nacional en el ciberespacio.* (2011). Madrid, Instituto de Estudios Estratégicos, Instituto Universitario General Gutiérrez Mellado. Ministerio de Defensa. 369 pp. Cuadernos de estrategia / Instituto Español de Estudios Estratégicos, 149. ISBN 978-84-9781-622-9. Más modernamente, *Ciberseguridad: la cooperación público-privada.* (2017). Madrid, Instituto de Estudios Estratégicos, Departamento de Seguridad Nacional, Ministerio de Defensa. 366 pp. Cuadernos de estrategia / Instituto Español de Estudios Estratégicos, 185. ISBN 978-84-9091-245-4. Gran parte de los documentos elaborados por el Instituto tocantes a la ciberseguridad en IEEE - Ciberseguridad.

[7] *BBC Mundo*. (2018). *Por qué Israel reconoce por primera vez que destruyó un reactor nuclear en Siria hace 11 años.* [Consulta: 28/9/2022]. Disponible en: https://www.bbc.com/mundo/noticias-internacional-43486931

redes de otra nación y el propósito de causar daños o perturbar su adecuado funcionamiento» (Clarke & Knake, 2011).

Los Estados fueron progresivamente conscientes de las graves consecuencias para sus infraestructuras críticas, no importando si estas pertenecían al ámbito civil o militar, a lo público o a lo privado, formando a personal y creando organismos capaces de garantizar la ciberseguridad, pues al riesgo de los actores estatales se fue sumando la ciberdelincuencia e incluso una forma híbrida, a medio camino entre ciberguerra y cibercrimen, ya que las fronteras y motivaciones de los atacantes no siempre son claras.



Evolución del número de ataques cibernéticos a nivel global a agencias gubernamentales, empresas de defensa y alta tecnología, o delitos económicos con pérdidas de más de un millón de dólares. Fuente: elaboración propia según datos del Center for Strategic & International Studies. Disponible en: 220906_Significant_Cyber_Incidents.pdf

Como antesala de los principales conflictos en el ciberespacio en la actualidad conviene hacer un recorrido histórico de los principales eventos ocurridos en el periodo anterior de 2008-2020. Muchas ciberguerras relevantes en la actualidad ya estaban en ciernes entonces, así como también las prácticas cibercriminales que no han hecho sino sofisticarse y expandirse en el ciberespacio. En el recorrido seguiremos la división que nos ofrece en una obra básica sobre el tema Ben Buchanan, que centra su análisis en los efectos de los ciberataques en la geopolítica. Para este experto la lucha entre Estados en el ciberespacio no es otra cosa que la continuidad, más avanzada tecnológicamente, de actos hostiles presentes en las relaciones internacionales desde al menos los tiempos de la Guerra Fría. Actos como el espionaje, el sabotaje y la desestabilización del enemigo (Buchanan, 2020).

2.1. El ciberespionaje

Nos referimos a los casos donde al menos dos Estados han estado implicados en el uso del ciberespacio para espiar o robar información crítica uno del otro. Hay ejemplos de ciberespionaje directamente estatal o por parte de un grupo de ciberdelincuentes al servicio encubierto de un Estado. Desde 2008 los principales actores globales implicados son China respecto a Estados Unidos y en menor medida el Reino Unido, así como Rusia y la Unión Europea, con especial interés en Alemania y casi siempre en materias económica e industrial, aunque también hacia organismos y sistemas de seguridad.

Estados Unidos fue objeto de ciberespionaje por parte de Rusia y China. El primer caso fue el virus de tipo gusano *Agent.btz*, capaz de replicarse a sí mismo, que en 2008 consiguió extraer información de varios equipos militares de Estados Unidos. El origen apuntaba a Rusia. La crisis fue de tal magnitud que condujo a la creación del Mando Cibernético de Estados Unidos en junio de 2009 (Quintana, 2016: 19-37). Efectivamente, como también demostraron los ciberataques a Estonia en 2007 —motivo de la creación de un centro de ciberseguridad de la OTAN— y Georgia en 2008, Rusia tenía la capacidad de atacar en el ciberespacio, aunque para ello más que una estructura organizada en el complejo militar, existían grupos de piratas informáticos organizados y con conexiones con las autoridades rusas (Clarke & Knake, 2011: 95-96).

Tras otras intrusiones, como en 2014 a los sistemas de la Casa Blanca y el Departamento de Estado y un año después a más de cien entidades bancarias, en 2016 por primera vez Estados Unidos sancionaba a Rusia debido a los ciberataques en la campaña electoral que llevaría a la victoria de Donald Trump[8].

Respecto a China, recordemos que en 1999 apareció publicado un libro sobre la doctrina militar de guerra «más allá de los límites»,

[8] Sanger, D. E. (2016). Obama sanciona a Rusia en respuesta a los ciberataques durante las elecciones. [Consulta: 26/9/2022]. Disponible en: https://www.nytimes.com/es/2016/12/29/espanol/obama-impone-sanciones-contra-rusia-en-respuesta-al-hackeo-electoral.html

una vuelta de tuerca al concepto de guerra híbrida. Se abogaba por que, en la lucha contra un enemigo muy superior en medios militares, como entonces era Estados Unidos, habría que utilizar armas no convencionales como el ciberespacio. China creó grupos de piratas informáticos civiles y unidades militares especializadas en ciberguerra, como la unidad 61.398 del Ejército de Liberación Popular, llevando a cabo campañas de ciberespionaje a instituciones y corporaciones estadounidenses, aunque también a japonesas y europeas (Clarke & Knake, 2011: 53-95). En 2014 desde Estados Unidos se acusó directamente a China de ciberespiar el sistema de la Oficina de Administración de Personal y empresas del sector energético, robando datos sensibles[9].

Para comprender mejor esta rivalidad en el ciberespacio entre Estados Unidos, de un lado, frente a Rusia y China de otro, algunas fuentes creen que desde 2015 rusos y chinos poseen un compromiso tácito de no agresión mutua, por lo que se habrían centrado aún más en su ciberactividad frente a Estados Unidos y otros países aliados como Taiwán, Corea del Sur o la Unión Europea[10].

2.2. Los cibersabotajes

Los sabotajes a infraestructuras mediante ciberataques representan el mayor riesgo para las vidas humanas, pues sus objetivos principales son sectores críticos como la seguridad, el comercio, los sistemas financieros, los transportes de mercancías o personas y las redes energéticas. Algunas acciones de ciberdelincuentes provocaron serias consecuencias. En Polonia se recuerda la serie de descarrilamientos de tranvías ocurridos en la ciudad de Lodz, en enero de 2008, cuando un joven consiguió piratear el sistema informático de la seguridad ferroviaria municipal, manejando las intersecciones de las vías a su antojo (Suárez Sánchez-Ochoa, 2015: 139-140). Estos cibersabotajes en medios y vías de comunicación son comunes y peligrosos. El transporte marítimo es otro ejemplo, pues es un sector altamente informatizado y afectado por los ataques de grupos ciberdelincuentes desde hace décadas. La manipulación de los sistemas de posicionamiento global,

[9] Bassets, M. (2014). Washington acusa a cinco militares chinos de ciberespionaje industrial. [Consulta: 27/9/2022]. Disponible en: https://elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html

[10] Razumovskaya, O. (2015). Russia and China Pledge Not to Hack Each Other. [Consulta: 27/9/2022]. Disponible en: https://www.wsj.com/articles/BL-DGB-41673

los transpondedores e incluso la toma del control remoto de los buques, suponen graves riesgos de accidentes y pérdidas multimillonarias para las navieras y empresas implicadas (Crawford, 2022).

El primer caso de cibersabotaje de un Estado a otro fue el que se produjo en mayo de 2007 en Estonia, uno de los países más conectados del mundo y que por ello era vulnerable. Tras una agria polémica debido a la retirada por parte de las autoridades estonias de un monumento en homenaje al soldado soviético en la II Guerra Mundial, un ataque de denegación de servicio (conocido como DDoS, en sus siglas en inglés) originado desde Rusia colapsó los servicios públicos, la red telefónica y el sistema financiero estonio. Expertos de la OTAN viajaron de urgencia a Estonia. También en la intervención rusa en Georgia de 2008 previamente se lanzaron una serie de ciberataques, antesala de la irrupción de las tropas convencionales (Clarke & Knake, 2011: 31-39).

El caso más resonado de cibersabotaje entre Estados fue el ocurrido en enero de 2010. En plena visita de los inspectores de la Agencia Internacional de Energía Atómica a la planta nuclear iraní de Natanz, las centrifugadoras para enriquecer uranio empezaron a fallar. Un sofisticado virus informático de tipo gusano, capaz de replicarse a sí mismo y conocido como *Stuxnet*, tomó el control dándoles ciertas instrucciones hasta llegar a averiarse por completo[11]. La investigación posterior demostró que este tipo de virus había llevado meses de programación y aunque se desconoce con certeza la autoría del ciberataque, diversos medios y empresas electrónicas apuntaron a Estados Unidos e Israel, que conjuntamente habrían elaborado esta potente arma de ciberguerra contra el plan nuclear iraní (Quintana, 2016: 119-162).

Si hablamos de las consecuencias económicas del cibersabotaje, con el pago de un rescate multimillonario a los ciberpiratas, nos tenemos que remontar a 2012 y el caso del virus *Shamoon*, que atacó el sistema informático de Aramco, la principal industria petrolera saudí. No se conoce quiénes estaban detrás o si el ataque provenía de algún Estado, pero consiguió detener temporalmente la producción de petróleo (Pagliery, 2015).

[11] *BBC Mundo* (2015). El virus que tomó control de mil máquinas y les ordenó autodestruirse. [Consulta: 27/9/2022]. Disponible en: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

2.3. Desestabilización desde el ciberespacio

La desestabilización a través de la red consiste en utilizar esta y sus aplicaciones como medios de transmitir determinada (des)información por parte de un Estado o grupo ciberdelincuente e influir en los usuarios receptores de otro país. Desde 2010 al menos la desestabilización a través de la red ha tomado diferentes objetivos, según el impacto del medio elegido. En cualquier caso, el efecto deseado no es tanto el mismo mensaje, sino la sensación de vulnerabilidad que se transmite al país atacado al haberse conseguido romper las barreras de ciberseguridad (Quintana, 2016: 202-225).

En enero de 2010 un grupo autodenominado el *ciberejército iraní* atacó el motor de búsqueda chino Baidu. Cuando los usuarios abrían esta página web eran redirigidos a otra con mensajes políticos iraníes[12]. Entonces las campañas de desestabilización en el ciberespacio fijaban sus objetivos en aquellas páginas en la red con mayor tráfico de usuarios, en primer lugar, estos motores de búsquedas, pues la estadounidense Google sufrió un ciberataque ese mismo año, en este caso desde China[13].

Posteriormente, el interés de estos ciberpiratas se centraría en los medios digitales de comunicación, con algunos ciberataques como el denunciado por la cadena británica BBC en 2012, cuando se interrumpieron las emisiones y, como en el caso de la china Baidu, se mostraron mensajes políticos iraníes. Un año después fueron los periódicos estadounidenses *The Wall Street, New York Times* y *Washington Post* los que denunciaron ciberataques continuados, en estas ocasiones apuntando a la autoría china, mientras ese mismo 2013 las cadenas de televisión de Corea del Sur denunciaron un ataque cibernético que consiguió interrumpir las emisiones con eslóganes políticos norcoreanos.

Por su gravedad, de más transcendencia fueron los ciberataques de febrero de 2015, un mes después de los atentados de *Charlie Hebdo*, por parte de un grupo de ciberpiratas al servicio del Estado Islámico, que consiguieron difundir mensajes yihadistas durante la emisión y en las redes sociales de la televisión francesa TV5 (Suárez Sánchez-Ochoa, 2015: 149-150).

---

[12] Branigan, T. (2010). 'Iranian' hackers paralyse Chinese search engine Baidu. [Consulta: 26/9/2022]. Disponible en: https://www.theguardian.com/technology/2010/jan/12/iranian-hackers-chinese-search-engine

[13] Finkle, J. (2010). Los 'hackers' que atacaron Google China robaron código fuente. [Consulta: 28/9/2022]. Disponible en: https://www.reuters.com/article/china-google-idESMAE6230F820100304

La etapa final en la evolución de los ciberataques de desestabilización llega hasta la actualidad con las campañas de desinformación que utilizan plataformas y redes sociales. Casos como los escándalos ocurridos con Facebook, Twitter y otras redes sociales, por ejemplo, durante las elecciones presidenciales de Estados Unidos del 2016 o el referéndum en Reino Unido sobre el Brexit en 2020. Las acusaciones señalaban a Rusia en dos claras muestras, aunque no únicas, de la utilización de la red para propagar noticias interesadas o falsas por parte de actores estatales que buscan influir en la opinión pública y desestabilizar a terceros países[14].

3. Ciberguerra desde 2021: mismos actores, pero más sofisticación

Los ciberataques, como Singer y Friedman ya resaltaron en su clásico *Cybersecurity and Cyberwar*, se mueven de forma literal a la velocidad de la luz, no se detienen en fronteras y la mayor parte de las veces es imposible identificar al responsable directo. Cuando esto se consigue todavía es más arduo obtener pruebas de que detrás hay un instigador real. En definitiva, hay poca información en contraposición a los efectos potencialmente graves de los ciberataques (Singer & Friedman, 2014).

Además, desde 2020 los ciberataques entre Estados y la cibercriminalidad no han hecho sino multiplicarse. En 2021 el ciberespacio fue incluido por primera vez como ámbito de armas no convencionales por parte del prestigioso Instituto Internacional de Estudios para la Paz de Estocolmo (SIPRI en sus siglas en inglés). En su anuario se hace hincapié en la amenaza que representa la ciberseguridad para los Estados, cifrando el aumento de los ciberataques en un 600 % más ya en 2020 respecto a 2019. Esto ha supuesto una mayor inversión en la cibergobernanza y el refuerzo de la ciberseguridad en información, comunicaciones e infraestructuras críticas y dependientes de conexión a red (Pytlak, 2022).

De 2021 a la actualidad los ciberataques están siendo usados como arma no convencional entre Estados, los principales implicados siguieron siendo los países que anteriormente tenían gran actividad en el ciberespacio, es decir Estados Unidos, China, Rusia y la Unión Europea, a los que se van sumando otras naciones

[14] *La Vanguardia*. (2018). Las guerras de la era de la desinformación. [Consulta: 26/9/2022]. Disponible en: https://www.lavanguardia.com/internacional/20180429/443014307399/guerra-desinformacion-hibrida-fria-fake-news-ruisa.html

hasta ahora poco beligerantes en la lucha cibernética, como la India, así como otros actores que siempre estuvieron activos, casos de Corea del Norte, Israel o Irán.

3.1. Estados Unidos, China y las acusaciones mutuas

La complicada relación en el ciberespacio entre Estados Unidos y China es el reflejo de las complejas relaciones reales y sigue siendo el ejemplo más visible de ciberguerra. La Comisión de Revisión Económica y de Seguridad entre Estados Unidos y China, creada por el Congreso de Estados Unidos en 2000 con el mandato de presentarle un informe anual sobre los efectos de las actividades chinas para la seguridad nacional del país, en su último documento de noviembre de 2021 dedica varios epígrafes al ciberespacio y los riesgos para Estados Unidos desde China, resumidos en:

- La competencia tecnológica en *software* y *hardware*.
- La ventaja china en el desarrollo de la «nueva movilidad», eufemismo para referirse a la revolución del 5G en telefonía móvil.
- El acceso de empresas de computación chinas a los Estados Unidos.
- El liderazgo chino para implementar una moneda digital en países en desarrollo.
- La participación de empresas chinas en el capital de corporaciones tecnológicas estadounidenses (U.S.-China Economic and Security Review Commission, 2021).

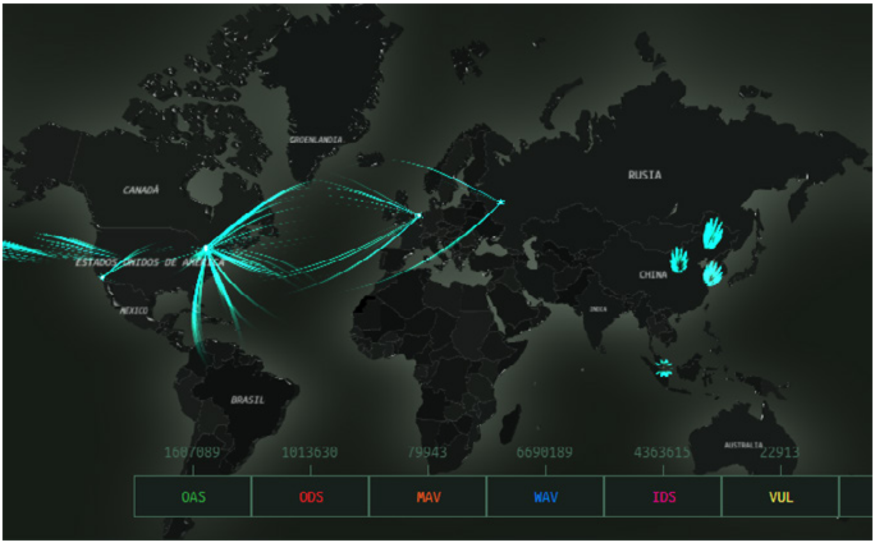
Recordemos que en 2019 el gigante chino de la telefonía móvil Huawei fue incluido en una lista negra estadounidense por riesgo contra la ciberseguridad de Estados Unidos[15], pero es significativo que las tradicionales acusaciones a China por este ciberespionaje, capital en informes anteriores (U.S.-China Economic and Security Review Commission, 2019), apenas se citaban en 2021. El informe sí resaltaba el peligro de la presencia china en los ciberespacios de África y Sudamérica, además de dar por sentado un potente ciberataque chino como inicio de una acción sobre Taiwán, región cuyo índice de ciberataques registrados es de los más altos del mundo, con millones al mes según fuentes oficiales[16].

[15] *BBC*. (2019). Huawei accuses US of cyber-attacks and threats to staff. [Consulta: 26/9/2022]. Disponible en: https://www.bbc.com/news/business-49574890

[16] *Taiwán News*. (2018). Taiwán buscará reforzar ciberseguridad en medio de amenazas de China. [Consulta: 25/9/2022]. Disponible en: https://www.roc-taiwan.org/es_es/post/12082.html

Los ciberataques provenientes de China son complicados de rastrear y aún más difícil es obtener la certeza de si son causados por grupos de ciberdelincuentes independientes o bien son encargos de instancias gubernamentales. En marzo de 2021, *Hafnium*, una organización de ciberdelincuentes supuestamente ubicada en China, aprovechó un fallo en los sistemas de la megacorporación Microsoft para robar multitud de datos de su servicio de correo electrónico, *Exchange*[17].

Estados Unidos y China son enemigos no declarados en el ciberespacio y también desde China se denuncian los ciberataques estadounidenses a sus infraestructuras sensibles. En junio de 2022 se produjo un ciberataque al sistema de cifrado del correo electrónico de la Universidad Politécnica de Xi'an, institución clave en la investigación aeroespacial china. Las autoridades acusaron a la Agencia de Seguridad de Estados Unidos (NSA, en sus siglas en inglés) del robo de datos sensibles y de otras intromisiones[18].



La empresa de antivirus Kaspersky posee una aplicación donde es posible observar los ciberataques a diferentes niveles en tiempo real. La imagen pertenece a la mañana del 28 de septiembre. Se observan los principales focos de actividad en torno a Estados Unidos y China. Es una dinámica que se repite, como se puede comprobar a diario en MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky

---

17 Alston, G. (2021). Microsoft hack will widen US-China rifts on cyber. [Consulta: 28/9/2022]. Disponible en: https://dailybrief.oxan.com/Analysis/DB260397

18 Kharpal, A. (2022). Chinese state media claims U.S. NSA infiltrated country's telecommunications networks. [Consulta: 26/9/2022]. Disponible en: https://www.cnbc.com/2022/09/22/us-nsa-hacked-chinas-telecommunications-networks-state-media-claims.html

El discurso beligerante entre Estados Unidos y China se retroalimenta con acusaciones mutuas de ciberpiratería. Otro campo de batalla es el 5G, donde China parece llevar ventaja, pues su control brindará el de los miles de millones de dispositivos conectados en todo el mundo[19].

3.2. Rusia y la Unión Europea

Como en el caso chino para Estados Unidos, la injerencia rusa en el ciberespacio parece cebarse en los países europeos. Nos podemos remontar a 2015, cuando un ciberataque proveniente de servidores rusos contra el sistema informático del Parlamento alemán hizo vulnerable información muy sensible. Esa sería la primera vez que la Unión Europea sancionase a Rusia como supuesta instigadora[20].

Desde 2021 aumentan los casos que afectan internamente a los países miembros de la Unión, como a las propias instituciones europeas y grandes corporaciones. Los intentos de ciberespionaje a políticos, periodistas, empresarios y personas de relevancia por parte de ciberpiratas rusos llevaron a que la ciberseguridad adquiriese rango prioritario en la Unión Europea, pues hasta 2021 gastaba un 41 % menos de presupuesto que Estados Unidos en la materia[21].

La guerra en Ucrania ha empeorado la situación por el incremento del riesgo de ciberataque procedente de Rusia, en especial contra las cadenas de suministros e infraestructuras sensibles de los países de la Unión. A estas ciberamenazas se sumaban los efectos de las campañas de desinformación, lo que ya era previsto por la Agencia Europea para la Ciberseguridad (ENISA, en sus siglas en inglés) en su informe sobre las perspectivas en ciberseguridad de la Unión para 2021-2022 (Agencia de la Unión Europea para la Ciberseguridad, 2021).

En la actualidad, teniendo en cuenta el fortalecimiento de la ciberdefensa resiliente de la Unión Europea, los ciberataques de procedencia rusa parecen haber cambiado el objetivo a otros países más débiles en el ciberespacio. En un lugar tan inestable

---

[19] Corral Hernández, D. (2020). *5G, una carrera por la hegemonía y el futuro con muchos beneficios.* Documento Marco IEEE, Issue 07/2020, p. 26. [Consulta: 27/9/2022]. Disponible en: https://www.ieee.es/publicaciones-new/documentos-marco/2020/DIEEEM07_2020DAVCOR_5G.html

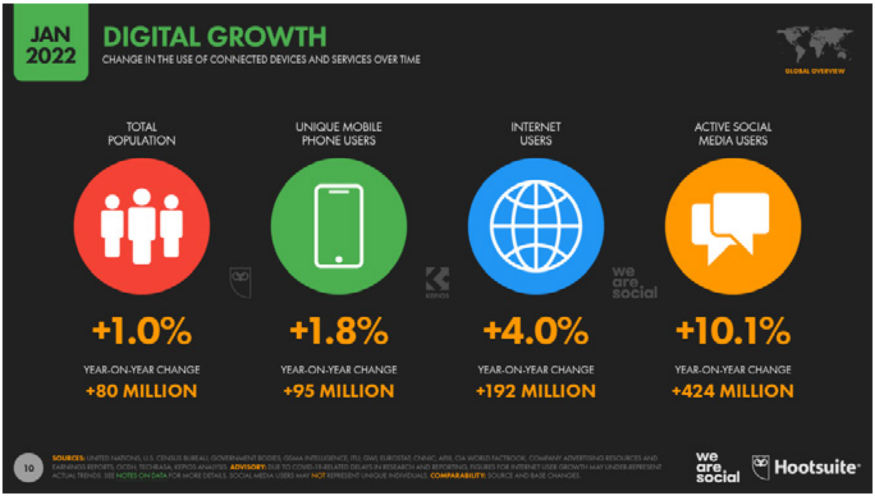
[20] Klinkartz, S. (2015). Ciberataque al Parlamento alemán: ¿puede ser espionaje? [Consulta: 28/9/2022]. Disponible en: https://p.dw.com/p/1FgOQ

[21] Merino, Á. (2022). Rusia quiere tus datos: los ciberataques se multiplican en la Unión Europea. [Consulta: 27/9/2022]. Disponible en: https://elordenmundial.com/rusia-quiere-tus-datos-los-ciberataques-se-multiplican-en-la-union-europea/

como los Balcanes, en agosto de 2022 se produjo un ciberataque contra Montenegro, país miembro de la OTAN, que vio desconectada temporalmente la sede informática del gobierno, diversas páginas estatales y servicios esenciales como el suministro de gas y agua. Las investigaciones apuntaron al grupo de ciberpiratas informáticos ruso *Cuba Ransomware*, relacionado a su vez con los servicios de seguridad[22].

3.3. A la ciberguerra se suman más países

Desde 2021 otros países aumentaron su actividad en el ciberespacio, ya sea como origen u objetivo de ciberataques. Corea del Sur estaría incluido en el segundo grupo. En 2009 el país sudcoreano se vio sorprendido por un ciberataque que paralizó temporalmente las instituciones gubernamentales, organizaciones comerciales y la red bancaria, culpándose a ciberpiratas de sus vecinos de Corea del Norte, otro país también activo en el ciberespacio, aunque como instigador de campañas de ciberataques (Clarke & Knake, 2011: 42-48).



El crecimiento exponencial del número total de usuarios en internet, de dispositivos móviles y de las redes sociales refleja la importancia del ciberespacio para actores estatales y otros cibergrupos. En la infografía se muestra como 192 millones de personas se sumaron a internet a principios de 2022 respecto al año anterior. Fuente: https://datareportal.com/

[22] *Oxford Analytica Daily Brief*. (2022). *Montenegro cyberattack underlines geostrategic trend.* [Consulta: 28/9/2022]. Disponible en: https://dailybrief.oxan.com/Analysis/DB271719

En agosto de 2022 el grupo de ciberpiratas iraquí conocido como *ALtaherea Team* lanzó un ciberataque masivo contra los sistemas de grandes puertos de Israel, poniendo en riesgo la seguridad del tráfico marítimo de la zona[23]. No es la primera vez que Israel aparece como protagonista en actos de ciberguerra, ya lo vimos como posible origen del ciberataque a una planta nuclear siria (2007) o en la creación del virus *Stuxnet,* lanzado contra la planta nuclear de Natanz (Irán, 2010), pero los israelíes se enfrentan también a peligrosos ataques desde el ciberespacio.

En septiembre de 2022 la Oficina de Control de Activos Extranjeros (OFAC en sus siglas en inglés) de Estados Unidos impuso sanciones al Ministerio de Inteligencia y Seguridad de Irán por un ciberataque contra Albania, país miembro de la OTAN. Irán es otro de los actores internacionales que van cobrando relevancia en el ciberespacio[24].

3.4. La guerra de Ucrania

Desde 2005 Rusia ha utilizado el ciberataque como arma contra los distintos gobiernos ucranianos que no son de su agrado. Ese mismo año el virus *Uroburos* permitió el robo de datos de organismos y empresas ucranianas. Un años después *Uroburos* aún andaba infectando sistemas de otros países, siguiendo operativo en Ucrania[25], mientras en 2007 un grupo conocido como Movimiento de Jóvenes Euroasiáticos, ciberpiratas autodenominados nacionalistas rusos realizó miles de ciberataques contra la página del entonces presidente ucraniano Yushchenko y durante el llamado Euromaidán se intensificaron los ciberataques masivos.

Durante la anexión rusa de la península de Crimea en febrero y marzo de 2014, los rusos consiguieron anular los centros de comunicación cortando las principales conexiones de cables de fibra óptica y logrando interrumpir la conexión entre Crimea y

[23] *Al Manar TV*. (2022). Ciberataque de grupo iraquí tumba los sitios web de cuatro puertos israelíes. [Consulta: 29/9/2022]. Disponible en: https://spanish.almanar.com.lb/653292

[24] *Oxford Analytica Daily Brief*. (2022). Albania cyberattack may have deterrence value. [Consulta: 25/9/2022]. Disponible en: https://dailybrief.oxan.com/Analysis/ES272682/Albania-cyberattack-may-have-deterrence-value

[25] *CSO*. (2014). Invisible Russian cyberweapon stalked US and Ukraine since 2005, new research reveals. [Consulta: 29/9/2022]. Disponible en: https://www2.cso.com.au/article/540097/invisible_russian_cyberweapon_stalked_us_ukraine_since_2005_new_research_reveals/

el resto de Ucrania. Las páginas, los medios de comunicación y las redes sociales del gobierno ucraniano también fueron desconectados mediante ciberataques (Geers, 2022). La guerra en el ciberespacio contra Ucrania siguió durante los dos años siguientes, siendo frecuentes los grandes apagones eléctricos debidos a ciberataques y afectando a decenas de miles de ucranianos.

Esta situación hizo que muchos analistas previeran que la invasión rusa de Ucrania de febrero de 2022 fuera precedida de ciberataques para anular las capacidades defensivas e infraestructuras críticas ucranianas. Nada de ello ocurrió y quizás la explicación venga de la experiencia de años anteriores, pues ante la gravedad de los ciberataques rusos, Ucrania ha reaccionado anticipándolos y evitando el colapso de sus redes, contando con el apoyo fundamental de unidades de la OTAN y la UE especializado en la ciberguerra[26].

Un informe de Microsoft afirma que, un día antes de la invasión, Rusia trató de anular los sistemas defensivos ucranianos, sus centros gubernamentales, energéticos, medios de comunicación y sistema financiero, fracasando (Microsoft, 2022). Antes de la guerra, la Agencia de Ciberseguridad e Infraestructura de Estados Unidos y el Servicio Estatal de Comunicaciones Especiales de Ucrania fortalecieron su colaboración, cristalizada en julio de 2022 con un acuerdo que mejora las capacidades ciberdefensivas ucranianas. En abril tuvo lugar el *Locked Shields*, un ejercicio de ciberdefensa de la OTAN, donde Ucrania fue invitada como país preferente, a instancias de Estados Unidos y el Reino Unido[27].

3.5. La OTAN y la ciberseguridad

En 2002 la Cumbre de la OTAN realizada en Praga incidió en la necesidad de que la Alianza se dotase de medios contra los ciberataques. Tras la citada creación del Centro Cooperativo de Excelencia Cibernético (CCDCOE, en sus siglas en inglés), con funciones de investigación y adiestramiento en ciberseguridad, el concepto estratégico de la OTAN de 2012 también dedicaba algunos epígrafes a alertar sobre el alarmante incremento de los

[26] Castillo, C. (2022). Rusia contra el mundo: Ucrania como escenario de ciberguerra global. [Consulta: 29/9/2022]. Disponible en: Rusia contra el mundo: Ucrania como escenario de ciberguerra global (eldiario.es).

[27] *Oxford Analytica Daily Brief*. (2022). US-Ukraine cybersecurity cooperation has limits. [Consulta: 26/9/2022]. Disponible en: https://dailybrief.oxan.com/Analysis/ES271782/US-Ukraine-cybersecurity-cooperation-has-limits

ciberataques, los riesgos crecientes de estos y las necesidad de contrarrestarlos (Fuente Cobo, 2022b), hasta el punto de que un ciberataque podría ser motivo para poner en marcha el artículo 5 de defensa colectiva del tratado fundacional de la Alianza[28].

En 2016 se firmó el Compromiso de Ciberdefensa entre los Estados miembros, para darle prioridad al desarrollo de infraestructuras nacionales en materia de ciberseguridad, dotadas además de recursos suficientes (OTAN, 2016).

En la Cumbre de Bruselas de junio de 2021 la Alianza aprobó una nueva política integral de defensa cibernética. Como novedad doctrinal la OTAN sería capaz de defenderse en el ciberespacio en todo momento y en cualquier circunstancia, es decir en tiempo de paz o en épocas conflictivas, tomando relieve el concepto de resiliencia continua (Fuente Cobo, 2022a). Esta política de ciberdefensa de la Alianza fue más beligerante y enfocada en anticipar, mediante acciones en el ciberespacio, a los posibles ataques de los que solo hubiera indicios (Weel, 2022).

La actual guerra de Ucrania responde a esta política de ciberdefensa de la Alianza. La rápida respuesta de la OTAN en ayuda de Ucrania ha resultado ser un éxito, anticipando y minimizando los ciberataques rusos.

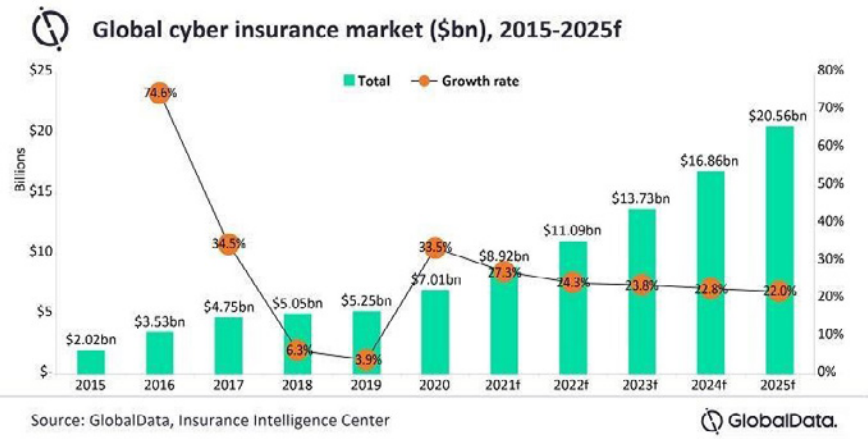
3.6. El cibercrimen

Desde 2021 los ciberataques de piratas informáticos en solitario o formando parte de grupos organizados han crecido de forma vertiginosa. Quizás el caso potencialmente más peligroso resultó el ciberataque al oleoducto Colonial Pipeline en mayo de 2021, una infraestructura petrolera capaz de transportar tres millones de barriles entre Texas y Nueva York. Se cerró el oleoducto y se pagó un oneroso rescate a *DarkSide*, el grupo ciberdelincuente responsable localizado por algunos medios en el este de Europa. El gobierno de Estados Unidos decretó el estado de emergencia ante la gravedad de la situación[29].

[28] Fibla, C. (2016). La OTAN incluye los ataques cibernéticos entre los posibles actos de guerra. [Consulta: 26/9/2022]. Disponible en: https://es.euronews.com/2016/06/15/la-otan-incluye-los-ataques-ciberneticos-entre-los-posibles-actos-de-guerra

[29] Egan, M. & Duffy, C. (2022). El Oleoducto Colonial reinicia operaciones después de un cierre de seis días por ciberataque. [Consulta: 26/9/2022]. Disponible en: https://cnnespanol.cnn.com/2021/05/13/oleoducto-colonial-reinicia-operaciones-gasolina-ciberataque-hackeo-trax/

Las petrolíferas, incluyendo las infraestructuras de transporte y refinado del crudo, parecen ser los nuevos objetivos de los cibercriminales debido a los lucrativos rescates. En 2022, durante febrero las terminales petroleras de diversos puertos de Alemania, Bélgica y Países Bajos fueron ciberatacadas[30] y en agosto otro ciberataque afectó a las redes informáticas de la petrolera ENI Italia[31].



El problema creciente de la ciberdelincuencia a nivel global: El mercado global de seguros cibernéticos alcanzará una inversión de 20.000 millones de dólares en 2025. Un crecimiento continuo y acelerado desde 2015. Fuente: https://www.insurancetimes.co.uk/news/cyber-insurance-industry-predicted-to-exceed-20bn-gwp-by-2025-globaldata/1438074.article

Del cibercrimen no se libran tampoco las empresas electrónicas avanzadas. Como principal ejemplo tenemos a la corporación Acer, que en marzo de 2021 tuvo que pagar un elevado rescate al grupo de ciberdelincuentes conocido como *REvil*, de origen ruso[32]. Meses después, *REvil* atacaba algunos sistemas vulnerables de Apple, pero en enero de 2022 el Servicio Federal de

30 *Dailymotion*. (2022). Ciberataque contra las terminales petroleras de puertos de Alemania, Bélgica y Países Bajos. [Consulta: 27/9/2022]. Disponible en: https://www.msn.com/es-es/dinero/newsspain/ciberataque-contra-las-terminales-petroleras-de-puertos-de-alemania-b%C3%A9lgica-y-pa%C3%ADses-bajos/vi-AATrIrN?category=foryou

31 *Primer Informe*. (2022). *Un ciberataque afectó redes informáticas de la petrolera ENI.* [Consulta: 28/9/2022]. Disponible en: https://primerinforme.com/petroleo/un-ciberataque-afecto-redes-informaticas-de-la-petrolera-eni/

32 Hope, A. (2021). *Acer Reportedly Suffered a REvil Ransomware Attack Attracting the Highest Ransom Demand in History of $50 Million.* [Consulta: 26/9/2022]. Disponible en: https://www.cpomagazine.com/cyber-security/acer-reportedly-suffered-a-revil-ransomware-attack-attracting-the-highest-ransom-demand-in-history-of-50-million/

Seguridad de Rusia anunció el desmantelamiento de este grupo de ciberdelincuentes.

Como señalábamos, el cibercrimen también golpea a instituciones públicas sensibles como sistemas sanitarios e instituciones educativas. Desde 2020 el sector educativo es uno de los más golpeados por los ciberpiratas. Un estudio cifra en el 44 % el total de escuelas víctimas de ciberataques en todo el mundo[33]. Algunas voces abogan por la urgencia de legislar globalmente contra cierto tipo de ciberataques.

4. Dos paradigmas: beligerancia y resiliencia en la ciberdefensa

A falta de acuerdos internacionales en ciberseguridad y lucha contra la ciberdelincuencia, quizás reflejo de que el ciberespacio sigue siendo un campo de batalla en permanente tensión, cada país desarrolla sus propios centros coordinadores de la ciberdefensa. No existen tratados globales con relación al ciberespacio, lo que no parecería una utopía al menos en los casos de ciberdelincuencia, ya que los perjudicados son gobiernos, corporaciones y ciudadanos de cualquier país. En 2021 el presidente estadounidense, Joe Biden, llegó a plantear a su homólogo ruso, Vladimir Putin, establecer ciertos límites para luchar contra el cibercrimen, sin concretarse acción alguna[34].

Joseph S. Nye escribe que, teniendo en cuenta la situación geopolítica actual, es difícil concienciar a los Estados sobre la necesidad de regular el alcance de las armas cibernéticas, como pasó en su momento con las nucleares o biológicas. De hecho, ya se hace complicado determinar si un virus informático puede ser considerado un arma (Nye, 2021).

En este sentido, Naciones Unidas creó en 2019 un Grupo de Trabajo de Composición Abierta (OEWG, por sus siglas en inglés) dedicado a la ciberseguridad. Dos años después presentó un documento abierto a los países miembros de la Asamblea General. En

[33] Carrasco, F. (2021). *Ciberataque en escuelas: ¿cómo protegerlas?* [Consulta: 26/9/2022]. Disponible en: http://tecnoeducacion.cl/2021/08/19/ciberataque-en-escuelas-como-protegerlas/

[34] *Agencia EFE*. (2021). Biden y Putin pactan la vuelta de embajadores y coooperar en ciberseguridad. [Consulta: 28/9/2022]. Disponible en: https://www.efe.com/efe/espana/mundo/biden-y-putin-pactan-la-vuelta-de-embajadores-cooperar-en-ciberseguridad/10001-4564153

él se vinculaba el uso del ciberespacio al respeto a los derechos humanos, haciéndose un llamamiento para aumentar las capacidades globales en ciberseguridad (Naciones Unidas, 2021). La realidad es que cada Estado invierte en función de sus propias capacidades y la percepción de sus principales ciberamenazas.

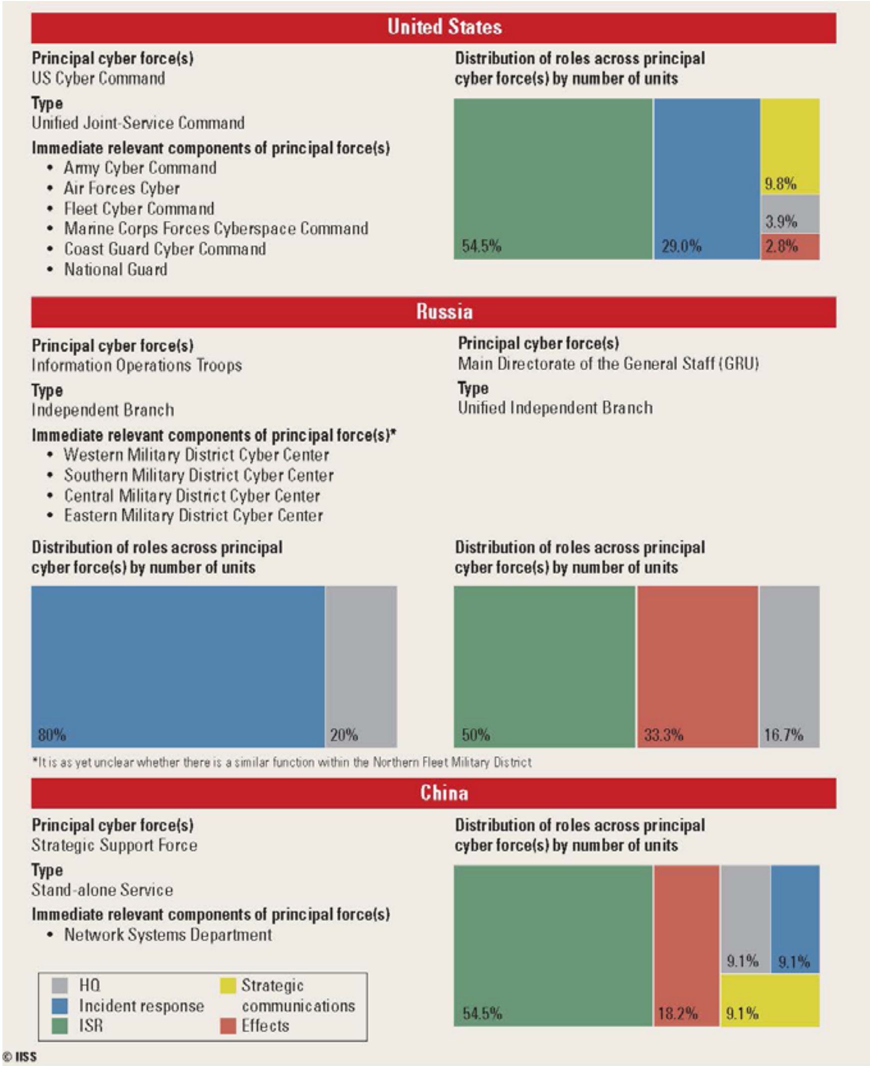
4.1. Centralización y beligerancia en Estados Unidos, China y Rusia

En mayo de 2021, al tiempo que ofrecía al presidente ruso cooperación en materia de ciberseguridad, el presidente Biden firmó una orden ejecutiva para renovar la ciberseguridad estadounidense mediante el establecimiento de nuevos estándares y cifrados. Las actuales líneas principales globales en ciberseguridad pasan por el refuerzo de centros nacionales que aglutinen recursos y coordinen al resto de organismos con alguna competencia en la materia, sean civiles o militares[35].

Con un fuerte desembolso en medios en los últimos años, los Estados apuestan por un entorno ciberseguro. Ejemplos de ello son las principales ciberpotencias globales que han creado estructuras o las han potenciado, caso de existir anteriormente. Los casos de Estados Unidos, China y Rusia constituyen ejemplos de centros más focalizados en lo beligerante que en lo resiliente, al contrario que en otras áreas, como veremos a continuación para la Unión Europea.

Así, tras décadas de experiencia la principal decisión, primeramente, ha sido conseguir la centralidad en la materia, que posibilita la atención al ciberespacio de manera más eficiente, en forma de dotar a un organismo superior y coordinador de diversos departamentos ya existentes. De esta forma, en Estados Unidos tenemos el Cíber Comando de Estados Unidos (USCYBERCOM, en sus siglas en inglés) creado en 2010 y que coordina a varias agencias militares y civiles; en China, la Fuerza de Apoyo Estratégico del Ejército Popular creada el 31 de diciembre de 2015 y vinculada al complejo militar como la quinta división del Ejército chino, mientras en Rusia se anunció en 2017 la creación de las llamadas Tropas de Operaciones de Información, también dentro del ámbito de la defensa y fuertes vínculos con actividades de

[35] *Stratfor Worldview*. (2021). U.S.: Biden Directs Federal Cybersecurity Revamp. [Consulta: 25/9/2022]. Disponible en: https://worldview.stratfor.com/situation-report/us-biden-directs-federal-cybersecurity-revamp



Estructura de las fuerzas cibernéticas de Estados Unidos, Rusia y China para 2022. Fuente: Military cyber capabilities. The Military Balance. (2022). 122:1, pp. 507-510.

contrapropaganda e información, además del ámbito cibernético en general (The Military Balance, 2022).

4.2. Hacia una ciberdefensa en la Unión Europea

En la actualidad, en la Unión Europea no existe un centro coordinador de los organismos de la organización o nacionales tocantes a la ciberseguridad, más allá de la Agencia Europea para la

Ciberseguridad (ENISA, en sus siglas en inglés), con labores de asesoramiento. El enfoque respecto al ciberespacio, aunque es una percepción que progresivamente irá cambiando, es el de la resiliencia y no la beligerancia. Además, la propia conformación de la Unión Europea, delicada desde los puntos de vista estratégico y jurídico, provoca ciertos recelos cuando se habla de una institución en ciberseguridad común a todos los países (Fuertes, 2022).

Con todo, la Unión Europea da pasos en su lucha contra la ciberdelincuencia y el impulso de una ciberdefensa común. En junio de 2019 se publicó el primer Reglamento de Ciberseguridad y en diciembre de 2020 la Comisión Europea presentó la Estrategia de Ciberseguridad Europea, con medidas concretas frente a las ciberamenazas externas y propuestas de herramientas de actuación e inversión en este campo, documento actualizado en 2021 (Consejo de la Unión Europea, 2022).

Por su parte, la Directiva sobre seguridad de las redes y de la información (NIS, en sus siglas en inglés) tiene como objetivo la ciberseguridad de todos los Estados miembros, reforzando los requisitos de seguridad, las cadenas de suministro, estandarizar las obligaciones de información e introducir medidas de supervisión estrictas y requisitos de aplicación más estrictos, incluidas sanciones armonizadas en toda la UE. El texto redactado por la Comisión de Industria, Investigación y Energía debe ser ratificado por el Parlamento Europeo[36].

Además, la Agencia Europea para la Ciberseguridad, creada ese 2019, se le ha añadido el Centro Europeo de Ciberdelincuencia, vinculado a Europol, mientras la Agencia Europea de Defensa colabora con los Estados miembros para crear y formar personal especializado en ciberdefensa. Mientras en abril de 2021 el Consejo anunció la creación del Centro de Competencia en Ciberseguridad, ubicado en Budapest y con funciones de apoyo a los Estados (Consejo de la Unión Europea, 2021).

Dentro de la ciberseguridad, el paliar la dependencia extranjera en sectores estratégicos para la política y economía de la Unión, también es una prioridad como, por ejemplo, demuestran las normativas sobre el 5G o de suministro de *chips*, en donde también aparece la resiliencia, en este caso de las cadenas de suministro tecnológicas, como principal objetivo (Rodríguez, 2021).

[36] Negreiro, M. (2020). The NIS2 Directive A high common level of cybersecurity in the EU. Briefing EU Legislation in Progress, junio, 2022. [Consulta: 30/9/2022]. Disponible en: The NIS2 Directive (europa.eu)

5. Conclusiones: todas las sociedades son cibercombatientes, aunque no lo sepan

Como hemos visto en los principales casos, la falta de atribución se une a la impunidad de muchos ciberataques, de los que no se llega a vislumbrar a sus actores e instigadores, más allá de las sospechas. Los riesgos de ciberseguridad para gobiernos, empresas y ciudadanos se han multiplicado en los últimos años, iniciándose este veloz aumento desde la suma de usuarios de internet como efecto colateral de la pandemia y sus restricciones de movilidad. Podríamos asegurar que cualquier organización gubernamental, pública o privada se enfrenta en mayor o menor medida a la presión de proporcionar seguridad a sus trabajadores y usuarios remotos.

Reflejo de enemistades históricas y de la tensa situación actual, que ha sumado nuevos actores al confuso mapa geopolítico, las tensiones en el ciberespacio se han intensificado desde 2020 con dañinos ataques cibernéticos contra objetivos críticos para muchos Estados prominentes por parte de otros agentes estatales y piratas informáticos criminales a su servicio. En el horizonte las democracias occidentales muestran una preocupación en aumento por la influencia de China sobre la infraestructura global de internet, no solamente por ser el origen de dañinos ataques en el ciberespacio, sino además porque en cuanto a los componentes de *hardware* y diversas aplicaciones *software*, China se presenta como un fabricante competitivo y el principal exportador, así como el país que lidera con claridad la implementación del 5G a escala global. Las propuestas de Pekín para aumentar el control centralizado de internet como, por ejemplo, mediante el «Nuevo Protocolo de Internet» desarrollado por la compañía china Huawei o las directrices de octubre de 2021 sobre normalización técnica, sean aceptadas por las democracias liberales, que a su vez optan en mayor medida por legislar para conseguir autonomía propia en la cadena que hace posible la conexión en el ciberespacio[37].

Las soluciones políticas y regulatorias globales a la ciberdelincuencia, también global, o a los efectos de la ciberguerra, con el fin de no traspasar determinadas y peligrosas líneas rojas, se antojan

[37] Oxford Analytica Daily Brief. (2021). Plans will raise China’s profile in standard-setting. [Consulta: 26/9/2022]. Disponible en: https://dailybrief.oxan.com/Analysis/DB265000

hoy muy lejanas con los enfrentamientos abiertos en la actualidad y el enconamiento de las rivalidades, a pesar del creciente y evidente daño económico, social y político para los Estados.

A medio plazo y de forma individual muchos países posiblemente sigan la línea marcada por Estados Unidos, exijan normas que reconozcan la relevancia del derecho internacional en el ciberespacio, integren los estándares estadounidenses y reclamen la prohibición del ataque a infraestructuras críticas mediante ataques cibernéticos, así como el daño deliberado a objetivos civiles. Por el contrario, otro obstáculo puede ser el recelo de ciertos países en compartir códigos, sistemas y estrategias, aunque sean Estados amigos o se cuenten entre los miembros de la OTAN.

Para ello y a nivel global, el papel de las diversas Fuerzas Armadas ante la ciberguerra ha ido transformándose durante la última década, pero sin perder sus elementos tradicionales de cohesión como la autoridad, el mando único o el carácter jerarquizado intrínseco a las estructuras militares. Su adaptación para responder a la lucha tecnológica en el ciberespacio pasó por una mayor flexibilidad, coordinación y rapidez, tres factores esenciales para dar respuesta a un ciberataque (Ágreda, 2022).

Relacionado y no menos importante es el refuerzo de la protección de datos personales de los militares en la red, en especial en las operaciones delicadas y para preservar su seguridad y el éxito en los objetivos, que pueden ser puestos en riesgo, por ejemplo, con el mal uso de los teléfonos inteligentes[38].

El futuro inmediato pasa por la adopción de arquitecturas de redes de confianza cero (ZTN, en sus siglas en inglés), donde los dispositivos conectados no serán nunca considerados fiables, aunque estén verificados desde una red reconocida, particularmente de grandes organizaciones que operen en infraestructuras críticas. Como señalábamos, en Estados Unidos ya se trabaja para restringir el acceso a los sistemas informáticos solo cuando sea necesario y se empieza a exigir certificaciones a los contratistas garantizando, bajo fuertes penas, que el software que entregan no contiene vulnerabilidades[39].

[38] Harkins, G. (2020). A Lance Corporal's Phone Selfie Got His Marine Unit 'Killed' at 29 Palms. [Consulta: 27/9/2022]. Disponible en: https://www.military.com/daily-news/2020/01/07/lance-corporals-phone-selfie-got-his-marine-unit-killed-29-palms.html

[39] Oxford Analytica Daily Brief. (2021). Adoption of zero trust cybersecurity faces hurdles. [Consulta: 28/9/2022]. Disponible en: https://dailybrief.oxan.com/Analysis/DB262554

La misma presión oficial crecerá contra las campañas de desinformación y desestabilización llegadas desde páginas de internet y redes sociales, tratándose de cierta forma de ciberguerra, aunque aquí esta cuestión puede chocar con derechos asentados en las sociedades occidentales como el de información y libertad de expresión. Especial atención requerirán las infraestructuras y servicios críticos, como demuestran los ejemplos de ciberataques a los sistemas sanitarios o de transporte, con riesgos ciertos en vidas humanas. Respecto a los ciudadanos y las corporaciones privadas, objetivos de grupos de ciberdelincuentes con el fin de extorsionarles a cambio de grandes cantidades de dinero, se necesita una amplia cooperación entre países, sobre todo entre aquellos donde se originan tales ciberataques y los que son víctimas, que hoy parece difícil de obtener.

En la actualidad, los conceptos de anticipación y resiliencia respecto al ciberespacio, entendidos como la capacidad continuada en el tiempo de prevenir ciberataques en sus puntos críticos, es el elemento central en las estrategias cibernéticas de muchos países, por ejemplo, en la española. En esta visión proactiva para minimizar las ciberamenazas son importantes los ejercicios de simulación como los efectuados por la OTAN. Se debe contar con la cooperación internacional, al igual que es imprescindible la colaboración público-privada, a fin de conseguir una mejor resiliencia.

Referencias

Agencia de la Unión Europea para la Ciberseguridad. (2021). *Informe «Panorama de amenazas» de ENISA de 2021*. ENISA, 2021. Disponible en enisa-threat-landscape-2021-2022-final_es.pdf (europa.eu)

Ágreda, Á. G. d. (2022). Ética para humanos en tiempo de máquinas. En: *Cuestiones sobre ética militar.* Madrid, Ministerio de Defensa, pp. 121-149.

Buchanan, B. (2020). *The hacker and the State: Cyber attacks and the new normal of geopolitics.* Cambrigde (Massachusetts), Harvard University Press.

Calvo Albero, J. L. (2022). Primeras impresiones militares. En: Ejércitos & Catarata (edits). *La guerra de Ucrania: Los 100 días que cambiaron Europa.* Madrid, pp. 65-94.

Clarke, R. A. & Knake, R. A. (2011). *Guerra en la red. Los nuevos campos de batalla.* Barcelona, Arial.

Consejo de la Unión Europea (2021). *El Consejo da luz verde al Centro de Competencia en Ciberseguridad con sede en Bucarest.* Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/

Consejo de la Unión Europea. (2022). *Ciberseguridad: cómo combate la UE las amenazas cibernéticas.* Disponible en: https://www.consilium.europa.eu/es/policies/cybersecurity/_

Crawford, J. C. (2022). Ciberataque al transporte marítimo ¿amenaza real o ciencia ficción? *Revista de Marina.* Julio-agosto. Año CXXXVIII. Volumen 140 (989). Disponible en: Ciberataque al transporte marítimo ¿amenaza real o ciencia ficción? | Revista de Marina (revistamarina.cl)

Fuente Cobo, I. (2022a). La OTAN y el ciberespacio: un nuevo dominio para las operaciones. *Revista Ejército.* 972, pp. 84-91. Disponible en: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/LaOTAN_ciberespacio.pdf

— 2022b. Los ocho conceptos estratégicos de la historia aliada. En: *El futuro de la OTAN tras la cumbre de Madrid 2022.* Madrid, Ministerio de Defensa, pp. 25-43. Disponible en: https://www.ieee.es/Galerias/fichero/cuadernos/CE_211/Cap_1_ocho_conceptos.pdf

Fuertes, M. (2022). *Metamorfosis del Estado. Maremoto digital y ciberseguridad.* Madrid, Marcial Pons.

Geers, K. (2022). *Cyber war in perspective: Russian aggression against Ukraine.* Tallin: NATO CCD COE Publications. Disponible en: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

IEEE. (2021). *Panorama de tendencias geopolíticas. Horizonte 2040.* 2.ª ed. Madrid, Ministerio de Defensa. Disponible en: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2021/Panorama_de_Tendencias_Geopoliticas_Horizonte_2040_SegundaEdicion.pdf

Microsoft, D. S. U. (2022). Special report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Disponible en: https://www.iisf.ie/files/UserFiles/Documents/2022/MS_UkraineSpecialReport.pdf

Naciones Unidas. (2021). *Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report*.

Disponible en: Developments in the field of information and telecommunications in the context of international security – UNODA

Nye, Joseph S. Jr. (14 diciembre 2021). The End of Cyber-Anarchy? *Foreign Affairs*. Disponible en: https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy

OTAN. (2016). *Cyber Defence Pledge.* Disponible en: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Pytlak, A. (2022). Cyberspace and the malicious use of information and communications technology. En: *SIPRI Yearbook 2022: Armaments, Disarmament and International Security.* Estocolmo, s. n., p. 784.

Quintana, Y. (2016). *Ciberguerra.* Madrid, Catarata.

Rodríguez, A. G. (2021). Ley europea de chips: estrategia y diplomacia. *CIDOB Opinion,* 10/2021, p. 3. Disponible en: https://www.cidob.org/en/publications/publication_series/opinion/2021/ley_europea_de_chips_estrategia_y_diplomacia

Singer, P. W. & Friedman, A. (2014). *Cibersecurity and cyberwar: What everyone needs to know.* Oxford, Oxford University Press.

Suárez Sánchez-Ochoa, A. (2015). *El quinto elemento: Espionaje, ciberguerra y terrorismo. Una amenaza real e inminente.* 2.ª ed. Barcelona, Deusto.

The Military Balance. (2022). Military cyber capabilities. En: *The Military Balance.* Pp. 507-510.

U.S.-China Economic and Security Review Commission. (2019). *How Chinese Companies Facilitate Technology Transfer from the United States.* Disponible en: How Chinese Companies Facilitate Technology Transfer from the United States | U.S.-CHINA | ECONOMIC and SECURITY REVIEW COMMISSION (uscc.gov)

U.S.-China Economic and Security Review Commisssion. (2021). *Report to Congress.* Disponible en: 2021 Annual Report to Congress | U.S.- CHINA | ECONOMIC and SECURITY REVIEW COMMISSION (uscc.gov)

Weel, D. V. (2022). Los nuevos retos de seguridad en un panorama estratégico cambiante. En: *El futuro de la OTAN tras la cumbre de Madrid 2022.* Madrid, Ministerio de Defensa, pp. 57-69. Disponible en: Cap_3_retos.pdf (ieee.es)

ANEXO
Cronología de veinte años de ciberguerra

FECHA	ACONTECIMIENTOS
2000	Primer plan estatal en ciberseguridad: Estrategia Nacional para la Seguridad del Ciberespacio de Estados Unidos.
2007	Primer ataque por denegación de servicio (DDoS) contra un Estado: en mayo, ciberataque a Estonia atribuido a Rusia.
	En septiembre, la Fuerza Área de Israel bombardea un reactor nuclear en Siria en la operación *Orchard*. Un ciberataque previo anula el sistema de defensa antiaérea sirio.
2008	Primer virus utilizado para ataques de secuestro de sistemas o *ransomware*: *Trojan.RandsomC*.
	El virus *Agent.btz* se considera el primer caso de ciberespionaje masivo. Se extraen datos de decenas de equipos de las Fuerzas Armadas de Estados Unidos. La crisis será de tal magnitud que un año después llevará a la creación del Mando Cibernético de Estados Unidos.
2010	Los papeles de Wikileaks, organización sin ánimo de lucro que publica documentos filtrados de instituciones oficiales, en especial del Departamento de Estado estadounidense, la guerra de Afganistán y la guerra de Iraq.
	Stuxnet, un complejo virus consigue paralizar la central nuclear de Narantz en Irán. Extendido a otros lugares, su origen fue un arma cibernética creada por Estados Unidos e Israel para sabotear el programa nuclear iraní.
2012	El *malware Shamoon*, de origen desconocido, paraliza la producción de crudo de la petrolera saudí Aramco. Se cree que es el peor ciberataque de la historia, en cuanto a sus costes económicos.
2013	Estalla el caso de Edward Snowden, antiguo analista de la NSA, que denuncia campañas sofisticadas de espionaje global por parte de la agencia estadounidense.
	Se descubre el virus *Red October*, que estuvo operando en todo el mundo durante cinco años, transmitiendo información sensible en decenas de países.
2014	Se da a conocer la vulnerabilidad *Heartbleed*, considerada la mayor vulnerabilidad de seguridad en internet, al afectar a los servicios de cifrado de las comunicaciones, lo que habría permitido obtener información sensible de los sistemas afectados y a nivel global.
2015	El ciberataque más importante de la historia de Estados Unidos: vulnerabilidad de los datos de más de 22 millones de personas en el sistema de la Oficina de Administración de Personal. El ataque provenía de China y tenía el objetivo de hacerse con la información de residentes chinos en Estados Unidos.
2016	Un ciberataque en enero provoca un apagón en el oeste de Ucrania. Es el primer incidente de este tipo provocado por un ataque cibernético.
2017	Un grupo de ciberdelincuentes consigue el acceso a más 360.000 ordenadores pertenecientes a empresas y ciudadanos europeos mediante *WannaCry*, un virus de tipo *ransomware*. El resultado fueron pérdidas estimadas en más de 4.000 millones de euros y daños informáticos sin precedentes.
2020	En septiembre las autoridades alemanas calificaron la muerte de una paciente en el hospital de Düsseldorf como la primera víctima real de un ciberataque. Aunque el estado de la paciente era crítico cuando llegó al hospital, no pudo ser intervenida debido al colapso del sistema informático del centro sanitario.

FECHA	ACONTECIMIENTOS
2021	*Hafnium*, organización de ciberdelincuentes supuestamente ubicada en China, roba los datos del servicio de correo electrónico de Microsoft, *Exchange*, de miles de organizaciones públicas y privadas en todo el mundo.
	Ciberataque al oleoducto estadounidense Colonial en mayo, que se cerró y se pagó un oneroso rescate a *DarkSide*, el grupo ciberdelincuente responsable. El gobierno de Estados Unidos decretó el estado de emergencia.
2022	Guerra de Ucrania, los ciberataques rusos son minimizados gracias a la ayuda de expertos de la OTAN y la Unión Europea.