Facultad de Ciencias Humanas y Sociales

Grado en Relaciones Internacionales

Trabajo Fin de Grado

La importancia del dominio cibernético en el contexto internacional actual como 5º dominio de la guerra

Actualización de la estrategia de ciberseguridad de la Unión Europea.

Estudiante: Clara Calzado Miranda

Director: Ana María Ovejero Puente

Madrid, Abril 2021

ÍNDICE DE CONTENIDOS

GLOSARIO

- AAPP: Administraciones Públicas.
- ADM: Armas de Destrucción Masiva.
- AED: Agencia Europea de Defensa.
- AR: Alto Representante de la Unión Europea.
- ASEAN: Asociación de Naciones del Sudeste Asiático.
- CCDCOE: Centro de Excelencia de la Ciberdefensa Cooperativa de la OTAN (por sus siglas en inglés).
- CC.PP: Ciencias Políticas.
- CDT: Cyber Diplomatic Toolbox.
- CFR: Council on Foreign Relations.
- CSIS: Centro de Estudios estratégicos Internacionales (por sus siglas en inglés).
- Daesh: Estado Islámico para Irak y Levante (por sus iniciales en árabe).
- DHS: Departamento de Seguridad Nacional de los Estados Unidos (por sus siglas en inglés).
- DIH: Derecho Internacional Humanitario.
- DNS: Sistema de nombres de dominio (por sus siglas en inglés).
- DoD: Departamento de Defensa de Estados Unidos (por sus siglas en inglés).
- ECI: Ejército Cibernético Iraní.
- EE.UU: Estados Unidos de América.
- EM: Estado Miembro.
- ENISA: Agencia Europea de Seguridad de las Redes y de la Información (por sus siglas en inglés).
- Europol: Oficina Europea de Policía.
- IA: Inteligencia Artificial.
- ICANN: Corporación de Internet para la Asignación de Nombres y Números.
- ITU: Unión Internacional de Telecomunicaciones.
- MIT: Instituto Tecnológico de Massachussets (por sus siglas en inglés).
- NHS: Servicio Nacional de Salud de Reino Unido (por sus siglas en inglés).
- NSA: Agencia de Seguridad Nacional de Estados Unidos (por sus siglas en inglés).
- OEA: Organización de Estados Americanos.

- OPM: United States Office of Personnel Management.
- OSCE: Organización para la Seguridad y la Cooperación en Europa.
- OTAN: Organización del Tratado del Atlántico Norte.
- PCSD: Política Común de Seguridad y Defensa de la Unión Europea.
- PE: Parlamento Europeo.
- PESC: Política Exterior y de Seguridad Común de la Unión Europea.
- PSYOPS: Operaciones Psicológicas (por sus siglas en inglés).
- PYMES: Pequeñas y Medianas Empresas.
- RR.II: Relaciones Internacionales.
- SCI: Sistemas de Control Industrial.
- SEAE: Servicio Europeo de Acción Exterior
- TIC: Tecnologías de la Información y la Comunicación.
- UE: Unión Europea.
- US-CERT: Equipo de preparación para emergencias informáticas de Estados Unidos (por sus siglas en inglés).
- USCYBERCOM: Cíber Comando de Estados Unidos.
- USD: Dólares Estadounidenses.
- 5G: Quinta Generación de Tecnologías de Telefonía Móvil.

Resumen

El uso de las nuevas tecnologías como instrumentos que sirven a unos intereses las convierte en armas nuevas y poderosas, con capacidad de influencia mundial en un entorno globalizado. Esto ha provocado que nos encontremos con un nuevo dominio de la guerra: el ciberespacio. Ante este nuevo escenario de batalla, los distintos actores que pueden ver sus intereses afectados deben diseñar y adaptar sus estrategias para que éstas resulten efectivas. El objeto de este trabajo de fin de grado es el análisis exhaustivo de este nuevo dominio y la realización de un análisis comparativo centrado en la estrategia de ciberseguridad vigente en la Unión Europea, para comprender cómo debería modificarse para aumentar su efectividad.

Palabras clave

Dominio cibernético, cíberseguridad, Unión Europea, guerra, estrategia.

Abstract

The use of new technologies as instruments that serve certain interests makes them new and powerful weapons, with the capacity for worldwide influence in a globalized environment. This has led to the emergence of a new domain of warfare: cyberspace. Faced with this new battle scenario, the different actors whose interests may be affected must design and adapt their strategies to be effective. The purpose of this thesis is the exhaustive analysis of this new domain and the realization of a comparative analysis focused on the current cybersecurity strategy in the European Union, in order to understand how it should be modified to increase its effectiveness.

Key Words

Cyber Domain, cybersecurity, European Union, war, strategy.

1) INTRODUCCIÓN

Nos encontramos inmersos en la "Cuarta Revolución Industrial" (Skilton et al., 2018), término que otros han simplificado en "Industria 4.0" (Meier, 2017). Es un fenómeno reciente del que todavía no podemos llegar a imaginar su alcance, su profundidad y sus efectos, aunque sí vislumbramos su relevancia para el panorama político internacional. Este concepto, acuñado en 2016, explica cómo los sistemas de fabricación virtuales y físicos cooperan entre sí de manera flexible a nivel global (Schwab, 2016), siendo la fusión tecnológica y su interacción mediante los dominios físicos, digitales y biológicos lo que hace que esta Cuarta Revolución Industrial sea diferente a las anteriores. Esta mejora de la productividad y eficiencia cuenta, sin embargo, con diversos inconvenientes, uno de los cuales analizaremos extensamente en este trabajo: los crecientes riesgos cibernéticos.

Hoy el poder esencial es la obtención y gestión de información. Lo ha sido desde la invención de la escritura, a finales del IV milenio a.C. La información es poder (Hobbes, 1651) y el elemento esencial de esta sociedad digital creada a partir de esta Cuarta Revolución Industrial es la información digitalizada, cuyo control tiene el potencial de alterar las dinámicas de poder económico, social y político en el panorama internacional. Toda esta información se encuentra en el dominio cibernético, que es abierto, ilimitable e incontrolable, donde el poder económico o militar de los estados puede verse en jaque por un ataque llevado a cabo por actores tradicionalmente menos poderosos, que en la actualidad cuentan con mejores sistemas de extracción y gestión de datos e información de la red. Si los sistemas utilizados para regular los aspectos económicos, sociales, militares o culturales se encentran en este dominio, es evidente que puede convertirse en un auténtico campo de batalla, en el que unos tratan de acceder a la información y otros de evitar tales accesos; y no tan sólo estados, sino todo tipo de organizaciones criminales, empresariales o individuos, que se aprovechan anonimidad que ofrece el ciberespacio para llevar a cabo sus objetivos. Hay que tener en cuenta, además que este tipo de actuaciones no se limitan tan sólo al robo de información, o al robo de datos de naturaleza personal, empresarial, o estatal, sino que pueden consistir en auténticos actos terroristas contra seres humanos o lugares físicos, si se atacan cibernéticamente industrias críticas, medios de transporte u hospitales, o instituciones de seguridad y defensa.

El dominio cibernético es además un campo de batalla que no exige grandes inversiones materiales en comparación al gasto militar tradicional, y pueden llevarse a cabo ataques de forma anónima y remota. Se ha llegado a comparar el atractivo de las armas digitales al de las armas nucleares: es un instrumento para que un actor que no tenga grandes medios económicos y materiales adquiera una verdadera capacidad de ataque contra objetivos públicos o privados en un escenario internacional (Perloth et al., 2013).

Estas características presentan un escenario preocupante; más aún cuando en pocos años habrá un crecimiento exponencial del uso de la red con la introducción de las redes de quinta generación, o 5G. El conocido como 5G es la evolución tecnológica aplicada a las redes de telecomunicaciones que sostienen la tecnología móvil gracias a lo cual se aumentará la velocidad de conexión, se reducirá al mínimo la latencia (el tiempo de respuesta de la web) y se multiplicará exponencialmente el número de dispositivos conectados. En otras palabras: estaremos conectados a todo, todo el día, y obtendremos respuestas el menor tiempo posible. Las próximas redes de banda ancha móvil reemplazarán la actual conexión 4G LTE, provocando que las velocidades de carga y descarga sean exponencialmente más rápidas, y significarán un incremento también exponencial en la cantidad y velocidad de los datos y de la información en circulación, de naturaleza cuantitativa (número de datos) y cualitativa (información sobre la que versan los datos). En consecuencia, se puede afirmar que no va a existir casi ningún ámbito de la actividad que a corto o medio plazo no vaya a ser gestionado por sistemas de información o que se vaya a profundizar su dependencia de los mismos hasta límites casi inimaginables.

Por lo tanto, se admite pacíficamente que Internet se ha convertido en el elemento clave para el crecimiento económico en nuestra sociedad actual, más aún en la sociedad post-pandemia, además de ser el recurso esencial del que otros sectores productivos dependen (pensemos en áreas como banca, finanzas, infraestructuras y medios de transporte, energía o sanidad). Es precisamente por este elevado grado de dependencia de Internet y las TIC que la seguridad de estos entornos cibernéticos es fundamental, ya que un fallo en la red o una incidencia sobre la misma podrían suponer una vulnerabilidad y/o amenaza en materia de seguridad, pudiendo hacer peligrar la supervivencia de un sector industrial (Machín et al, 2016). Por tanto, a nivel internacional, la ciberdefensa y la ciberseguridad son destacadas como una de las mayores prioridades de seguridad, debiendo ser tratadas a nivel global.

En el presente trabajo analizaremos detalladamente lo que ahora se esboza, prestando atención a los sujetos implicados, y al objeto y tipos de ataques.

Para hacer frente a un escenario tan complejo y que, de no ser gestionado correctamente, puede tener tan graves consecuencias, tanto empresas como estados y organizaciones internacionales han desarrollado estrategias y tácticas para gestionar la seguridad de sus redes de información. El objetivo que perseguimos es examinar los planes de ciberseguridad de diversas potencias, y en especial el de la UE, para concluir cuáles son sus elementos esenciales, cuáles son sus fortalezas y debilidades y cómo debería avanzarse en este sentido para garantizar la seguridad en la red en los próximos años. La cuestión esencial es determinar si es adecuada o puede tener éxito esta estrategia, admitiendo que las dudas son evidentes, teniendo en cuenta las dificultades con las que se encuentra la UE para acordar posiciones comunes en áreas tan sensibles como esta. ¿Tiene la UE una estrategia de ciberseguridad correcta y operativa cuando no tiene una política exterior, de defensa o de inmigración verdaderamente común?

Partimos de una clara situación de desventaja: frente a estados centralizados no democráticos y con ausencia o duras limitaciones de derechos individuales, una comunidad política de derecho, como es la UE, que en diversas ocasiones se ha visto en dificultades para definir una política a seguir por todos sus miembros, cuenta con una posición de partida desventajosa, por su respeto a la diversidad y a la idiosincrasia propia de cada uno de sus estados miembros.

Ante la necesidad de una unidad de acción, de estrategia y decisión, durante la reunión extraordinaria del Consejo Europeo de octubre de 2020, los dirigentes de la UE instaron a mejorar la capacidad de la misma para protegerse contra las ciberamenazas, proporcionar un entorno de comunicación seguro y garantizar el acceso a los datos a efectos judiciales y policiales (Arauzo, 2020). En diciembre de 2020 la Comisión Europea y el Servicio Europeo de Acción Exterior presentaron la nueva Estrategia de Ciberseguridad de la UE, con el fin de reforzar la resiliencia de Europa frente a las ciberamenazas, incluyendo propuestas concretas para la implantación de instrumentos normativos, políticos y de inversión (Comisión Europea, 2020).

En definitiva, nos proponemos analizar la adecuación de esta estrategia a los retos cibernéticos actuales y futuros, para poder realizar una propuesta de mejora, con el fin de identificar qué elementos de la estrategia diseñada por la UE deberían ser modificados para que la misma sea más efectiva y viable. Esto es extremadamente útil

para todos los estados miembros, ya que "si no se controla adecuadamente el ciberespacio, desde allí puede ver una nación amenazada su libertad de acción y no tan sólo su cíberseguridad sino toda la Seguridad Nacional". (Feliú, 2012).

2) COMPRENDIENDO EL PAPEL DEL SISTEMA CIBERNÉTICO EN LAS RELACIONES INTERNACIONALES: ESTADO DE LA CUESTIÓN Y ELEMENTOS DE ANÁLISIS

2.1 Estado de la cuestión: El funcionamiento de las dinámicas del ciberespacio.

Debido a la novedad que han supuesto los rápidos avances tecnológicos y sus aplicaciones a prácticamente todas las áreas de la vida, las implicaciones en materia de seguridad son extensas. La conectividad digital puede verse como "una oportunidad para alterar las tradicionales distribuciones de poder y como un factor que contribuye a exacerbar las vulnerabilidades de estados y organizaciones" (Valeriano, et al., 2018).

El interés público sobre el cíberterrorismo y la utilización del dominio cibernético para conducir acciones dañinas nación a principios de la década de 1990, cuando se acuñó el término "ciberterrorismo" (Collin, 1997) y las definiciones de "netwar" y "cyberwar" (Arquilla et al., 1993). Sin embargo, para comprender las posibles implicaciones de la seguridad en el ciberespacio y su impacto en las relaciones internacionales debemos diferenciar una serie de conceptos que aparecen muchas veces confundidos en el lenguaje periodístico, no así en el lenguaje técnico

Entendemos el **ciberespacio** como "un dominio mundial en el ecosistema de la información, consistente en una red independiente de sistemas de redes de infraestructuras de servicios de información" (CSRC, 2021). Dentro de este espacio puede operar cualquier actor, estatal o no estatal, pueden ejercitar su poder en el ciberespacio. Pueden llevar a cabo ataques cibernéticos o cíberataques, actividades ilegales que persiguen fines económicos, políticos o personales (Aguilar et al, 2011).

Cuando se trata de actores privados sus acciones pueden causar daños en el dominio virtual, como la pérdida masiva de datos, o daños materiales, si por ejemplo se ataca una red eléctrica o una central nuclear. En el caso de actores estatales, se pueden llevar a cabo operaciones cibernéticas, realizadas por sus divisiones militares o mediante *proxys*

(actores no estatales contratados a un estado para realizar ataques u operaciones cibernéticas a su favor), las cuales buscan causar pérdidas económicas o materiales a otros actores estatales con quienes se mantienen divergencias u objetivos cibernéticos en conflicto.

También debemos analizar la **ciberguerra**. Cuando se produce una intervención dañina que puede poner en riesgo la red o los servicios que utilizan la red, el último escalón de hostilidad en este dominio virtual sería la cíberguerra, que tiene lugar cuando los ataques cibernéticos o las operaciones cibernéticas están organizadas, y alcanzan un umbral de hostilidad que supera el umbral de la fuerza tolerada por la comunidad internacional y definida por el DIH (Sigholm, 2013).

El ciberespacio es un campo que tratan de comprender un sinfín de actores, debido a los diversos campos a los que puede afectar, y los autores de referencia sobre la materia provienen de muy diversas áreas. En este sentido destaca especialmente el trabajo de Nazli Choucri, profesora de CC.PP del MIT, experta en RRII y economía política internacional enfocada hacia el ciberespacio, que ha centrado sus investigaciones en el campo de la ciberpolítica en RRII, y que junto con el profesor Robert C. North ha desarrollado la "Teoría de la Presión Lateral en las RRII", que mencionaremos nuevamente, y que trata sobre la extensión del comportamiento estatal fuera de los límites territoriales, cuando estos se ven integrados en una gama de redes (formales e informales) a través de las que interactúan con otros actores internacionales y las causas y consecuencias de este comportamiento. Su trabajo es muy relevante a la hora de analizar el uso del ciberespacio por actores estatales y no estatales con fines políticos y los nuevos modos en que los estados interactúan en este dominio y que se apartan de las tradicionales dinámicas de poder, lo que es necesario comprender para determinar el papel de la UE en este nuevo escenario e identificar cómo su Estrategia de Ciberseguridad debe adaptarse ante este escenario.

También debemos mencionar a Richard A. Clarke, el primer asesor *de facto* del gobierno de EE.UU en materia de cíberseguridad y autor de numerosas publicaciones y libros sobre la cíberguerra, incluyendo "The Fifth Domain", que afirma la inevitabilidad de reconocimiento el ciberespacio como quinto dominio de la guerra. Otro autor muy citado en este ámbito, P.W. Singer, reconocido especialista en dinámicas de conflicto en el siglo XXI, que es actualmente *strategy analyst* en Rand (un *think tank* que describiremos a continuación) y autor de "*Cybersecurity and Cyberwar: What Everyone*

Needs to Know", incluido en las listas de lecturas oficiales del Ejército de los EE.UU, trabajan estos conceptos diferenciando el tema general de ciberseguridad del problema concreto de la ciberguerra. Por último, cabe destacar a John Arquilla, que fue, como ya mencionamos, el primero en acuñar el término "netwar" y "cyberwar" (Arquilla, 1993) y ha promovido la idea de adaptar la estructura jerárquica militar actual hacia una estructura de red, adaptada a los retos que introducen estas nuevas formas de conflicto.

El conflicto cibernético se puede abordar desde perspectivas muy distintas. Todas ellas tratadas profusamente por la doctrina y la ciencia política. En primer lugar, es una cuestión emergente desde la perspectiva de las Relaciones Internacionales. De hecho la disciplina siempre estuvo relacionada con el examen teórico y ético en relación con la seguridad, independientemente del contexto donde dicha cuestión de seguridad se diera, e independientemente de dónde se diesen las situaciones de amenaza o riesgo, aunque con un problema recurrente. Según señala parte de la academia, la utilización de marcos teóricos antiguos es problemática cuando se aplica a estos nuevos métodos de interacción (Valeriano et al., 2018) ya que durante la década de 1990 la atención académica se centró en las potenciales consecuencias de esta tecnología (Domingo, 2015), sin comprender primero el dominio, su potencial coercitivo y su potencial uso por parte de diversos actores.

Muchos autores consideran que las actuales teorías de RR.II no pueden contribuir de forma efectiva al estudio del conflicto en el dominio cibernético (Kello, 2013). Sin embargo, la mayoría consideran que la teoría de las RR.II debería considerar la distinción entre qué es posible y qué es probable en el dominio cibernético, utilizando cálculos racionales, lo cual atemperará las predicciones alarmistas, muy comunes en el campo del conflicto cibernético (Gartzke, 2013).

Otros autores consideran útil la aplicación de la mencionada "Teoría de la presión lateral" de las RRII, al campo de la ciberseguridad, para predecir cómo estados con distintas características socioeconómicas y políticas pueden comportarse en el dominio digital, y las consecuencias de este comportamiento (Choucri, 2012).

Un marco del que parten múltiples expertos acerca de la ciberseguridad en relación con la Teoría de las Relaciones Internacionales es que "*the gates are down*" (las barreras están bajadas), y que en esta Cuarta Revolución Industrial el estado es incapaz de mantener su monopolio sobre la seguridad. Por esta razón, la utilización del método comparativo ha sido tan problemática, porque no se pueden extrapolar las ideas propias

de la seguridad en las relaciones internacionales, en contextos no físicos, sino virtuales, y en los que hay una incidencia tan alta de la tecnología en relación con todo tipo de contexto. Por eso, se suelen investigar eventos aislados y atípicos.

Otro marco teórico del que debemos partir es la conceptualización del cíberespacio desde una perspectiva estrictamente militar, naciendo el concepto de cíberguerra. Algunos autores opinan que la ciberguerra alterarán las dinámicas de interacción de los estados (Kello, 2013), argumentando otros que hay múltiples limitaciones para que los estados empleen todo su armamento cibernético. El ciberespacio es visto desde un punto de vista militar como un nuevo dominio de conflicto, que amplía y modifica las prácticas militares existentes, pero en el que se seguirán aplicando la planificación y el lenguaje operativo militar tradicional (Cornish, 2019).

Esta controversia alimenta el debate sobre si esta tecnología alterará la balanza de poder y favorecerá a pequeños estados, como Corea del Norte, que cada vez lleva a cabo operaciones cibernéticas sofisticadas y mantiene una estrategia asimétrica unificada, diseñada para presionar a la comunidad internacional en el espacio físico y en el espacio virtual (Raska, 2020).

Hay opiniones discrepantes, ya que otros autores opinan que los grandes poderes serán los que obtendrán un mayor beneficio de esta tecnología (Lindsay, 2013), ya que las armas cibernéticas son costosas y difíciles de utilizar (Maness et al., 2015).

Las corrientes más recientes señalan que enfocar los ataques cibernéticos como "amenazas" puede ser desastroso para el desarrollo de políticas efectivas (Guitton, 2013), ya que las amenazas suelen exagerarse, por lo que un gran número de autores aboga por un marco constructivista (Hansen et al., 2009) ya que la naturaleza de las ciberamenazas y las narrativas asociadas con esta cuestión en muchos casos son construcciones sociales, y una perspectiva errónea podría llevar a la securitización de Internet en sociedades libres.

Aunque el número de operaciones cibernéticas ha aumentado exponencialmente desde 2001, su severidad e impacto se ha mantenido constante y a un nivel relativamente bajo (Valeriano et al., 2014), lo que sugiere que el contexto es importante. Es lo que se ha denominado "enfoque ambientalista" (Langø, 2013). Esta corriente se basa en el análisis y la cuantificación de la ciberseguridad y de las ciberamenazas considerando el contexto en el que se producen. La perspectiva militar también se centra la evaluación

contextualizada de los nuevos escenarios bélicos y de las tecnologías utilizables para la defensa en el ciberespacio (Felíu et al., 2012). Algunos autores tratan de comprender cómo aplicar principios militares tradicionales, basados en entornos físicos a este nuevo dominio virtual (Dietz et al., 2012) con el fin de que no sea necesaria una reformulación completa de las estrategias militares, sino una adaptación al nuevo contexto. Pero diversos estados han optado por reenfocar por completo su política de defensa para adaptarla al ciberespacio (Ehl, 2018), aceptando no solo una transformación del contexto donde debe producirse la seguridad y las acciones de defensa, sino el contexto virtual como un dominio totalmente distinto del físico.

Desde la perspectiva de la CC.PP debemos introducir el concepto de **"ciberpolítica"**, un concepto que refleja la conjunción de dos realidades: las interacciones humanas que rodean la determinación sobre quién obtiene qué, cuando y donde, y la formación de espacios virtuales que tienen su propia realidad (Choucri, 2000). Se conoce por ciberpolítica al desarrollo de la política en los medios electrónicos a través de 3 ejes o herramientas de gobernanza: el gobierno electrónico; la comunicación política en internet y a través de las redes sociales; y la movilización política. Hay que tener en cuenta que la doctrina entiende la ciberpolítica no como una actividad exclusiva de los profesionales de la política, sino como un espacio de desarrollo de las capacidades del hombre como animal político, en la medida en que posibilita y alienta nuevas y más amplias formas de participación ciudadana. La ciberpolítica es, por tanto, la existencia de una nueva ágora digital unitaria pero tremendamente diferenciada pues permite formas de interacción entre el gobierno y los ciudadanos, entre éstos y los partidos políticos, entre las empresas y los órganos legislativos, entre ciudadanos de un régimen político y entre ciudadanos del mundo (Cotarelo, 2013).

Los primeros artículos académicos sobre la "ciberpolítica" se centraban en cómo el ciberespacio podría empoderar a actores no estatales, pero en la actualidad la mayoría de las investigaciones sobre cíberpolítica se centran en comprender cómo los estados se han convertido en actores ciberpolíticos, abandonando la perspectiva del ciberespacio como un ente separado del mundo real, ya que los estados lo utilizan para llevar a cabo sus interacciones, incluyendo sus interacciones físicas.

La actual literatura académica se centra en comprender las innumerables formas en que los estados buscan resistir y controlar la actividad ciberpolítica (Banta, 2020). Si bien definir los límites del control estatal sobre el ciberespacio es difícil, es urgente

identificar la intención y el efecto de sus acciones, y determinar quién tiene el poder de vigilar y categorizar el comportamiento de los estados y qué nivel de propiedad del dominio cibernético por parte de los estados es aceptable (Potter, 2018).

Los principales *think tanks* que tratan la materia se encuentran, como era esperable, en EE.UU, aunque debemos destacaremos el trabajo de otros *think tanks* internacionales que introducen una perspectiva más plural y más multilateral para comprender mejor el fenómeno en términos globales. En clave el trabajo de la Corporación Rand, creada como grupo de análisis de las Fuerzas Armadas de EE.UU y que actualmente asiste a otros gobiernos y OOII. Al estar especializada en cuestiones de defensa, ha publicado y desarrollado numerosos estudios sobre potenciales amenazas cibernéticas y sus implicaciones para la privacidad de personas e instituciones, y sus informes se reflejarán en este trabajo. Otro *think tank* digno de mención es el CSIS, cuyo departamento de ciberseguridad se centra en diseñar una estrategia de ciberseguridad nacional para EE.UU que tenga en consideración tanto las amenazas para la seguridad mundial como el respeto a la privacidad y las libertades civiles, por lo que es especialmente relevante para este trabajo. En España, el Real Instituto El Cano, publica desde hace varios años "CIBERelcano" un informe mensual en que se abordan todos los aspectos de las políticas de seguridad nacional e internacional, analizando aspectos de seguridad, regulación y gobernanza relacionados con el ciberespacio. Debido a que los avances en el dominio tecnológico se suceden con rapidez abrumadora, el hecho de que se analicen mensualmente cómo las dinámicas de poder se suceden en el dominio cibernético es gran utilidad para este trabajo.

En cuanto a publicaciones especializadas en cíberseguridad, podemos encontrar tanto revistas académicas como publicaciones especializadas de *think tanks*. "Journal of Cybersecurity" publica artículos de investigación relacionados con el dominio cibernético pero enfocado desde una serie de disciplinas alejadas de la informática, antropológicas, legales, psicológicas etc. Y cuenta con gran cantidad de artículos sobre ciberseguridad desde el enfoque de las CC.PP y RR.II, analizadas en este trabajo. El "The Journal of Cyber Security and Information Systems" analiza la cíberseguridad desde un enfoque técnico, pero que ayuda a comprender las últimas innovaciones, especialmente en instrumentos ofensivos cibernéticos, tipos de virus y *malware,* cuyo coste, desarrollo y disponibilidad contribuye a comprender las capacidades armamentísticas cibernéticas. También son relevantes para este trabajo las publicaciones

del "Cybersecurity Skills Journal" publicadas por el "National Cyberwatch Center", un consorcio de instituciones educativas, empresas y agencias gubernamentales que trabajan para fortalecer la defensa cibernética nacional de EE.UU. También hay que resaltar el importante papel de "CIBERelcano", que, como mencionamos permite una adaptación rápida ante los retos cibernéticos. Asimismo, es destacable la revista "Cloud Computing", que publica constantemente actualizaciones sobre las amenazas más recientes que aparecen en el espacio cibernético y realizan análisis profundos sobre la efectividad de las distintas medidas de ciberseguridad ante amenazas nuevas. Por último debemos destacar el importante papel de la serie de monografías que publica anualmente el Centro Superior de Estudios de la Defensa Nacional del Ministerio de Defensa, algunas de las cuales se centran en materia de ciberseguridad, y que desarrollan, de la mano de distintos expertos, estrategias a seguir por los actores estatales en el ciberespacio, evaluaciones de conflicto en el escenario cibernético y capacidades de defensa en el ciberespacio.

2.2 Necesidad de adaptación de las estrategias de defensa por parte de los Estados y Organizaciones Internacionales: Objetivos del trabajo

Debido al rápido cambio que experimenta el dominio cibernético y su prematura edad, hay muchas preguntas relativas al papel que juegan estos nuevos espacios cibernéticos en las dinámicas de poder de los estados. Si el ciberespacio se ha convertido en el nuevo foro a través del cual se desarrollan las relaciones humanas en todos los ámbitos, es comprensible que el Estado quiera organizar dichas relaciones, respetando los mismos principios políticos que rigen en los foros físicos; principios como el respeto a los derechos humanos, al Estado de derecho o al imperio de la Ley, que ordenan la vida en sociedad en el mundo *off-line*. Es lógico también, que este nuevo espacio se haya convertido en una de las áreas donde se produce la lucha por el poder o la disputa por el control de las influencias sociales. Consecuentemente, los estados y las organizaciones estatales deben velar por asegurar que en dichos espacios las relaciones humanas se produzcan con plena garantía, al igual que lo hacen en los espacios físicos. La ciberpolítica, la ciberseguridad y la ciberguerra son por lo tanto, fenómenos consecuencia de la evolución cibernética y tecnológica que se ha producido en los últimos 30 años, y de las nuevas fórmulas de relación humana en el espacio virtual.

Por todo ello, consideramos esencial para este trabajo analizar la ciberseguridad a partir del análisis de la ciberpolítica, para comprender las principales características de la guerra cibernética, incluyendo los diversos problemas que plantea: atribución del adversario, asimetría, convergencia física-cibernética y el problema de su falta de regulación en el Derecho Internacional Humanitario. También debemos comprender hasta qué punto va a cambiar la forma en la que analizamos a nuestros enemigos, qué clase de desafíos pueden encontrar los estados y cuáles son las estrategias más efectivas para adaptarse a la creciente importancia de este dominio. Analizaremos los tipos de ataques cibernéticos que podemos encontrar y los actores implicados, cuestionando si el papel de los actores no estatales es tan significativo cómo se concibe generalmente o si los actores estatales son los que tienen mayor capacidad de ofensiva cibernética.

Cómo el principal objetivo de este trabajo es comprender la amenaza que representa la guerra cibernética y analizar cómo la Estrategia de Cíberseguridad de la UE debería ser adaptada, se utilizará una comparativa de las estrategias de estados con amplia tradición en este campo y que han invertido una gran cantidad de recursos en sus programas de cíberdefensa. Por último, para completar el estudio analizaremos otras herramientas de defensa relativamente inexploradas, como la importancia de la "cíberdiplomacia" y la necesidad de incluir al sector privado como colaborador necesario para garantizar la eficacia de una buena ciberseguridad pública.

2.3 Planteamientos de análisis: Hipótesis y metodología.

El dominio cibernético se ha convertido en el quinto dominio de la guerra y debemos comprender cómo debemos adaptar la Estrategia de Cíberseguridad de la UE para hacer frente a los diversos retos que se plantean para los estados. Utilizaremos el método comparativo para probar esta hipótesis, a través de la comparación sistemática de casos en un análisis que en su mayoría se aplica con fines de generalización empírica y con verificación de hipótesis (Reyes, 2009). Los fines del análisis comparativo se persiguen, en este caso, haciendo uso de un método científico-social de control y ordenación de la complejidad observada. En este trabajo realizamos un estudio de un número reducido de casos (únicamente tres), con un grado medio de información entre ellos (Reyes, 2009). Según los fines de esta investigación, el tipo de comparativa será tanto universalizadora como *variation finding*, ya que trataremos de buscar pautas generales efectivas estudiando todos los casos pero también encontrando condiciones de variación, es decir,

objetivos o medidas que son introducidas en tan sólo uno o dos de los casos, y cuya aplicación a los otros fuese útil (Tilly, 1984). En base a la comparabilidad atribuida a los casos y a la especificidad respecto a los demás, nuestro estudio se concentra en la especificidad de las estrategias de estos tres países y sus diferencias entre ellas (Elder, 1976). Según el nivel de análisis e inferencia, realizamos un análisis a nivel individual, observando las relaciones dentro del sistema cibernético, utilizando como unidades de observación y análisis a los diferentes actores que operan dentro de este dominio, tratando de adecuar el análisis de las estrategias de ciberseguridad y nuestra propuesta a esta realidad (Przeworski et al, 1970), adecuando nuestro análisis a tratar de realizar lo que se conoce como una "ilustración comparativa sistemática" (Smellser, 1976).

Hemos decidido comparar la Estrategia de Cíberseguridad de la UE únicamente con esos dos planes nacionales porque se ha considerado preferible tomar como criterio de comparación aquellas estrategias valoradas por la doctrina como de mayor calidad que coinciden con políticas de seguridad de estados han invertido muchos recursos públicos en este campo. En definitiva, se ha preferido realizar una comparación intensiva de las estrategias, sus contenidos y su capacidad de adaptación ante los rápidos cambios que observamos en el uso del ciberespacio, para comprender la mejor forma de adaptar la Estrategia de Cíberseguridad de la UE a los sistemas más avanzados del mundo, y que en la actualidad marcan las tendencias políticas del futuro. Es una comparación múltiple entre los tres casos, todos parecidos, para resaltar los puntos comunes fuertes de todos ellos que pueden aplicarse a la estrategia de la UE e identificar si alguno de alguna estrategia particular es especialmente eficaz para considerar su aplicación en la UE.

Por lo tanto, la comparativa será horizontal y simultánea entre estas estrategias, para comprender las distintas formas de actuación y organización de la defensa cibernética en un estado y considerar cuales pueden ser aplicables para hacer más efectiva la Estrategia de Cíberseguridad de la UE. Se centrará en realizar un análisis integrado sobre qué clase de enseñanzas debería la UE, entendida como "comunidad política de derecho constituida en régimen sui géneris de organización internacional nacida para propiciar y acoger la integración y gobernanza en común de los Estados y los pueblos de Europa" (Díez-Picazo, 2008) aplicar. El análisis integrado ayudará a comprender cómo extrapolar elementos que podrían ser de utilidad para proteger el ciberespacio de la UE, y los ciudadanos, empresas y organizaciones gubernamentales de sus países.

2.4 Marco temporal y geográfico: Contextualización y origen de los conflictos en el ciberespacio.

En cuanto al encuadre temporal del que vamos a partir, el trabajo se va a centrar en el periodo de tiempo desde 2015 hasta 2020, porque es entonces cuando fue publicada la Estrategia de Cíberseguridad de la UE.

Utilizaremos un enfoque sincrónico, ya que nos centraremos en el estado actual del ciberespacio y en las amenazas actuales contra las que deben lidiar los estados en dicho dominio, tanto de actores estatales, como no estatales que utilizan el ciberespacio para lograr sus fines económicos, comerciales o de influencia, así como los tipos de ataques que pueden realizar.

Consideramos que este enfoque es el más adecuado porque la propuesta de una nueva Estrategia de Cíberseguridad de la UE debe adaptarse al estado del ciberespacio actual, teniendo en cuenta la velocidad exponencial a la que van produciéndose los cambios tecnológicos en este campo.

A la vez debemos basarnos en el análisis de las tendencias futuras, que han identificado los expertos como posibles riesgos cibernéticos, como la próxima introducción generalizada del 5G (Arteaga, 2021) para que las propuestas que hagamos permitan a la Estrategia de la UE funcionar en el futuro. Sería poco viable y realista esperar que estos planes se actualizasen anualmente, y pretendemos que cualquier idea que expongamos pueda sea efectiva durante al menos 5 años, que es el tiempo en el que se volverá a revisar y actualizar la estrategia anterior.

También hay que tener en consideración que las Estrategias de Ciberseguridad que analizaremos datan del periodo de tiempo comprendido en este trabajo: la de Corea del Sur data de diciembre de 2019 y la de EE.UU fue establecida para un periodo de cinco años (2018-2023), aunque se espera que sufra modificaciones una vez finalizado el mandato del Presidente Trump y habiendo entrado una nueva administración con el Presidente Biden en la Casa Blanca.

El marco temporal escogido es clave para este estudio porque debido a la rápida evolución de las TIC debemos centrarnos en el estado más reciente de la tecnología, considerando los retos y amenazas identificadas en los últimos años y los avances más recientes en este campo. Centrarnos en un marco temporal más extenso carecería de utilidad ya que el salto cuantitativo y cualitativo tecnológico hasta el presente sería

demasiado amplio para realizar un estudio profundo sobre los problemas que rodean al ciberespacio en la actualidad, y es más conveniente centrarse en el estado actual de la tecnología e investigar sus implicaciones futuras que analizar todos los desarrollos tecnológicos que han tenido lugar durante un periodo más extenso de tiempo. Por esto centramos el marco en el periodo 2015-2020, comprendiendo los últimos avances tecnológicos que pueden suscitar diversas cuestiones en el panorama internacional actual, emitiendo recomendaciones en consecuencia. Desde 2015 la actividad en el dominio cibernético de los actores estatales ha aumentado significativamente, en comparación con el periodo 2010-2015, aumentando los incidentes diplomáticos relacionados con esta materia (CSIS, 2020), por lo que, a fin de comprender la ciberguerra, debemos centrarnos en el marco temporal en que los actores estatales han comenzado a considerar y utilizar el dominio cibernético más extensamente.

En cuanto al marco geográfico escogido, lo fijamos en la UE, en EE.UU y en Corea del Sur, cuyas estrategias en materia de ciberseguridad analizaremos.

Hemos escogido estos dos países porque son identificados en la propia estrategia de la UE como países afines, con los que se tratará de aumentar la cooperación en materia de ciberseguridad, ya que comparten y promueven una serie de valores comunes en el espacio cibernético: la protección a los DDHH y la promoción de un ciberespacio global, abierto, libre y seguro. Ambos países son potenciales aliados de la UE y es conveniente analizar sus estrategias de ciberseguridad porque compartirán los valores sobre los que se sustenta la Estrategia de Ciberseguridad de la UE pero ofrecerán un punto de vista distinto, conteniendo elementos operativos novedosos que pueden ser extrapolables a la UE para lograr de manera más efectiva estos objetivos comunes. Asimismo, ambos países cuentan con una amplia tradición en materia de ciberseguridad, ya que, debido a su posición internacional como primera potencia mundial (McNeil, 2019) EE.UU es objeto constante de múltiples amenazas cibernéticas, mientras que Corea del Sur lleva recibiendo ataques cibernéticos de Corea del Norte semanalmente desde 2014 (Park, 2016), por lo que centran gran parte de su estrategia en técnicas defensivas, lo cual es extremadamente importante para la UE teniendo en cuenta que en los últimos años se ha señalado que ha aumentado en un 70% su riesgo de sufrir próximamente un ataque cibernético que afecte a la Infraestructura Crítica de varios EM (ENISA, 2020). La amplia tradición defensiva de estas potencias puede aportar a la UE directrices sobre cómo enfocar esta difícil cuestión.

2.5 Contemplando los conflictos en el dominio cibernético desde un enfoque realista

El realismo es un marco teórico dominante en el campo de las RR.II y se basa en asunciones generales sobre la política internacional: que los estados son los actores internacionales más importantes, que operan de forma independiente en un sistema internacional sin una autoridad centralizada, persiguiendo sus propios fines (Schmidt, 2002). Las teorías realistas sobre disuasión y conflicto pueden ser utilizadas en nuestro trabajo para comprender si el ciberespacio es un campo estable o inestable, si las tecnologías cibernéticas serán una nueva fuente de conflicto o contribuirán a que éste sea menos destructivo; y si los estados comenzarán una carrera armamentística cibernética, lo que nos ofrece la oportunidad de evaluar el papel de esta teoría de RRII y su aplicación en este campo.

La anarquía es la asunción fundamental en las teorías estructurales realistas y se refiere a la falta de autoridad para controlar el sistema internacional, lo cual genera desconfianza entre estados (Waltz, 1979) y fuerza a los estados a depender de sus propias capacidades para perseguir o proteger sus propios intereses. La anarquía es una de las principales características del ciberespacio, que carece de cualquier tipo de gobernanza institucional, pues no hay ninguna OOII relacionada con esta materia que cuente con inspecciones de inspección, sanción o resolución de conflictos.

El realismo también contribuye a explicar la carrera armamentística cibernética como una respuesta a las amenazas en este sistema anárquico (Jervis, 1978), ya que el "dilema de seguridad" se vuelve más intenso cuando las capacidades ofensivas y defensivas son indistinguibles-; lo cual sucede en el ciberespacio. Cuando las organizaciones cibermilitares aumentan su presupuesto no se conoce si invierten en capacidad ofensiva o defensiva, lo que aumenta la incertidumbre y la competición entre estados en la carrera armamentística cibernética (Craig et al., 2018).

El concepto de las dinámicas de poder es central al realismo porque gracias a esta explicación teórica podemos entender de qué forma se asegura la independencia y supervivencia del estado (Mearsheimer, 2006).

Los realistas equiparan el poder de un estado a los recursos, capacidad industrial, capacidad militar y población que el estado posee (Morgenthau, 1948) y la forma

distribución de estas capacidades -en términos globales- entre estados tiene implicaciones para la estabilidad del sistema internacional. El cíberpoder, que es definido como "la habilidad para obtener los resultados deseados a través del uso de recursos consistentes en información electrónica interconectada que hallamos en el dominio cibernético" (Nye, 2010), depende también de los recursos y de las capacidades que despliegan los estados y otros agentes (privados y públicos) en el ciberespacio; y aunque actualmente no existe ninguna teoría en la literatura realista sobre el uso del cíberpoder, lo cierto es que es un marco útil para comprender como se producen las nuevas relaciones entre estados y como se distribuyen estas nuevas fórmulas de poder entre ellos. Hay que tener en cuenta que las capacidades y recursos del mundo cibernético tienen un bajo coste de entrada, y por ello, estados tradicionalmente más débiles pueden desafiar a estados más poderosos (Lango, 2016) en el mundo on line. Aun así, es controversial la teoría de que el ciberespacio alterará completamente las dinámicas de poder, aumentando las vulnerabilidades de estados con fuerte dependencia en la infraestructura digital (Kolet, 2001), ya que otros autores argumentan que sólo las superpotencias tecnológicas desarrollarán las cíberarmas más sofisticadas, como ocurre de hecho en el mundo no virtual, sugiriendo que la naturaleza asimétrica de estos conflictos ha sido exagerada (Lindsay, 2013) y que la distribución de poder entre grandes y pequeños terminará siendo muy parecida a la del mundo físico.

En definitiva, consideramos que la aplicación al análisis de este trabajo de las teorías del realismo, que se centra en cuestiones de seguridad nacional y dinámicas de poder, nos permitirá obtener un marco relevante de referencia para comprender los problemas de seguridad que plantea el dominio cibernético. En conclusión se puede afirmar que el dominio cibernético es realista; de naturaleza anárquica; con una falta de instituciones de gobernanza; donde los estados temen las posibles capacidades de otros estados y actores internacionales, y, en consecuencia, desarrollan sus capacidades cibernéticas, tanto ofensivas como defensivas.

3) EL CIBERESPACIO COMO "EL QUINTO DOMINIO DE LA GUERRA"

3.1 Conceptos principales sobre la cuestión. Las dinámicas de poder.

Entendemos la guerra como un conflicto armado, llevado a cabo entre estados, gobiernos, sociedades o grupos paramilitares como mercenarios, insurgentes y milicias

(Beer, 2001). La guerra se ha llevado a cabo tradicionalmente con una serie de barreras temporales y geográficas y una serie de objetivos específicos, que o eran conquistados o abandonados. Estos conflictos se llevaban a cabo en terrenos identificables: tierra, mar, aire y, desde hace unos 20 años, en el espacio (Benedict, 2012), como ya mencionamos. Se consideraba que un estado estaba en guerra cuando realizaba una declaración formal mediante un documento, proveniente de un Estado hacia otro, donde el primero declaraba el inicio de hostilidades (Boisen, 2020). El crecimiento de Internet, y su naturaleza expansiva han abierto un nuevo terreno para la guerra, cuya característica esencial es que no está delimitado, no tiene fronteras tradicionales y por lo tanto, no obedece a las normas ni a las reglas de funcionamiento que se han venido aplicando al mundo físico. No es fácilmente aplicable el concepto de "estado de guerra" a los conflictos en el ciberespacio, ya que no se suele realizar una declaración formal como tal, sino que cualquier actor puede atacar de forma continua a otro, como veremos en el caso de Corea del Norte, que explicaré detalladamente más adelante, que lleva varios años realizando ataques continuos a Corea del Sur, los cuales no reconoce y realiza por medio de actores no estatales que colaboran con el gobierno norcoreano. Asimismo, las peculiares características que diferencian al dominio cibernético del resto de dominios en los que se ha llevado a cabo tradicionalmente la guerra, hacen que no sean extrapolables los elementos diferenciadores de la guerra en cada uno de estos dominios tradicionales al dominio cibernético. Algunos expertos han llegado a afirmar que aún no es definible una guerra en el espacio cibernético, pues aún no se sabe cómo se llevaría a cabo, cómo y cuándo estallaría una guerra cibernética como tal y cuáles serían sus consecuencias (Schneier, 2003).

Para comprender correctamente la guerra en el ámbito cibernético debemos entender primero qué implica el **"cíberpoder"**.

Como mencionamos en la introducción "el poder basado en la posesión de información no es nuevo, pero el cíberpoder lo es" (Nye, 2010). Por lo tanto, ciberpoder no equivale a poseer información solamente. El cíberpoder es la habilidad para utilizar el ciberespacio para crear ventajas comparativas en propio beneficio e influenciar en otros entornos operacionales, sociales, empresariales, económicos y políticos a través del uso de instrumentos tecnológicos de poder, ya sean estos tradicionales o fruto de la innovación (Kuehl, 2009). Resulta interesante analizar cómo se ha ido construyendo esta definición, para entender los distintos aspectos de la misma. Debemos comprender

que el ciberespacio es un espacio operacional, donde cualquier actor estatal o no estatal lleva a cabo acciones que provocan efectos, que pueden verse reflejados en el propio dominio cibernético o en otros dominios. Este esfuerzo por influenciar, ya sea a un individuo, una organización o a una sociedad entera, convierte al ciberespacio en un medio operacional, en el que se lleva a cabo influencia estratégica. Al ser el ciberespacio un dominio tecnológico, completamente distinto a un dominio físico, hace que se puedan llevar a cabo dicha influencia de forma distinta a los dominios tradicionales, y también expande el número de actores que pueden actuar en el mismo. Por último, también considera cómo el modo en que el ciberespacio ha modificado la creación, almacenaje y modificación de información ha transformado la forma en que los actores utilizan sus instrumentos de poder, influenciando todo tipo de entornos.

El ciberpoder puede ser utilizado para obtener los resultados deseados dentro del ciberespacio o para producir los resultados deseados en otros dominios exteriores al ciberespacio. Desde un punto de vista estratégico, las definiciones tienen poca importancia, porque "lo que en realidad más importa es percibir la esfera de información como un lugar que existe, comprender su naturaleza y considerarla como algo que puede ser manipulado y usado como una ventaja estratégica". Por lo tanto, lo que define el ciberpoder es la consideración del espacio cibernético como una esfera de información, donde se producen relaciones humanas, que puede ser manipulado por aquellos que quieren ejercer su control, para usarlo en su beneficio como una ventaja frente a los demás y sus intereses (Lonsdale, 2004).

Lo importante es que, una vez reconocido este nuevo ámbito, podemos entender que el conflicto y las dinámicas de poder que se producen en este dominio son distintos a los que se producían en dominios tradicionales. Los estados concebían la seguridad en los cuatro dominios operacionales tradicionales (mar, aire, tierra y más adelante, espacio), llevando a cabo operaciones militares para salvaguardar su seguridad en estos dominios. El medio terrestre requiere unos medios concretos y específicos para el tansporte y movimiento de fuerzas, y el empleo de las fuerzas terrestres se basa en el movimiento, un adecuado reconocimiento previo, la búsqueda de una posición ventajosa, y la sorpresa (Feliú et al., 2012). El medio marítimo tambien presenta características únicas, siendo necesario unos medios específicos para el movimiento sobre o bajo la superficie del medio acuático, y el empleo de las fuerzas marítimas se rige por iguales principios al medio terrestre, movimiento, reconocimiento previo, posición ventajosa y sorpresa. En

cuanto al dominio aéreo, presenta unas características únicas y diferenciadas, como el empleo de las tres dimensiones, y una mayor velocidad de actuación que en los demás dominios, requiriendo el combate en el aire medios totalmente diferentes y tácticas y procedimientos específicos (Feliú et al., 2012). En cuanto al dominio espacial, la utilización real de armamento en el espacio es- por lo poco que se sabe, porque es información guardada con mucho celo- bastante reducida. Sólo los estados que tienen fuerzas y medios para poder combatir viablemente en el espacio, muy pocos debido a los altos costes que supone, lo han contemplado como un escenario de conflicto. Estos cuatro dominios presentan características comunes: las actividades de defensa u ofensiva se llevan a cabo en un escenario físico único y diferenciado, requieren la utilización de medios específicos para moverse, desenvolverse y combatir en él, disponen de técnicas y tácticas de combate adecuados al medio concreto en que se desenvuelven y el factor humano es imprescindible para el combate. Sin embargo, el "Quinto Dominio", el ciberespacio, que se ha hecho tan crítico como la tierra, el mar, el aire y el espacio (Feliú et al., 2012), es también un espacio único y diferenciado, que requiere medios específicos para moverse, desenvolverse y entrar en combate en él y el factor humano es también determinante. Sin embargo tiene algunas características diferenciadoras: es un dominio no delimitado físicamente, y en constante evolución, las armas utilizadas son armas cinéticas, los actores son diversos y su principal valor, la información, es verdaderamente inmaterial.

En conclusión, se puede decir que las dinámicas de poder en el caso del ciberespacio son distintas de las existentes en los dominios tradicionales de la guerra, por lo que debemos comprender las características y dinámicas de este dominio y sus implicaciones, con el fin de identificar qué elementos debe incorporar una estrategia de ciberseguridad y de qué forma, con el fin de que sean efectivos.

3.2 Comprendiendo las dinámicas de la guerra cibernética

3.2.1 La complejidad de un dominio infinito y la convergencia tecnológica.

Uno de los principales problemas que encontramos en este 5º dominio de la guerra es su gran tamaño y compleja estructura. El rápido crecimiento exponencial del dominio informático, habiendo en 2020 30 mil millones de dispositivos conectados a Internet (Maayan, 2020), provoca una infinita cantidad de interacciones. A esto hay que sumar la convergencia tecnológica actual, ya que la tecnología se ha integrado en un número de

plataformas cada vez menor con el propósito de mayor eficiencia y conveniencia. El concentrar altísimas cantidades de datos de todo tipo en *Smartphones,* es arriesgado, ya que en caso de sufrir un borrado completo de datos, las pérdidas económicas y personales serían enormes. El elemento de convergencia también implica que las vulnerabilidades en programas de ordenador que controlan el funcionamiento de lugares físicos, como los SCI, puedan extenderse y tener serias repercusiones- debido a la convergencia, una vulnerabilidad virtual se vuelve análoga a una vulnerabilidad física (Chang, 2012). La adaptación e integración del IoT ha difuminado las funciones de la cíberseguridad y la seguridad física. Por ejemplo, en 2017, el grupo *hacker* "Lázarus" lanzó el virus informático "Wannacry", que infectó más de 232,000 ordenadores en 150 países (Jones, 2017) que no habían instalado la última actualización de seguridad de Microsoft. El sistema digital del NHS de Reino Unido se paralizó, miles de carpetas conteniendo información clínica desaparecieron y todos los ordenadores, máquinas refrigeradoras y escáneres MRI se apagaron. Aunque no hubo que lamentar ninguna víctima porque se logró paralizar el ataque rápidamente, si hubiese tenido lugar durante una pandemia mundial las consecuencias podrían haber sido distintas, por lo que no debemos subestimar su peligro.

Por lo tanto, la complejidad de un dominio infinito y la convergencia tecnológica implican que las estrategias aplicables deben decidirse tomando en consideración los cambios que puede experimentar el mismo, y debe tomarse en consideración la protección de infraestructuras críticas, ya que sus vulnerabilidades aumentan exponencialmente debido a la convergencia tecnológica. Además de esto, también es necesario tener en cuenta cómo identificar las amenazas y capacidades ofensivas de los actores que interactúan en este dominio, con el fin de que las estrategias de ciberseguridad consideren de forma efectiva las diversas amenazas que se pueden experimentar.

3.2.2 Midiendo la capacidad ofensiva cibernética: elementos de coerción y disuasión

A pesar de que cada vez más estados y actores internacionales actúan en el dominio cibernético, medir sus capacidades en dicho ámbito es problemático (IISS, 2014). Entendemos la coerción en las relaciones interestatales como el uso del gobierno de un estado de algún tipo de presión (como amenazas, intimidación o el uso de la fuerza) para obligar al gobierno de otro Estado a que actúe de una determinada manera (Joyner,

2006). La idea de que los ataques cibernéticos son más baratos, fáciles de ejecutar, y efectivos, los han convertido en una estrategia coercitiva prevalente para muchos actores internacionales.

Entendemos la disuasión como "disuadir al adversario de emprender una acción por el temor a que sus costes excedan los posibles beneficios" (Nye, 2017). La disuasión en el ciberespacio implica mecanismos complejos, y las amenazas disuasorias no tienen por qué limitarse a respuestas en el dominio cibernético. Hay dos principales métodos de disuasión en el ciberespacio: amenaza de castigo y negación (Nye, 2017). En cuanto a las amenazas de castigo, aunque muchos estados optan por estrategias cíber-kinéticas, como se puede observar en la estrategia seguida por el Pentágono (Friedman et al., 2014), que consiste en que el "castigo" se lleve a cabo a través de otro dominio donde las consecuencias sean más evidentes. La negación es la forma de disuasión más utilizada, ya que se basa en aumentar la resiliencia para que el estado se pueda recuperar rápidamente de un cíber ataque de forma que se reduzcan los incentivos de ataque para el adversario, porque el mismo sea fútil. Unas buenas defensas cibernéticas "pueden eliminar la mayoría de potenciales ataques de actores que cuenten con medios no muy sofisticados" (Zetter, 2009). La disuasión depende de percepciones y las diferentes partes de una organización compleja pueden percibir las mismas acciones (en cuanto a costes y beneficios) desde perspectivas muy diferentes, y lo que se considera un riesgo asumible puede variar, por lo que se deben invertir recursos en analizar en profundidad a toda potencial amenaza (Demchak et al., 2015) con el fin de que las técnicas de disuasión empleadas sean efectivas.

Por todo ello, cualquier diseño estratégico de ciberseguridad deberá tener en cuenta la capacidad ofensiva cibernética y determinar los elementos de coerción y disuasión existentes, para que incrementen el nivel de resiliencia de los sectores públicos y privados críticos y ofrezcan una protección efectiva. Sin embargo, también es importante identificar de donde pueden provenir las amenazas, que no están limitadas únicamente a actores estatales, ya que cualquier actor puede tener acceso al dominio cibernético y utilizarlo para lograr sus fines, por lo que debemos analizar cómo desarrollar la capacidad de atribución de ataques cibernéticos.

3.2.3 La asimetría y el problema de la atribución

La cíberguerra es un conflicto inherentemente asimétrico, ya que, debido a las características del ciberespacio, resulta posible que un actor con recursos limitados

pueda enfrentarse a un actor más poderoso. Debido que el dominio cibernético fue creado artificialmente con un diseño abierto para facilitar su uso por todo tipo de usuarios, mantener una defensa impenetrable es más difícil y costoso que llevar a cabo una ofensiva. Asimismo, las armas cibernéticas costosas y de gran complejidad técnica desarrolladas por un gobierno pueden ser repelidas y transformadas y adaptadas para contraatacar por otros actores. La asimetría en este "Quinto Dominio" favorece a "actores pequeños y ágiles, difícilmente localizables, lo cual es un punto clave que debe comprenderse para adoptar estrategias de mitigación efectivas" (Chang, 2012). Las grandes potencias con altos niveles de desarrollo, como EE.UU y la mayoría de estados occidentales tienen una fuerte dependencia cibernética, lo cual las hace "particularmente vulnerables a cíberataques asimétricos, ya que probablemente EE.UU sería disuadida de iniciar un ataque cibernético a gran escala por el temor a las represalias en sus redes cibernéticas" (Clark et al., 2010).

El problema de la atribución consiste en "atribuir la responsabilidad de un ataque cibernético a un actor o un grupo de actores, desvelando su identidad real" (Saalbach, 2019). La atribución a un actor de un ataque informático es problemática, ya que unas líneas de código maligno pueden ser escritas originalmente por un actor o adquiridas en Internet. Para identificar quien es responsable de un ataque cibernético es necesaria una investigación para analizar los aspectos humanos de la operación, el desarrollo del ataque, los recursos invertidos en el mismo y una comprensión contexto geopolítico que lo rodea, lo que convierte la cíber-atribución en un juicio político basado en información técnica y estratégica. Debemos también distinguir asignar un ataque cibernético a un adversario específico, y luego enlazar a este adversario con un actor estatal o no estatal, la "auténtica atribución" (Lee, 2016). La atribución auténtica estatal es problemática ya que es complicado determinar la relación entre un individuo o un grupo de individuos con un estado, si han sido contratados por un gobierno, se hallan vagamente vinculados al mismo pero otorgó ningún tipo de beneplácito ante la realización de este ataque cibernético o si operan en base a sus convicciones ideológicas y políticas.

En conclusión, debemos considerar el desarrollo de las capacidades de atribución e identificación de amenazas, ya que es vital comprender cuales son las amenazas a las que nos enfrentamos a la hora de diseñar una estrategia de ciberseguridad que sea efectiva, ya que, debido a las características del dominio cibernético resulta

especialmente difícil comprender las verdaderas capacidades de los distintos actores que operan en este dominio, sus capacidades, motivos, objetivos y su estrategia operacional.

3.3 Convergencia física-cibernética y el concepto de guerra híbrida

Tras desarrollar estos elementos de análisis, debemos comprender cómo se llevaría a cabo una guerra en el dominio cibernético. Las fuerzas militares actuales deben explotar todas las ventajas que pueda aportar el genio tecnológico, pero diversos expertos argumentan que los principales ingredientes de la victoria militar continuarán reflejando la naturaleza de la guerra en la misma medida que los eventuales medios empleados en la consecución de la misma (Van Riper, 1997). Debemos considerar la guerra como una lucha de voluntades, no de máquinas, en la que los medios han de estar subordinados a los fines si los resultados tienen que justificar los costes. Debido a la complejidad del dominio cibernético y a nuestro mundo globalizado, los fines perseguidos serán probablemente más complicados, y las circunstancias en las que son perseguidos, menos predecibles que nunca anteriormente en la historia. Los actores estatales deben adaptarse y ser capaces de combatir en cualquier campo de batalla, bajo cualquier condición y con los medios que la naturaleza de la contienda exija (Van Riper, 1997), así como los actores no estatales también deben comprender de qué forma pueden verse envueltos en conflicto en este dominio.

Por lo tanto, la habilidad para integrar el dominio cibernético en un marco operativo más amplio es necesaria para entender su importancia (Chang, 2017). En los últimos años "han aumentado los incidentes kinéticos, en que los cíber-ataques causan daño físico directo o indirecto mediante la explotación de sistemas de información vulnerables, como los ataques la infraestructura o la industria de un país, con la interrupción total o parcial de ciertos servicios" (Applegate, 2013). Esto es un ejemplo de la "guerra híbrida", en la que "los adversarios controlan y emplean una serie de diferentes herramientas para lograr sus objetivos" (Pawlak, 2015). El dominio cibernético es adecuado para la realización de una guerra híbrida, debido al problema de la atribución, ya que los estados pueden llevar a cabo ofensivas con un menor riesgo político, utilizando "proxys" (Chang, 2017) y el DIH en relación a los ataques cibernéticos sigue siendo una "zona gris", lo que les da libertad operativa.

Hay una necesidad de reorganización, ya que esta expansión del campo de batalla requiere una compleja comprensión y la planificación sinérgica adaptada a las nuevas tecnologías (Danyk. et al., 2017). La ventaja estratégica la tendrá el actor que pueda implementar sistemas tecnológicos avanzados para aumentar la efectividad de su potencial militar existente y logre multiplicar sus capacidades. El Parlamento Europeo presentó en 2015 un documento de trabajo explicando la necesidad de un "enfoque integral", concluyendo que eran necesarias "estrategias gubernamentales a nivel estatal que aumentasen la resiliencia de un país ante ataques híbridos, que los recursos dedicados a luchar contra estos ataques pudiesen ser utilizados tanto por gobiernos, como empresas, la sociedad civil y el sector privado, el diseño de marcos legales para hacer frente a este problema, y adaptar las instituciones estatales existentes para hacer frente a la guerra híbrida" (Pawlak, 2015).

3.3.1 La cíberguerra y el Derecho Internacional Humanitario

Uno de los principales problemas al que nos enfrentamos en cuanto al dominio cibernético es su falta de regulación en el DIH. A pesar de los intentos por crear un marco legal internacional sobre la materia, ninguno ha sido aceptado por un número significativo de actores. En el ámbito ciberespacial se aplican la Carta de la ONU y los demás principios derivados de la soberanía estatal (Tsagourias, 2015), pero debido a las características de este dominio las normas consuetudinarias sobre la responsabilidad internacional del Estado no resultan adecuadas. El Manual de Tallin (publicado en 2013 y realizado por un comité de expertos del CCDCOE) es un documento no vinculante, pero útil en cuanto analiza la aplicación del DIH y el *ius ad bellum* a los ataques cibernéticos y, pese a no ser un instrumento jurídico obligatorio, se adoptó en el seno de la OTAN, organización neurálgica para facilitar la cooperación internacional en ciberseguridad (Cocchini, 2021). Observa que el DIH resultaría aplicable en el caso de que un ataque cibernético equivaliese a un conflicto armado, causando daños severos a propiedad privada y la muerte de seres humanos. Reino Unido (NNUU, 2004), Australia (NNUU, 2011) y China (Zhang, 2012) han declarado que consideran el DIH aplicable a los ataques cibernéticos cuando sus consecuencias son las equivalentes al conflicto armado, pero aun así hay una falta de previsiones en el DIH que lo hagan aplicable a los ciberataques. A esto se suma la dificultad de atribución, de probar quien es responsable de un ataque o su conexión con el actor estatal que lo utiliza como "proxy". Desde el "Real Instituto El Cano" se ha propuesto el concepto de "ciberdiligencia debida" a partir

de la extensión del criterio tradicional de "diligencia debida", que facilite saber cómo y cuándo atribuir la responsabilidad internacional a los Estados por los ciberataques mencionados (Cocchini, 2021) pero aun hoy la falta de una respuesta eficaz a este problema genera una total o relativa impunidad en la mayoría de cíberataques.

3.4 Formas de hacer la guerra cibernética. Motivaciones de los ataques.

La guerra cibernética puede presentar distintas amenazas hacia una nación. No sólo como elemento de la "guerra híbrida", sino de forma independiente y como soporte a otro tipo de acciones, como el espionaje o la propaganda, que no constituyen actos de guerra en sí mismos, pero que pueden comprometer seriamente la seguridad y estabilidad de un estado, y promover la violencia social o contra la sociedad.

En cuanto a las operaciones cibernéticas llevadas a cabo por actores estatales contra otros actores estatales, debido al problema de la atribución, suele ser también difícil identificar la motivación. Los cíberataques suelen ser contemplados como una opción atractiva tanto en tiempos de conflicto como de paz por una serie de actores estatales y no estatales. Un gran número de cíberataques tienen una motivación militar, debido a la falta de regulación en el DIH y la propia naturaleza de los ataques cibernéticos, que provoca que sea difícil determinar la motivación e identificar al atacante, por lo que no es claro cuando un acto debe considerarse un acto de guerra. Actualmente prácticamente todas las grandes potencias llevan a cabo constantemente cíber-operaciones militares, las cuales se dividen a su vez en operaciones de defensa cibernética, de ofensiva cibernética y de espionaje cibernético (Brantly et al., 2020).

Los ataques cibernéticos también pueden realizarse con fines políticos. Son realizados por actores estatales o no estatales, con el fin de expresar su apoyo por cierta ideología política, con el fin de hacerla visible, o para expresar su desacuerdo con otros actores que no la comparten (Defsec Media, 2019). Los actores estatales pueden utilizarlo para dañar a otros estados con los que mantienen conflictos, o cuya desestabilización política pueda beneficiar. Asimismo, los actores no estatales que persiguen fines políticos, que pretenden dañar a un gobierno o a un partido político determinado pueden llevar a cabo ataques cibernéticos con un coste-riesgo bajo, logrando sus objetivos más efectivamente que utilizando medios tradicionales, como manifestaciones o protestas. Sin embargo, pueden ser erróneamente atribuidos a otros actores estatales, considerados enemigos

tradicionales del recipiente, causando escaladas de conflicto y tensión, cuando en realidad han sido llevados cabo por un actor no estatal. De la misma manera, los actores estatales que quieren dañar a otros estados pueden utilizar *proxys*, para dañar a su adversario sin que se les atribuya a ellos el ataque y evitar posibles represalias.

Algunos ataques tienen una motivación estrictamente económica, y es la utilizada por estados como por actores no estatales. Corea del Norte, obtuvo en 2019 más de dos billones de dólares mediante cíberataques sofisticados a entidades bancarias y páginas de intercambio de criptomonedas, evadiendo las sanciones que les habían sido impuestas por el Consejo de Seguridad de las NNUU, e invirtiendo dichos ingresos en su programa armamentístico nuclear (Nichols, 2019). También hay que considerar que los cíberataques son utilizados como una forma de espionaje industrial, y son dirigidos tanto hacia grandes corporaciones como a pequeñas empresas, estimándose que en 2024 la implementación de estrategias e instrumentos de protección cibernética costará a las empresas unos 5.2 trillones USD a nivel mundial (Bissell et al., 2019), siendo importante resaltar que toda estrategia de cíberseguridad debe aspirar a proteger tanto a instituciones gubernamentales como a la empresa privada, que pueden sufrir tanto pérdidas económicas como daños físicos como resultado de estas actividades.

Por último, los atacantes cibernéticos pueden ser movidos por conflictos socio-culturales o ideológicos, o bien trabajar como mercenarios, defendiendo los intereses operativos de terceros. Actores estatales o regionales que mantienen conflictos históricos pueden utilizar este dominio para llevar a cabo su ofensiva, como podemos ver en los constantes ataques que lleva a cabo Corea del Norte contra Corea del Sur, tratando de desestabilizarlo económica y políticamente mediante ofensivas a sus instituciones financieras y gubernamentales, llevando a cabo una guerra de desgaste de forma relativamente clandestina (Parsons, 2020). Numerosos actores también utilizan este dominio para promover su ideología, especialmente grupos terroristas como Daesh, que utiliza la red con fines propagandísticos, de captación de adeptos, para planificar y ejecutar ataques cibernéticos y como fuente de financiación (UNODC, 2013), compartiendo su ideología utilizando un tono inclusivo con el fin de atraer al mayor número de personas posibles y socavar la cohesión social (Morillas, 2020).

3.5 Tipos de actores implicados

A medida que crecen las redes de sistemas de información, aumenta su uso por distintos actores para ejercer su influencia. Este quinto dominio cuestiona la tradicional primacía de los actores estatales, como muestra la Teoría de la Difusión de Poder, que explica cómo a raíz de la revolución de la información el tradicional monopolio de poder de los gobiernos y actores estatales ha sido modificado y que actualmente el poder también es ostentado por actores no gubernamentales y no estatales (Nye, 2011). Es indudable que sus características, la asimetría, la dificultad de atribución y el anonimato, hacen que sea un dominio atractivo para actores no estatales. También debemos considerar el rol de estados tradicionalmente débiles, ya que el bajo coste operativo en el dominio cibernético puede fortalecer su posición y reconfigurar la distribución de poder en las RRII (Lango, 2016).

3.5.1 Actores estatales en el dominio cibernético

El dominio cibernético desempeña un importante papel en las relaciones interestatales, ya que permite realizar operaciones de espionaje y ataques a infraestructuras de forma clandestina. Durante la última década se ha evidenciado un incremento en el uso de código dañino por parte de actores estatales, cuyo objetivo más frecuente es obtener información sobre el grado de implantación de las medidas de seguridad de organizaciones e instituciones extranjeras (CNN-CERT, 2019). Vamos a centrarnos en las principales potencias cibernéticas estatales y en estados que son potencias emergentes en este dominio y que han desarrollado grandes capacidades ofensivas.

La República Popular **China** implementó el concepto "guerra informática irrestricta" en su estrategia de Defensa Nacional de 2008 (Mancera, 2014), resaltando la importancia para el país de mantener una "superioridad informativa". Su estrategia militar cibernética se centra en construir y mantener dicha superioridad sin restricciones, combinando operaciones de robo de datos e infiltración en instituciones y empresas extranjeras (Qiao, 2017). Trata de adquirir una ventaja competitiva sobre sus principales potencias competidoras, especialmente sobre EE.UU, considerado un enemigo que peca de una grave dependencia tecnológica, lo que crea una vulnerabilidad que China puede explotar. China también ha promovido diversas campañas de desinformación sofisticadas y complejas en medios de comunicación y redes sociales, tratando de influenciar la opinión pública mundial y desestabilizar política y socialmente a sus adversarios (Cook, 2021). El gobierno chino también recurre constantemente a los

proxies con el fin de eludir las constantes acusaciones de cíberespionaje que recibe de instituciones gubernamentales y empresas extranjeras.

Rusia concibe las operaciones cibernéticas como un subelemento de una guerra de la información amplia, y ha llevado a cabo tanto ataques cibernéticos como operaciones de desinformación para desestabilizar a sus enemigos y coaccionarles para que tome decisiones beneficiosas para Rusia, enfoque denominado "coacción integral" (Mahnken, 2018). La guerra psicológica es un elemento central de esta estrategia, y el gobierno ruso ha creado un ejército de comentaristas políticos que participan en blogs, redes sociales y foros diseminando propaganda pro-Rusia (Sultan, 2019) o contaminando dichos foros con *fake news*, aludiendo a conspiraciones o imposibilitando el diálogo entre participantes cuando pueden censurar información negativa sobre el gobierno ruso (Bugorkova, 2015). Rusia ha coordinado o dirigido un altísimo número de ataques informáticos contra multinacionales, agencias de gobiernos extranjeros, partidos políticos y organizaciones internacionales, en los últimos años, en un gran número de casos, sin esconder su autoría, y actuando en otros casos mediante *proxys* que aparentan ser *hacktivistas* pro-Rusia o *hackers* patrióticos.

Cabe destacar su ya mencionada intervención en las elecciones presidenciales estadounidenses de 2016. Se ha demostrado que el Presidente Putin ordenó directamente la realización de la operación, denominada "Proyecto Lakhta", que consistía en la utilización de diversos grupos de *hackers* vinculados al gobierno ruso para boicotear la candidatura de Hillary Clinton y promover la de su rival, Donald Trump. Estos grupos de *hackers* crearon miles de cuentas en redes sociales, haciéndose pasar por ciudadanos estadounidenses que apoyaban a grupos políticos radicales y promovían eventos apoyando a Trump. Estos grupos también crearon y difundieron desinformación sobre la campaña de Clinton, su vida privada y su carrera profesional. También se utilizaron *hackers* afiliados al servicio de inteligencia militar ruso para infiltrarse en los sistemas de información del Comité Nacional Demócrata y el Comité de Campaña del Congreso Demócrata, sustrayendo y difundiendo correos electrónicos del equipo de Clinton. Esto causó que durante el mandato del Presidente Trump hubiese una gran parte de la población americana no considerase válida la elección de Trump, aumentando la oposición a su mandato radicalmente durante los primeros meses del mismo, cuando se destapó la interferencia rusa. Asimismo, el rechazo a la evaluación de la CIA (Mueller, 2019) sobre esta interferencia por parte de Trump creó una ruptura sin

precedentes entre la comunidad de inteligencia estadounidense y el presidente electo, los cuales expresaron su consternación ante la actitud del Presidente hacia tan grave problema de seguridad nacional. Esta actitud también provocó graves fracturas en el seno del Partido Republicano, ya que muchos de sus miembros se mostraron en profundo desacuerdo ante la actitud del Presidente, provocándose una escisión entre los miembros que apoyaban a Trump y los que no compartían su postura y consideraban la inferencia una cuestión que debía ser analizada en profundidad y debatida en el propio partido (Abrams, 2019).

EE.UU mantiene una estrategia proactiva de cíber defensa, y considera que un ataque cibernético es *casus belli* (Bumiller, 2011), no considerando que haya distinción entre el dominio cibernético y el resto de dominios de la guerra, comparando su Secretaría de Defensa la guerra cibernética a la Guerra Fría, recomendando que "en caso de un ataque cibernético catastrófico, las armas nucleares serían la respuesta disuasoria definitiva" (Defense Science Board, 2013). EE.UU se ha centrado en aumentar sus capacidades ofensivas cibernéticas, pero no ha aumentado su capacidad defensiva al mismo nivel, lo que le ha hecho vulnerable ante otros actores. Las tensiones derivadas de ataques cibernéticos han causado un deterioro en sus RR.II con China y Rusia, a medida que EE.UU ve que no tiene capacidad para impedir con importantes consecuencias para la nación, como la ya confirmada inferencia rusa en las elecciones presidenciales de EE.UU de 2016, cuyo objetivo fue socavar la fe pública en el proceso democrático de Estados Unidos y efectivamente perjudicó la candidatura de Clinton (National Intelligence Council, 2019), o el ya mencionado ataque a su OPM, atribuido a China, que robó los datos de millones de funcionarios, por lo que este actor estatal está desarrollando su Estrategia de Ciberseguridad para aumentar sus capacidades defensivas.

En cuanto a analizar las potencias emergentes, nos centraremos en **Irán** y **Corea del Norte**, los cuales han visto en el dominio cibernético una oportunidad para modificar las tradicionales dinámicas de poder estatales y mejorar su posición internacional. Irán es uno de los actores estatales más activos en el dominio cibernético y ha centrado su actividad cibernética en silenciar la oposición doméstica al régimen gobernante y dañar a estados que llevan a cabo actividades percibidas como "anti-Iraníes" (Denning, 2017). Cuenta con una unidad militar especializada, el ECI, considerado el cuarto mayor ejército cibernético del mundo (INSS, 2012) y varios *proxies,* que realizan operaciones

contra sus tradicionales enemigos regionales con un fin disuasorio: evitar interferencias extranjeras en asuntos domésticos iraníes. El Régimen también cuenta con grupos *hacktivistas* de corte chiita que operan a su favor, y coordinados con grupos extranjeros afines, como el "Syrian Electronic Army" y el grupo libanés "Hizballah" (Connell, 2014), y desde la firma de un acuerdo de cooperación técnica en 2012, se presume que también colabora con Corea del Norte (Arteaga, 2019).

Desde hace más de una década **Corea del Norte** se ha convertido en heraldo de un nuevo patrón de disrupción en las RRII, marcado por ataques indiscriminados que afectan a todo tipo de instituciones gubernamentales, instituciones financieras e industrias, con el fin de obtener ingresos para sus programas de ADM y misiles balísticos. El gobierno norcoreano no ha publicado su enfoque de las operaciones cibernéticas, por lo que su conceptualización de dichas operaciones se basan en inferencias o análisis del comportamiento de este actor estatal, como los publicados por *think tanks* como Rand o firmas de cíberseguridad como Kaspersky (Hodgson et al., 2019). Se ha concluido que hay dos instituciones gubernamentales- la Oficina de Reconocimiento y el Departamento de Estado Mayor, las que preparan las operaciones cibernéticas, combinando ataques disruptivos de baja intensidad con otros que rozan el umbral del uso de la fuerza (Jun et al., 2015). Asimismo, ha invertido grandes cantidades de recursos en la creación de un ejército de *hackers* (Martin, 2018), que actúan sobre fallos de seguridad en *software* rápidamente y son capaces de crear códigos maliciosos sofisticados. En comparación con su sonado programa nuclear, la guerra cibernética tiene una medición entre riesgo y rendimiento opuesta: es barata, de bajo riesgo, es una fuente de ingresos constante para un país con grave problemas económicos, y el problema de la atribución en el cíber espacio hace que no constituya una violación flagrante de las sanciones impuestas por las NNUU (Parsons, 2020).

3.5.2 Actores no estatales en el dominio cibernético

El ciberespacio es un dominio accesible a actores con diferentes necesidades, metas e intenciones, que pueden actuar solos, vagamente conectados o que forman parte de una estructura compleja. Es importante tener en cuenta que los roles de estos actores pueden variar según la situación, dependiendo de sus objetivos y metas (Sigholm, 2013), pero en todo caso coincide en ellos un interés crematístico directo o indirecto en el uso o manipulación de la red. Los medios que puede poner un estado al servicio de la ciberguerra quedan lejos de la capacidad operativa que pueda tener un actor no-estatal.

Las motivaciones que llevan a realizar ataques cibernéticos pueden ser de la más diversa índole: corporaciones y empresas pueden robar datos e información que les proporcione ventajas a la hora de realizar sus operaciones, con el consiguiente aumento de beneficios y posicionamiento en el mercado; *hacktivistas* que reivindican cambios políticos o sociales, pueden alterar, modificar o borrar páginas web de administraciones y organizaciones públicas; lobos solitarios que quieren poner a prueba sus habilidades tratando de penetrar los sistemas de seguridad de empresas o gobiernos. Quizás no cuenten con medios muy significativos, pero es justamente esto lo que les hace más peligrosos: la imprevisibilidad (Fernández, 2019).

En primer lugar debemos considerar a los actores individuales que pueden realizar acciones potencialmente peligrosas en el dominio cibernético: los hackers, individuos con conocimientos informáticos profundos, movidos por fines económicos, políticos, ideológicos o pura curiosidad. Dependiendo de su motivación, pueden ser dañinos o inofensivos. Algunos *hackers* llevan a cabo actividades criminales, sustrayendo información privada de sus víctimas para utilizarla o venderla, obteniendo un beneficio económico, mientras otros utilizan sus conocimientos de forma ética y se centran en estudiar, comprender o mejorar la seguridad de sistemas informáticos (Tate, 2010).

Los *hacktivistas*, mencionados anteriormente, tratan de promover su perspectiva de justicia social. Estos grupos muestran la versatilidad de los actores no estatales, ya que los colectivos *hacktivistas* cuentan con numerosos miembros cuya lealtad puede variar, pudiendo unirse o dejar el grupo en cualquier momento y que pueden formar parte de otros grupos. Su clandestinidad y versatilidad hace que sean sospechosos, porque pueden estar actuando bajo el mando de otros actores. De hecho, gran parte del movimiento *hacktivista* considera que los ataques cibernéticos maliciosos son una forma aceptable de acción directa, por lo que los actores estatales pueden hacerse pasar por *hacktivistas* para llevar a cabo ataques cibernéticos y que no les sean atribuidos directamente (Rodríguez, 2019). Entre ellos hay que destacar al grupo "Anonymous", formado por *hackers* de todo el mundo, que ha realizado diversos ataques contra gobiernos, instituciones y agencias gubernamentales, así como corporaciones, en represalia contra lo que ellos consideran violaciones a sus ideales. Un ejemplo se pudo observar en 2013, cuando el gobierno de Singapur introdujo regulaciones censoras para agencias web de noticias con al menos 50.000 visitas al mes, las cuales debían pagar una garantía de rendimiento de 50.000 dólares singapurenses. "Anonymous" consideró

esto un atentado a la libertad de expresión y al uso de Internet, y modificó varias páginas web relacionadas con el gobierno, entre ellas, la del primer ministro, sustituyendo su contenido por eslóganes defendiendo la libertad de expresión en Internet.

Los cíberterroristas son individuos u organizaciones influenciados por grupos terroristas, que operan en el dominio cibernético para cabo acciones terroristas directas- ataques que puedan potencialmente dañar a seres humanos, o indirectas- como medio de comunicación para planear ataques, captar adeptos, o conseguir financiación (Zerzi, 2017). El grupo Daesh, ya mencionado es pionero en el uso de redes sociales para atraer seguidores, creando programas de ordenador con instrucciones y vídeos sobre cómo llevar a cabo acciones terroristas (Zerzi, 2017). Los cíberataques terroristas han consistido principalmente en la desconfiguración de páginas web, sustituyendo su contenido por eslóganes políticos o religiosos, no causando grandes daños. A pesar de que hasta la fecha ningún grupo terrorista ha causado daños personales o materiales mediante ataques cibernéticos, los expertos advierten que es cuestión de tiempo que adquieran tecnología más avanzada que provoque mayores daños (Zerzri, 2017).

En el ciberespacio también existen bandas criminales organizadas, y la falta de fronteras y la naturaleza anónima de este dominio hace sencilla la asociación de individuos de distintas partes del mundo con fines criminales comunes. La dificultad de aplicar la ley en el ciberespacio, la inexistente rendición de cuentas y el acceso a grandes cantidades de objetivos potenciales facilitan la ciberdelincuencia organizada (UNODC, 2010). En la mayoría de países en vías de desarrollo, donde la ciberdelincuencia es considerada una profesión lucrativa, y las instituciones estatales no cuentan con la suficiente capacidad para perseguir estas acciones, una gran cantidad de jóvenes opta por considerarlo una carrera profesional aceptable, y, dada la naturaleza abierta del cíberespacio, este problema no se limitará a los países en vías de desarrollo, sino que puede tener un impacto mundial (Hassan, 2012).

Finalmente también debemos considerar a los cíberespias, los cuales utilizan técnicas de infiltración para obtener información que pasa por redes que consideran de especial interés. Dichos datos se utilizan y analizan para la preparación de informes de inteligencia para la entidad que los encarga, ya sea con fines militares, políticos o económicos, ya que la monitorización de las capacidades cibernéticas de los adversarios es esencial para la seguridad nacional de los estados (Wilson, 2009). Asimismo,

diversos actores estatales también han implementado programas espías propios, como la red ECHELON, controlada por EE.UU, Reino Unido, Australia, Nueva Zelanda y Canadá, que intercepta comunicaciones por radio y satélite, llamadas de teléfono, faxes y correos electrónicos en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones (Sánchez Medero, 2010).

4) ANÁLISIS COMPARADO DE ESTRATEGIAS DE CÍBERSEGURIDAD

4.1 Unión Europea

4.1.1 Antecedentes históricos: cómo ha abordado la cíberseguridad la UE.

La evolución de la política sobre ciberseguridad en la UE está condicionada por su propia estructura. Por un lado, la UE tiene capacidad de decisión absoluta en lo relativo a sus instituciones pero, al ser una comunidad política de derecho, basada en la cooperación, tiene una muy limitada potestad normativa de aplicación directa a todos los EM. Sin embargo, los retos y riesgos del ciberespacio son comunes a todos los EM y cada uno tiene su propia política de ciberseguridad. Por tanto es imprescindible la coordinación y fijación de una estrategia común a la que se ciña cada EM y que no sea un simple complemento a su propia estrategia de ciberseguridad.

En 2004 se creó la ENISA, un centro de conocimientos especializados para la seguridad cibernética, con funciones de asesoramiento a la UE y a los EM (ENISA, 2005). En 2007 se introdujo el Programa Europeo para la Protección de Infraestructuras Críticas, que creó un marco para la protección de "aquellas infraestructuras cuya interrupción o destrucción afecte a dos o más EM, o a un solo EM si la infraestructura crítica está situada en otro EM" (Comisión Europea, 2006) contra ataques remotos. En 2010 se aprobó la Estrategia de Seguridad Interior de la UE, estresándose la necesidad de colaboración entre EM en materia de ciberseguridad, pero sin proponer medidas específicas para solucionar esta cuestión.

En 2013 se aprobó la primera Estrategia Europea de Ciberseguridad, entre cuyos objetivos se encontraban el aumento de la capacidad de ciberresiliencia de la UE, el control de las ciberdelincuencia y el establecimiento de una política común de ciberdefensa (Comisión Europea, 2013), careciendo, sin embargo, de un enfoque adecuado para luchar contra amenazas cambiantes y no contemplaba la colaboración

con el sector privado en materia de ciberseguridad. En 2016 el Parlamento Europeo publicó la Directiva relativa a medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información, conocida como Directiva NIS, que admitía la necesidad de actualización de las capacidades de cíberseguridad de la UE (Parlamento Europeo, 2016) estableciendo mínimos comunes sobre el desarrollo de capacidades cibernéticas, potenciando el intercambio de información con los operadores de servicios. Su siguiente revisión está teniendo lugar actualmente, muy tardíamente, teniendo en cuenta los rápidos cambios que desde entonces ha experimentado el dominio cibernético, como la expansión masiva de técnicas de desinformación, los ataques cibernéticos mundiales, como el mencionado "Wannacry" o la constatada inferencia cibernética extranjera en procesos electorales. En 2018 la UE reconoció el dominio cibernético como dominio de operaciones, y anunció que adaptaría su PESC para hacer frente a sus retos y amenazas (Parlamento Europeo, 2018).

En cuanto a la evolución del gasto en la materia, en 2019 la Corte Europea de Auditores señaló la falta de transparencia en los gastos en materia de ciberseguridad, ya que los conceptos que describían cada partida específica eran excesivamente vagos (ECA, 2019), y que el gasto era fragmentado e insuficiente, incidiendo en que la debilidad de la gobernanza en ciberseguridad afecta a los sectores público y privado de la UE. En sus recomendaciones señalaron que era esencial aumentar la capacidad de resiliencia de la UE ante ataques cibernéticos y diseñar políticas cuyos resultados pudiesen evaluarse para aprovechar mejor los resultados de los gastos de investigación (ECA, 2019).

4.1.2 La estrategia de ciberseguridad de la UE.

En diciembre de 2020 la Comisión aprobó la Estrategia de Ciberseguridad de la Unión Europea para la Década Digital (Comisión Europea, 2020). Debemos distinguir en primer lugar los objetivos planteados en la misma y los medios que establece para lograrlos. Los objetivos que persigue esta estrategia son tres: Aumento de la capacidad de resiliencia y mantenimiento de su soberanía tecnológica en el ciberespacio, desarrollo de la capacidad operativa para prevenir, detener y responder a los ataques cibernéticos y promoción de un ciberespacio abierto y global.

Para la Unión Europea es esencial actuar contra las amenazas cibernéticas para garantizar que todos los ciudadanos y empresas europeas pudieran beneficiarse plenamente de servicios fiables y fiables tanto virtuales como en el mundo real. La estrategia de ciberseguridad permitiría a la UE intensificar su liderazgo en las normas y

estándares internacionales en el ciberespacio y fortalecer la cooperación con socios de todo el mundo para promover un ciberespacio global, abierto, estable y seguro; basado en el estado de derecho, los derechos humanos, libertades fundamentales y valores democráticos (PAE, 2020). Por lo tanto, no se trata solo de garantizar la seguridad en la red, sino de hacerlo de acuerdo con unos valores políticos esenciales, y siempre salvaguardando los derechos fundamentales de los europeos. No se trata, por tanto, de una intervención neutral por parte de la UE con el único objetivo de salvaguardar la seguridad de sus TIC, sino que es una intervención que responde a unos principios políticos de respeto a la democracia y a los DDHH, así como respeto a la soberanía de todos los EM de la UE, lo cual limita su campo de actuación y efectividad y la distingue del resto de estas estrategias, porque estos principios no son únicamente mencionados sino que verdaderamente informan su contenido.

4.1.2.1 Aumento de la capacidad de resiliencia, soberanía tecnológica y liderazgo en el ciberespacio

Dentro de este objetivo se señala en primer lugar que algunas funciones esenciales de Internet, como los DNS (un servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados) son controladas por un número limitado de compañías privadas (Bohmelaer de Leusse et al., 2019). Esto crea una vulnerabilidad que afectaría a la economía y sociedad europeas en caso de ataques cibernéticos contra alguna de estas empresas, comprometiendo el uso de Internet en la UE, y los servicios que estas compañías ofrecen tanto en el sector privado (a otras empresas) como en el sector público (a los servicios que ofrece el estado directamente o a través de agentes o agencias) (PAE, 2020). El objetivo también contempla un plan de contingencia y la creación de un servicio propio de resolución de DNS, el servicio "DNS4EU", que ofrecerá un servicio europeo alternativo para acceder a Internet, ajustado a las últimas normas en materia de seguridad y protección de datos (ENISA, 2020).

Esta iniciativa es muy positiva ya que prueba que la UE promueve la cooperación con el sector privado, cuya colaboración es muy importante para aumentar la resiliencia en materia de cíberseguridad, pero reduciendo a la vez su dependencia del mismo, promoviendo su propia soberanía tecnológica, que podrá gestionar de manera independiente en caso de necesidad, garantizando el acceso a Internet de los usuarios europeos.

La Estrategia menciona que se está estudiando la revisión de la "Directiva de protección de las Infraestructuras Críticas" y la Directiva NIS, que han quedado obsoletas, así como crear una nueva Directiva sobre resiliencia de entidades críticas. Estas cubrirán una amplia gama de sectores y tienen como objetivo abordar los riesgos actuales y futuros en línea y fuera de línea, desde ciberataques hasta delitos o desastres naturales, de manera coherente y complementaria (PAE, 2020). Sobre la primera, se establece que cada EM deberá identificar esas entidades críticas mediante análisis de riesgos, reservándose la Comisión el derecho de supervisar las que afecten a varios estados. Consideramos este importante avance como muy adecuado porque a los EM les interesa identificar sus infraestructuras críticas y protegerlas de ataques, por lo que prevemos que la cooperación con la UE será fluida y efectiva. Sobre la Directiva NIS se ha optado por introducir cambios sistémicos y estructurales en relación con el ámbito, los actores, la armonización y la exigencia de las obligaciones (Arteaga, 2021), una actualización muy necesaria debido a los rápidos cambios que han experimentado las TIC los últimos años. Su ámbito de aplicación se amplía a nuevos sectores, como las Administraciones Públicas, los servicios postales, la gestión de aguas y la alimentación, y se introducen medidas para institucionalizar un marco europeo en la gestión de crisis y asegurar las cadenas de suministro- avance propiciado por la pandemia mundial actual (Arteaga, 2021). Esto es uno de los mayores avances de la presente Estrategia, ya que salvaguardará las TIC que se emplean en las AAPP, instituciones gubernamentales y servicios esenciales de los EM, protegiéndolas en caso de disrupción y asegurando su provisión a los ciudadanos en caso de crisis. También se impone la declaración de incidentes cibernéticos para PYMES a las autoridades de los EM. Este cambio es también significativo, ya que ayudará a la protección de todo tipo de empresas y a la resolución de incidentes de forma más rápida y efectiva, muy importante para las pequeñas empresas teniendo en cuenta que el 43% de los ciberataques a nivel mundial se dan en PYMES (Juanes, 2020).

Por último lugar, en el marco de este objetivo la Comisión propone crear una red de centros de operaciones de seguridad, que funcionarán con tecnología de IA (PAE, 2020) y constituirán un "Escudo de ciberseguridad" para la UE, capaz de detectar ataques cibernéticos con antelación y permitir respuestas efectivas y rápidas. La UE apoyará la creación de centros de operaciones de seguridad nuevos y la mejora de los existentes, que recibirán apoyo de ENISA. Se destinarán 300 millones de euros para apoyar la

cooperación público-privada en la creación de redes nacionales y sectoriales que conformen una red de seguridad, y para la introducción de tecnologías que mejoren la detección, análisis y respuesta a incidentes. Consideramos que será un proyecto eficiente para proteger tanto a los EM como a la UE, ya que los centros podrán compartir y correlacionar de forma eficiente las señales de ciberataques detectadas y compartir con sus autoridades nacionales, otros EM y la UE, sus descubrimientos, promoviendo un conocimiento completo y colectivo de las amenazas en el ciberespacio. Su introducción protegerá tanto a los EM como a sus ciudadanos y empresas, ya que les permitirá anticiparse a toda actividad cibernética peligrosa, y reducirá el tiempo que los expertos en cíberseguridad dedican a la toma de decisiones críticas, permitiendo una respuesta coordinada y efectiva a las amenazas cibernéticas.

Las medidas adicionales incluirán apoyo dedicado a las pequeñas y medianas empresas (PYME), en el marco de los Centros de innovación digital, así como un mayor esfuerzo para mejorar la fuerza laboral, atraer y retener al mejor talento en ciberseguridad e invertir en investigación e innovación abierta, el cual esté basado en la excelencia (PAE, 2020).

4.1.2.2 Desarrollo de la capacidad operativa de prevención, disuasión y respuesta.

Con el fin de construir la suficiente capacidad operativa para prevenir, disuadir y responder a las amenazas cibernéticas se establece la creación de una "Unidad Cibernética Conjunta", que, gracias a un proceso progresivo e integrador con los EM, dará lugar a plataforma virtual y física para las diferentes comunidades de ciberseguridad de la UE, para prevenir, disuadir y responder a los ciberataques, incluidos los civiles, por medio de las fuerzas del orden nacionales, las comunidades diplomáticas y de ciberdefensa. Ésta se centrará en la coordinación operativa y técnica contra incidentes y amenazas cibernéticas transfronterizas, mejorando la protección contra ataques cibernéticos mediante unidades de respuesta que analicen rápidamente el incidente y ayuden a todos los implicados a responder coordinadamente.

Esta iniciativa muestra la capacidad de adaptación de la UE, ya que actualmente la asistencia mutua entre países es limitada al no existir un mecanismo operacional entre los EM y las instituciones de la UE o con el sector privado para tratar incidentes muy graves por su extensión o en supuestos de crisis (ENISA, 2019). Esta medida no modifica las funciones de las autoridades de los EM en materia de ciberseguridad, sino que establece un marco para compartir experiencias y conocimientos entre instituciones

públicas y privadas, necesario para aumentar la competitividad técnica de esta Estrategia, siendo la cooperación extremadamente necesaria para proteger a las empresas, EM y a la propia UE ante un escenario técnico cambiante.

También hay que resaltar la actualización de la CDT, un marco de cooperación introducido en 2017 con el fin de que la UE pudiese dar una respuesta diplomática conjunta a las actividades cibernéticas maliciosas, disuadiendo a los potenciales agresores en el dominio cibernético a largo plazo (EU Cyber Direct, 2019). El AR, junto a la Comisión deberá presentar una propuesta para que la UE defina más extensamente su postura de disuasión cibernética. Esta postura debería contribuir a la cooperación en el ciberespacio, y orientar la lucha contra los ciberataques más significativos, especialmente los que afectan a infraestructuras críticas e instituciones y procesos democráticos. Asimismo, el AT y la Comisión deberán proponer una actualización de la CDT para aumentar la eficacia del proceso de toma de decisiones, y estudiar cómo la UE la cooperación con potencias extranjeras. Consideramos que el elemento más importante de esta iniciativa es el desarrollo de la postura de disuasión cibernética de la UE, ya que, como mencionamos anteriormente, puede tener potencial para disuadir a actores estatales y no estatales de llevar a cabo ciberataques a instituciones de la UE y sus EM. Sin embargo, tan sólo se menciona vagamente el fomento de la diplomacia cibernética con terceros estados, que continúa siendo un terreno inexplorado y no se proporcionan ejemplos ni medidas concretas para aumentar esta cooperación, mostrando que la UE tiene una comprensión un tanto unilateral de su estrategia cibernética.

La Estrategia hace referencia a cómo la creciente dependencia tecnológica hace más vulnerable a los ciudadanos, instituciones y empresas de la UE ante actividades criminales cibernéticas. La Comisión deberá presentar un plan de acción para aumentar la capacidad digital de los cuerpos de seguridad de la UE y Europol continuará prestando apoyo técnico a las autoridades nacionales encargadas de la ciberdelincuencia. Consideramos que el éxito de esta iniciativa depende del mantenimiento de una comunicación fluida entre Europol y las autoridades de los EM, y de que estos inviertan en la investigación de actividades cibercriminales. Asimismo, consideramos que para responder eficazmente ante actividades criminales cibernéticas, tanto la UE como las autoridades nacionales de los EM deben aumentar las capacidades de las fuerzas del orden para investigar estas actividades, implementando legislación para mejorar la rapidez y eficacia de las investigaciones digitales.

4.1.2.3 Promoción de un ciberespacio global y abierto mediante una mayor cooperación

La UE promueve y defiende su visión del ciberespacio como un espacio global y los valores y principios europeos como instrumentos eficaces para una gobernanza justa de la globalización. Por ello, toda la estrategia de ciberseguridad de la UE se basa en una intensificación de su participación y liderazgo en los procesos internacionales relativos al gobierno del ciberespacio, y necesita -como condición previa- una intensificación de su trabajo con sus socios internacionales para fortalecer su defensa de un orden global basado en reglas, seguro y estable. Por eso, la UE está comprometida a trabajar en este campo de la mano de Naciones Unidas reforzando la ciber diplomacia y la cooperación con terceros países organizaciones regionales e internacionales, así como con la comunidad internacional.

Como parte de esta estrategia, el Plan europeo parte de la necesidad de definición *apriorística* de los objetivos en materia de normativa y de estandarización internacional de criterios de seguridad, que deben ser sancionados por la comunidad internacional. Sin embargo, la falta de competencias supranacionales de la UE podría ser problemática a la hora de configurar esta normativa, ya que la UE podría efectivamente coordinar la labor de los EM pero no establecer una serie de reglas sin consenso por parte de los EM, aunque es viable que se acuerden una serie de mínimos.

Asimismo, la UE quiere promover el respeto del Derecho Internacional y el Derecho internacional humanitario y de los DDHH en el ciberespacio, en particular los derechos y principios contenidos en la Carta de NNUU y las normas, reglas y principios sobre comportamiento estatal responsable, respetadas durante décadas por la comunidad internacional. Se fija la necesidad de que la UE y los EM adopten una postura proactiva en los foros internacionales en relación a esta materia, y que adopten cuanto antes una posición común de la UE sobre la aplicación del DI y DIH en el ciberespacio.

En cuanto a la promoción de la protección de los DDHH en el ciberespacio, la UE cuenta con un "Plan de Acción sobre DDHH y Democracia 2020-2024" (Comisión Europea, 2020), con el que se pretende reforzar la colaboración con gobiernos, empresas e interlocutores sobre rendición de cuentas estatal en la materia. El Plan actualizará las "Directrices en materia de DDHH sobre la libertad de expresión en línea y fuera de línea" (Consejo de la Unión Europea, 2014), incorporando elementos de ciberseguridad y ciberdefensa novedosos.

La efectividad de esta iniciativa tan completa de la UE se ha visto muy limitada por la falta de consenso internacional sobre la elaboración de una normativa para responder a las operaciones cibernéticas que rozan el umbral de la fuerza, ya que sólo un número de limitado de países han pronunciado sus consideraciones sobre esta materia. La UE no ha conseguido desplegar los esfuerzos diplomáticos previstos y son muchos los intereses económicos que propugnan la autarquía en este terreno. Sin embargo, a pesar estas dificultades, muchos autores coinciden en defender la vía de la cooperación internacional, y la consulta y trabajo estrecho con empresas del sector privado para elaborar las bases de una normativa (Van der Meulen et al., 2019), que al final es imprescindible y necesaria para evitar el abuso y la imposición por la fuerza de los más poderosos en el ciberespacio.

En línea con este objetivo, es imprescindible que se aumente el diálogo con terceros estados y el intercambio de buenas prácticas con la Unión Africana, la ASEAN, la OEA y la OSCE. También se considera necesario que la UE forme una "Red Informal de Cíberdiplomacia de la UE" en colaboración con las delegaciones de la UE y las embajadas de los EM en todo el mundo, para promover su visión sobre el ciberespacio entre empresas, individuos y actores privados como organizaciones no gubernamentales u otros entes públicos.

Esta iniciativa de la UE muestra la capacidad de innovación y adaptación de la UE, que apuesta por crear su modelo de gobernanza del ciberespacio, sin que ninguna empresa, gobierno u OOII trate de controlar monopolísticamente el mismo, evitando el abuso, la imposición por la fuerza o la manipulación, lo cual encaja con esa visión particular del ciberespacio que trata de promover la UE. La integración de todos los actores interesados y el intercambio de información regular promoverán la visión de un ciberespacio global en que se mantenga el respeto y protección los DDHH de forma efectiva.

En todo caso, toda esta estrategia requiere también medios materiales para poderse llevar a cabo. Por ello, la UE se ha comprometido a realizar las inversiones en infraestructuras necesarias, para generar una auténtica transición digital en la UE a través de 3 programas de inversión: el Programa Europa Digital, el programa Horizonte Europa, y el Plan de recuperación para Europa. Para ejecutarlo los Estados miembros deberán hacer uso del Mecanismo de recuperación y resiliencia de la UE, que contempla como objetivos específicos el impulso de la ciberseguridad mediante inversiones

combinadas de la UE, los Estados miembros y la industria, especialmente en el marco del Centro de competencia en ciberseguridad y la Red de centros de coordinación, garantizando que una parte importante de los recursos llegue a las PYME y a los ciudadanos.

La Comisión también tiene como objetivo reforzar las capacidades industriales y tecnológicas de la UE en materia de ciberseguridad, mediante proyectos financiados conjuntamente por los presupuestos nacionales y de la UE. Porque la ciberseguridad se entiende como una oportunidad excepcional de mejorar la autonomía estratégica y el liderazgo de la UE, en todos los puntos de la cadena de suministro digital (incluidos datos y nube, tecnologías de procesadores de próxima generación, conectividad ultrasegura y redes 5G (Comisión Europea, 2020).

4.1.3 Conclusiones sobre la Estrategia de Cíberseguridad de la UE.

La UE ha expresado su fuerte compromiso con esta Estrategia anunciando una inversión sin precedentes en la transición digital de la UE durante el periodo 2021-2027. Podemos ver cómo se han tomado en consideración las recomendaciones de la Corte Europea de Auditores, estableciéndose la resiliencia tecnológica como uno de los objetivos de la Estrategia, y disponiendo de presupuesto procedente tanto de los fondos comunes del Marco Financiero Plurianual ordinario como del Mecanismo de Recuperación y Resiliencia, creado para hacer frente a las repercusiones económicas y sociales de la pandemia de COVID-19 y a los retos que plantean las transiciones ecológica y digital, además de las partidas previstas anteriormente. Este aumento de la inversión estratégica servirá para proteger más adecuada y efectivamente el ciberespacio en la UE.

Desde los antecedentes de la actual Estrategia de Cíberseguridad hasta el análisis de la misma observamos una gran evolución: desde un inicio dubitativo se ha pasado a afrontar con decisión los retos de la ciberseguridad y es cada vez más una materia que desborda la vertiente nacional. Esta Estrategia refleja la creciente europeización de la ciberseguridad, con mayor protagonismo de la Comisión, ENISA y los órganos de gestión de crisis y coordinación operativa, así como de los fondos comunes, lo cual implica una mayor participación del PE. Es muy positivo que los actores no estatales asuman un mayor protagonismo en el desarrollo de la soberanía digital frente a los EM, lo que no significa que estos hayan perdido su liderazgo en los procesos de decisión y de regulación, sino que deben tener en cuenta los cambios de agenda para adaptar sus

políticas de ciberseguridad. Este enfoque sin duda será muy beneficioso tanto para la UE como sus EM y para el sector privado (Arteaga, 2021).

Sin embargo, la presente Estrategia también presenta algunos problemas. El principal es la falta de plazos establecidos para llevar a cabo cada iniciativa específica. El hecho de que esta Estrategia no se ha implementado por un periodo determinado de años, sino que es aplicable indeterminadamente, hasta que la UE decida actualizarla nuevamente, exacerba este problema, ya que no hay objetivos claros a corto plazo. Tampoco se ha establecido un paquete de medidas para luchar contra la desinformación, técnica utilizada en gran medida por dos de los actores estatales más importantes en este dominio cibernético, China y Rusia, y que afecta en gran medida a la UE. Además, aunque se menciona la importancia del acceso a pruebas digitales transfronterizas en el curso de investigaciones criminales, no se establece el desarrollo de un marco de colaboración jurídico-privada internacional que facilite a las fuerzas de seguridad y operadores judiciales el conocimiento técnico y la participación en la implantación de soluciones sobre esta materia (Lecuit, 2021). Este era un asunto urgente debido al creciente aumento de delitos cibernéticos, y la UE continua sin establecer un paquete de medidas concreto en este ámbito.

También sigue pendiente de resolución el problema de la aplicación de criterios comunes en relación con la seguridad de las redes 5G. Ya mencionamos su importancia anteriormente, pero debido a su relación con objetivos centrales de esta Estrategia, como la soberanía tecnológica, y por sus implicaciones económicas y geopolíticas, debería haber sido objeto de desarrollo en esta Estrategia. Las redes 5G posibilitan la conexión simultánea de muchísimos más dispositivos, permitiendo la recolección y análisis de datos en tiempo real, mejorando la infraestructura esencial de la Cuarta Revolución Industrial, pero también provocando inversamente millones de posibles accesos no deseados y ataques cibernéticos. En 2019 EE.UU excluyó a empresas chinas, como Huawei, del futuro despliegue de redes 5G en su territorio debido a sus estrechos vínculos con el gobierno chino, alegando que podían utilizar dicha infraestructura para llevar a cabo ciberespionaje, solicitando a la UE que adoptase la misma postura (Sánchez del Campo, 2019). La UE introdujo el paquete de medidas "EU Toolbox", que orientaba y permitía una mayor sinergia y coordinación entre países, operadores y proveedores, pero los EM mantenían la responsabilidad sobre su decisión, lo cual causó tensiones diplomáticas entre la UE y EE.UU, y dividió a los EM, que adoptaron

decisiones basadas en criterios muy dispares (Wintour, 2020). Esta Estrategia no propone la creación de una posición unitaria, y esto hace perder a la UE su oportunidad de aprovechar su fuerte posición en la innovación inalámbrica, ya que tiene un mayor número de patentes de 5G que China y EE.UU juntos (Bird & Bird, 2020). Una línea más fuerte podría animar a las empresas líderes en materia de TIC y 5G de la UE, Nokia y Ericsson, a continuar su sólido historial de innovación y presentar una posición más fuerte frente a sus competidoras y hubiese sido una oportunidad para que la UE utilizase su mecanismo de cooperación internacional para emprender un diálogo con países afines con el fin de alcanzar un consenso global sobre la visión, las normas y los requisitos del espectro de la 5G, ya que es una cuestión que afecta a todo actor estatal y no estatal a nivel mundial, como mencionaremos en nuestra propuesta.

4.2 La estrategia de cíberseguridad de EE.UU

La estrategia de cíberseguridad de EE.UU sigue una línea semejante a la de la UE, aunque se centra principalmente en el aumento de su capacidad de resiliencia y disuasión cibernética, (DHS, 2018), ya que, como mencionamos anteriormente, su capacidad ofensiva cibernética era superior a su capacidad defensiva. Esta estrategia se define en su preámbulo como "realista", porque reconoce el papel central del poder en la política internacional y define claramente los objetivos de la EE.UU (DHS, 2018). Esta estrategia se enfoca especialmente en la reducción de riesgos y vulnerabilidades, basada en cuatro pilares, que describiremos a continuación, y destacaremos los elementos de esta estrategia que consideramos dignos de interés para su posterior extrapolación a la estrategia de la UE.

En primer lugar, el primer pilar de esta estrategia es "la protección de la patria". Se introduce la necesidad de evaluación de los riesgos de ciberseguridad en constante evolución, para informar las actividades de gestión de riesgos y permitir el ajuste regular de las políticas de ciberseguridad, para que sean efectivas a pesar de la evolución tecnológica (DHS, 2018), desarrollando planes operativos que consideren futuros desarrollos tecnológicos e innovaciones potencialmente disruptivas, invirtiendo en IA que analice los ataques actuales para predecir comportamientos futuros. Este objetivo se centra en aumentar la capacidad de anticipación, permitiendo abordar lagunas en capacidades analíticas e identificar los futuros riesgos de ciberseguridad. Su aplicación a la estrategia de la UE sería muy útil, ya que uno de sus principales

problemas es la falta de disposiciones relativas a su actualización, lo cual puede hacer peligrar sus objetivos, especialmente el relativo al desarrollo de la capacidad operativa de prevención, disuasión y respuesta, ya que para desarrollar dicha capacidad es fundamental una anticipación a la evolución de este dominio. Criticábamos anteriormente la falta de direccionamiento por parte de la UE en relación a las redes 5G, y es necesario que, de cara a los próximos retos tecnológicos, la UE invierta en IA, ya que, mediante el aprendizaje automático- que se entrena recibiendo y analizando millones de datos de ataques cibernéticos pasados- puede crear modelos de previsión y prevención.

En el segundo pilar, "promover la prosperidad estadounidense", la estrategia de EE.UU introduce la necesidad de educar y entrenar a sus funcionarios, tanto a nivel estatal como federal, en materia de ciberseguridad. Se fomentará el desarrollo y aplicación de programas de formación diseñados en base a los conocimientos técnicos previos y el área de trabajo de cada grupo funcionarial. Se trata así de mantener un cuadro de profesionales con una formación adecuada en materia de ciberseguridad en todo departamento e institución tanto a nivel estatal como federal (DHS, 2018). Ya que las instituciones y agencias estatales son potenciales objetivos de ciberataques, como observamos en el caso del robo de datos de millones de funcionarios de la OPM estadounidense, la adecuada formación de su personal permitirá que se reporten incidentes con mayor rapidez, y una respuesta inmediata permitirá que la respuesta y mitigación de consecuencias sea más efectiva. Debido a su importancia política, económica y social a nivel mundial, los órganos e instituciones de la UE son un objetivo de ataques cibernéticos, y la introducción de un programa de formación en materia de ciberseguridad para sus funcionarios, así como la incorporación de medidas de apoyo a los EM para que formen a sus propios funcionarios incrementaría la seguridad tanto de la UE como de sus EM, permitiendo actuaciones rápidas y eficaces en materia de prevención y respuesta a riesgos cibernéticos.

En el tercer pilar "preservar la paz a través de la fuerza", la estrategia apuesta por un incremento masivo de las capacidades de defensa cibernética, fortaleciendo sus capacidades en este ámbito, incluidas las que se han descuidado (IEEE, 2018). Aludimos anteriormente a que EE.UU considera el dominio cibernético equivalente al resto de dominios de la guerra, por lo que en su estrategia establece la promoción de coordinación entre los sectores privados y público y el USCYBERCOM (que desde

2018 es considerada una unidad combatiente plena, dependiente del DoD) en cuanto a la identificación de actividad cibernética sospechosa, resaltando EE.UU que la posibilidad de una guerra cibernética debe integrarse en la agenda de seguridad y defensa (DHS, 2018). Esto resulta de gran relevancia, ya que permitirá definir qué misiones y operaciones militares son permitidas en el ciberespacio. La UE también fomentar la innovación y desarrollo de capacidades de ciberdefensa, estableciendo sinergias entre las iniciativas de ciberdefensa llevadas a cabo por los EM en el marco de la PESC, así como con ENISA, mediante el intercambio de información y apoyo mutuo.

Por último, y dentro del cuarto pilar de esta estrategia "incremento de la influencia estadounidense para beneficiar a la humanidad", hemos de destacar que la estrategia de EE.UU también considera de extrema importancia la lucha contra los delitos cibernéticos transfronterizos, y centrará sus investigaciones en comprender cómo las organizaciones criminales utilizan el ciberespacio para llevar a cabo actividades ilícitas, centrándose especialmente en la trata de seres humanos y la explotación infantil. Se llevarán a cabo operaciones para desbaratar, contrarrestar y disuadir adecuadamente a las organizaciones criminales transnacionales y lograr la detención y el enjuiciamiento de los delincuentes individuales (DHS, 2018). La dependencia tecnológica ha aumentado exponencialmente la capacidad operativa de los ciberdelincuentes, y no se puede pretender lograr un ciberespacio global y abierto sin combatir el crimen cibernético (Kaspersky, 2020). La introducción de una medida semejante en la UE sería beneficiosa para promover un ciberespacio en que se respeten los DDHH, con especial atención en los derechos de los niños, ya que en los últimos años, se ha registrado un incremento significativo en el número de casos de abuso y explotación sexual infantil en línea (Europol, 2020). La UE menciona tan sólo brevemente en su Estrategia que Europol continuará cooperando en materia de ciberseguridad con los EM, pero se debería aprovechar más eficientemente su papel. Para lograr el objetivo de la Estrategia de Ciberseguridad de la UE de lograr un ciberespacio global, abierto y seguro en el que se respeten los DDHH resulta vital un refuerzo de la lucha contra los delitos cibernéticos, y será tratada en nuestra propuesta.

4.3 La estrategia de cíberseguridad de Corea del Sur

La estrategia de ciberseguridad de la República de Corea está condicionada por la amenaza que plantea Corea del Norte para su seguridad y modo de vida. De hecho, para

Corea del Sur el ciberespacio es el escenario de conflicto más habitual en sus relaciones de vecindad por la creciente capacidad cibernética que ha ido alcanzando en los últimos años Corea del Norte. Según han informado los medios de comunicación, los ataques cibernéticos procedentes de Corea del Norte llevan suponiendo graves daños económicos para Corea del Sur desde 2015 (Martin, 2018). Los ataques de 2013 que interrumpieron el servicio de varias cadenas de televisión y dos bancos surcoreanos, y el *hackeo* al operador de una planta nuclear en diciembre de 2014 tuvieron repercusión global y movilizaron recursos propios y de sus aliados para su defensa (Lewis, 2016).

La actual estrategia de cíberseguridad de Corea del Sur presenta muchos elementos interesantes, que, de ser extrapolados a la Estrategia de Ciberseguridad de la UE, permitirían una más efectiva consecución de sus objetivos.

En primer lugar, Corea del Sur, al igual que la UE, apuesta por aumentar su capacidad de resiliencia en el ciberespacio, para lo que ha establecido la necesidad de implementar inspecciones anuales en materia de detección y prevención de vulnerabilidades cibernéticas en las redes nacionales de información y comunicación (NSOROK, 2019), con el fin de evitar ciberataques que tengan por objetivo la promoción de desinformación, lo que podría ser efectivo a nivel de la UE si ésta implementase la obligación de que sus EM llevasen a cabo dichas inspecciones a nivel nacional, contribuyendo a la seguridad de los medios de comunicación europeos, previniendo las posibles inferencias de actores estatales o no estatales que tienen por objetivo atacar la estabilidad política y social europea.

En relación a la protección de Infraestructura Crítica, se introduce la realización de evaluaciones de ciberseguridad voluntarias en empresas privadas que operen en sectores considerados críticos en Corea del Sur. Se establece que se realizará una clasificación de estos sectores, se elaborarán normas para la evaluación de riesgos de seguridad críticos de cada sector específico, y una vez realizadas estas inspecciones se aportarán una serie de recomendaciones de ciberseguridad a cada empresa analizada. En relación a la UE, debemos destacar el papel que ENISA podría jugar en relación a la implementación de una medida similar. Actualmente ENISA tan sólo asesora a las instituciones de la UE en pero se podría reforzar su papel, ofreciendo asesoramiento en materia de ciberseguridad a empresas privadas establecidas en la UE, lo cual reforzaría aún más la necesaria cooperación con el sector privado, respetando su autonomía, aumentando la eficiencia de ENISA, explotando más eficazmente sus conocimientos y recursos.

Debido a su relación con Corea del Norte, potencia emergente muy activa en el dominio cibernético, que centra la mayor parte de sus ataques en Corea del Sur, gran parte de la estrategia surcoreana se ha centrado en el refuerzo de la preparación contra ciberataques masivos: se ha establecido la necesidad de evaluar y mejorar el sistema de intercambio de información, investigación y respuesta de los organismos pertinentes en relación con un ciberataque y se van a realizar simulacros conjuntos público-privados de gestión de crisis. Al igual que EE.UU, Corea del Sur implementará sistemas de IA que procesen distintas tendencias en materia de ciberataques para desarrollar mecanismos de previsión y prevención. Resulta muy interesante la implementación de esta sinergia público-privada para aumentar las capacidades de preparación ante ataques cibernéticos, y que sería posible introducir en la "Unidad Cibernética Conjunta" creada en la UE, que no contempla ni la realización de simulacros, ejercicio útil para identificar aspectos de mejora en la forma de responder a un ciberataque. La inversión en IA, que funciona mediante el aprendizaje automático, identificará las relaciones entre amenazas en apenas unos segundos o minutos, permitiendo a los analistas de seguridad responder a las amenazas hasta 60 veces más rápido (IBM, 2020).

La estrategia surcoreana asegura su capacidad de disuasión cibernética efectiva. Se creará un directorio de recopilación, gestión y eliminación de vulnerabilidades en el ciberespacio y desarrollará sus capacidades para identificar a los actores estatales y no estatales responsables (NSOROK, 2019). La creación de un directorio puede ser de gran utilidad para la gestión de medidas de ciberseguridad de actores públicos y privados. La capacidad de identificación de los culpables también puede ser útil para que los mismos puedan ser objeto de sanciones por parte de la NNUU, y para emplear el método disuasorio de la amenaza de castigo, cuyas consecuencias pueden frenar futuros ataques. En cuanto a la aplicación de esta medida a la UE, hemos de mencionar que pese a que la estrategia de la UE establece la creación de una posición común en materia de disuasión, la introducción de un directorio de ciberamenazas a nivel de la UE, a cuya creación contribuirían tanto los EM como las empresas privadas residentes en la UE podría ser extremadamente útil como medio para compartir conocimientos en relación a amenazas identificadas o posibles vulnerabilidades, lo cual contribuiría a aumentar la ciberseguridad comunitaria. La identificación de responsables permitiría que pudiesen ser objeto de sanciones por parte de la UE, lo que serviría como instrumento disuasorio.

Corea del Sur comparte la posición de la UE en relación a la necesidad de contribuir al establecimiento de un ciberespacio global y abierto, en que los DDHH sean respetados. Una de sus medidas se centra en el desarrollo de medios para recoger la opinión pública para promover la participación y confianza del público en el proceso de formulación de medidas en relación a la ciberseguridad. Esto es muy importante para asegurar que el público comprenda por completo el proceso de toma de decisiones en la materia y cómo les pueden afectar personalmente las medidas adoptadas. A nivel de la UE, a pesar de que la misma ha realizado numerosas consultas públicas en relación al papel de ENISA, la mencionada Directiva NIS o sobre la ciberseguridad de las redes 5G, sería conveniente la realización de sesiones de preguntas y respuestas con la ciudadanía para la elaboración de una "Hoja Informativa" que informase a los ciudadanos europeos sobre la introducción de la Estrategia de Ciberseguridad y diese respuesta a las cuestiones que les pudiese suscitar, tanto para mayor transparencia como para que los ciudadanos sean conscientes de los diversos riesgos del ciberespacio, cómo les pueden afectar, y el papel de la UE en su protección.

Por último, es destacable añadir que Corea del Sur ha mencionado en su estrategia que participará activamente en discusiones para promover la confianza entre actores estatales y resolver confusiones o malentendidos que tengan lugar en el dominio cibernético. Esta medida novedosa es muy necesaria ya que, debido al problema de la atribución y al gran número de actores no estatales que operan en este dominio, un ataque cibernético puede ser atribuido injustamente a un actor estatal, lo cual puede causar tensiones internacionales y desviar la atención de los auténticos actores dañinos. La UE debería también reafirmar su compromiso con estas iniciativas, ya que su privilegiada posición internacional a nivel diplomático, podría ser beneficiosa para fomentar la cooperación cibernética entre países y evitar escaladas de conflicto innecesarias.

5) PROPUESTA DE UNA NUEVA ESTRATEGIA DE CÍBERSEGURIDAD PARA LA UNIÓN EUROPEA.

5.1 Necesidad de la modificación de la estrategia actual.

A pesar de considerar que los objetivos sobre los que se basa la Estrategia de Cíberseguridad de la UE son adecuados, algunas medidas deben reenfocarse o

reestructurarse en mayor o menor medida y deben tratarse temas que no han sido tomados en consideración y son necesarios para lograr un ciberespacio seguro en las condiciones y características actuales. Mediante el análisis integrado realizado a las tres estrategias de ciberseguridad hemos identificado tanto debilidades en las medidas introducidas en la Estrategia de Ciberseguridad de la UE como aspectos interesantes que podrían contribuir a los objetivos de la misma y mejorar la efectividad de su aplicación, derivados de las estrategias de EE.UU y Corea del Sur, cuyo contenido y extrapolación a la UE hemos analizado. Pero además de las recomendaciones incluidas en el análisis integrado, debemos extraer una serie de puntos de mejora que pueden aportar ideas a la discusión permanente sobre qué se necesita para garantizar la seguridad en el espacio cibernético, dadas las actuales características y dada la actual evolución tecnológica, acelerada como consecuencia de la pandemia provocada por el COVID19. Los expertos en ciberseguridad de muchas empresas europeas de referencia comparten que las compañías han tenido que afrontar grandes desafíos, frente a los cuales, no estaban preparadas. La pandemia global ha cambiado la forma en la que las empresas y los estados afrontan las estrategias de ciberseguridad, se han tenido que afrontar nuevos retos de carácter tecnológico, y por supuesto de seguridad informática y esto se ha convertido en un aspecto prioritario, para adaptarse a esta nueva realidad en la que lo virtual se ha convertido en el espacio de desarrollo de todas las actividades humanas confinadas. Esto ha supuesto grandes desafíos para los que no todas las organizaciones estaban preparadas. El aceleramiento masivo del uso del ciberespacio durante la pandemia de COVID-19, abocando a prácticamente toda la población de los EM de la UE a un confinamiento domiciliario, provocó que durante meses no hubiera otro espacio público más que el virtual. Esto ha sido un claro ejemplo de la verdadera importancia que tiene este dominio para todos los ciudadanos, empresas y gobiernos europeos, por lo que la UE debería contribuir a asegurar su seguridad. Por tanto, pasaremos a explicar cuáles son estas modificaciones que proponemos para la Estrategia de Ciberseguridad de la UE, y cómo contribuyen a la efectividad de cada uno de sus objetivos.

5.2 Propuesta de modificación de la Estrategia de Ciberseguridad de la UE.

A) Aplicación de Inteligencia Artificial a la Ciberseguridad

En primer lugar, centrándonos en el objetivo del aumento de la capacidad de resiliencia de la UE, hemos de destacar que la UE debe dedicar parte de los fondos de esta estrategia para el desarrollo y aplicación de la IA a la cíberseguridad. La IA es la capacidad de un sistema informático para interpretar datos externos, aprender de dichos datos y emplear esos conocimientos para lograr tareas y metas concretas a través de la adaptación flexible (IBM, 2020). Aplicado a la cíberseguridad, una máquina podría utilizar la IA para aprender en base a todo tipo de datos recopilados acerca de ciberataques pasados, su frecuencia, tipo, origen y consecuencias, para identificar relaciones entre amenazas y así mejorar las capacidades de identificación, protección, detección, respuesta y recuperación ante incidentes (Ayerbe, 2020), eliminando las tareas de investigación realizadas por operadores humanos, que son más lenta. Así, la IA proporcionaría un análisis organizado de los riesgos, reduciendo el tiempo que los analistas de seguridad necesitan para tomar decisiones críticas y coordinar la neutralización de una amenaza (IBM, 2020), lo cual desarrollaría las capacidades de respuesta ante ataques cibernéticos. La UE debe perseguir la implementación de la IA, ya que permitirá optimizar costes y mejorar la detección, prevención y lucha contra las amenazas cibernéticas, como están realizando EE.UU y Corea del Sur. La Comisión debería proponer formas de aumentar las inversiones europeas y nacionales públicas y privadas en la investigación, la innovación y el despliegue de IA y asegurar una mejor coordinación, entre los centros europeos de investigación basadas en la excelencia (Consejo Europeo, 2021).

B) Crear mecanismos de rendición de cuentas y de control con capacidad de actuación en el sector privado y público

Debemos considerar diversos mecanismos que podemos introducir para lograr una mejora en la sinergia entre los sectores público y privado. Introduciremos la posibilidad de que las empresas privadas, tanto PYMES como medianas y grandes empresas residentes en la UE puedan someterse a evaluaciones voluntarias, que serían llevadas a cabo por ENISA, como centro de conocimientos especializado para la seguridad cibernética en la UE, contribuyendo así al desarrollo de una cultura de red y seguridad de la información. ENISA debería llevar a cabo una clasificación de las diferentes empresas dependiendo del sector en que operen y las potenciales amenazas cibernéticas a las que se puedan enfrentar y publicar una serie de recomendaciones por sector, para que las empresas puedan implementar medidas más efectivas de protección y respuesta

a ataques cibernéticos. ENISA también podría asesorar a las empresas privadas que lo soliciten en el desarrollo de planes operativos de prevención y respuesta, ayudando a identificar lagunas y vulnerabilidades en las capacidades de protección de las mismas, y fomentando su actualización constante. Esto será muy positivo porque impulsará el papel de ENISA, cuya labor informará las actuaciones de gestión de riesgos de empresas privadas, haciendo más efectivo su papel, y también permitiendo una más rápida actualización de las capacidades de ciberseguridad de las mismas, lo que aumentará su efectividad y protegerá más eficazmente a las PYMES, que aunque deben notificar sus ciberataques, verán su capacidad de prevención y anticipación mejorada.

C) Formación de expertos en ciberseguridad

Asimismo, con el fin de aumentar su capacidad de resiliencia la UE debe apostar por la promoción y formación de expertos en ciberseguridad, esforzándose por desarrollar, atraer y retener talento en materia de ciberseguridad e invirtiendo en investigación e innovación en la materia, ya que esto constituye un importante componente de la protección contra amenazas cibernéticas. A medida que avanzan las amenazas cibernéticas son más necesarios los especialistas en ciberseguridad, siendo imprescindible invertir y desarrollar la formación a nivel de la UE en este campo. La Estrategia de Ciberseguridad de la UE debería dedicar parte de su presupuesto en el fomento de programas de formación sobre la materia en los EM, para cuyo desarrollo se podría utilizar como modelo los programas de formación ya implementados en algunos EM, como Estonia, que ha creado programas educativos en la escuela primaria, secundaria y en la universidad, y ha introducido campañas de formación y concienciación sobre ciberseguridad a nivel estatal (Lewis, 2016). Para que esta medida resulte efectiva es necesaria un claro consenso político a nivel europeo sobre la importancia de implementar la formación sobre nuevas tecnologías y ciberseguridad en el sistema educativo, y la implicación directa de las instituciones educativas públicas y privadas, y sería muy positiva la implicación de la empresa privada. Numerosas empresas, como Google (GoogleActívate, 2021) o Amazon (AWS, 2021) ofrecen programas gratuitos en línea sobre técnicas de ciberseguridad para particulares o empresas, por lo que podrían colaborar con el sector educativo para compartir sus experiencias sobre la materia y colaborar en la creación de métodos de aprendizaje efectivos. Igualmente podrían evaluar el diseño de estos planes de formación ENISA o la AED, para asegurar su correcto enfoque y su efectividad.

D) Creación y aplicación de normativa sancionadora

Dentro del segundo objetivo de la Estrategia de Ciberseguridad de la UE, aumentar las capacidades de prevención, disuasión y respuesta, debemos considerar la necesidad de reforzar la lucha contra las actividades criminales cibernéticas. La Comisión podría presentar un plan de acción específico para aumentar la capacidad operativa en el ciberespacio de los cuerpos de seguridad de cada EM, sirviendo Europol como centro de apoyo a los EM para coordinar investigaciones que permitan la desmantelación de redes criminales internacionales que operen en el dominio cibernético. Europol y ENISA también podrían crear redes de cooperación y coordinación entre los equipos de respuesta a incidentes de seguridad informática, las fuerzas del orden y el poder judicial de cada EM, sinergias necesarias en la lucha contra la ciberdelincuencia (ENISA, 2021). También resulta necesario que la Comisión trabaje para habilitar canales de comunicación apropiados y clarifique las normas para solicitar el acceso a pruebas electrónicas transfronterizas para investigaciones penales, ya que son necesarias en el 85% de las investigaciones (Comisión Europea, 2018). En 2019 el Consejo autorizó a la Comisión a negociar acuerdos internacionales sobre pruebas electrónicas con terceros estados (Consejo Europeo, 2019), pero esos esfuerzos se interrumpieron en 2020, debiendo retomarse, ya que permitirán una cooperación judicial penal más efectiva. Debe reforzarse también el papel de Europol, más aun teniendo en cuenta que en 2019 se acordó la creación del "Europol Innovation Lab and Hub" (Europol, 2020) que sirviese de observatorio de los avances tecnológicos e impulsase la innovación en el ámbito de la seguridad interior (Consejo Europeo, 2021). Mediante este laboratorio Europol debe continuar desarrollando su papel como centro de conocimientos técnicos de apoyo a las autoridades nacionales de los EM, contribuyendo a la definición de normas forenses comunes de aplicación para mejorar la capacidad de reacción ante los desafíos cibernéticos de la UE, aunque la efectividad de estas medidas depende de un aprovechamiento y una colaboración adecuada por parte de los EM.

E) Mejora de los sistemas preventivos y de análisis de redes

Para mejorar la capacidad de prevención se debe promover el análisis y actualización de las capacidades de ciberseguridad. Para esto se debería realizar un informe anual de aplicación de esta Estrategia, y cubriendo la evolución de los ataques cibernéticos, la vulnerabilidad de las Infraestructuras Críticas, riesgos emergentes en materia de

ciberseguridad en los sectores público y privado y el comportamiento de actores estatales y no estatales. Se podría crear un departamento especializado dentro de ENISA, cuya función sea coordinar las labores de comprobación de cumplimiento de objetivos, y vigilar el proceso de implantación de esta estrategia. Esto requerirá que las agencias de ciberseguridad de los EM y las empresas privadas de ciberseguridad compartan sus datos con ENISA, para que su evaluación informe el futuro de la ciberseguridad. Aunque esto aumentaría la capacidad de prevención, para desarrollar la capacidad de disuasión cibernética debería desarrollarse un procedimiento de atribución de autoría de un ataque cibernético. A pesar de que cada EM tiene un procedimiento distinto para atribuir la autoría de un ataque cibernético, siendo esto un acto soberano, la propia UE debería contar con un procedimiento de atribución. Esto podría ser realizado por el SEAE, informado por ENISA, Europol, y en caso de que el ataque cibernético haya perjudicado a algún EM, las autoridades estatales del mismo, para que pueda declarar públicamente quien es responsable de un ataque cibernético, lo que tendrá un efecto disuasorio.

F) Fortalecimiento de la ciberdiplomacia comunitaria y las alianzas estratégicas con terceros estados en los entonos internacionales de decisión

Dentro del tercer objetivo debemos señalar que, aunque el enfoque de la Estrategia de Ciberseguridad de la UE en el ámbito de la ciberdiplomacia es positivo, puede ser mejorable. En primer lugar debemos señalar que tan sólo menciona brevemente la necesidad de cooperación de la UE con la OTAN en el ciberespacio, sin especificar cómo se reforzará. Hay que resaltar el papel del CCDCOE, que podría servir de puente de conexión en esta colaboración, que podría colaborar junto con ENISA y la AED. El CCDCOE realiza actualmente un proyecto sobre la construcción de la capacidad de "resiliencia jurídica" sobre amenazas cibernéticas, desarrollando un marco de referencia que asigne la responsabilidad a los Estados que realizan operaciones cibernéticas dañinas para evitar la escalada de conflictos en el ciberespacio, cuya transformación en una serie de principios consensuados entre la UE y la OTAN podrían significar un avance normativo en materia de DI aplicable al ciberespacio. Asimismo, considerando la importancia del establecimiento de una cooperación internacional más fuerte, se debería introducir en la Estrategia de Ciberseguridad de la UE la necesidad de establecer en un corto periodo de tiempo coaliciones *ad hoc* (es decir, a corto plazo, ya que la creación de una liga o asociación internacional en la materia tardaría más en

materializarse, y es una cuestión urgente) entre la UE y otros estados democráticos, para presentar un fuerte unido frente a estados autoritarios que utilizan el dominio cibernético para restringir libertades individuales o llevan a cabo operaciones cibernéticas dañinas. Convendría revisar y adaptar el mandato del SEAE, ampliando sus competencias y financiación para que se halle adecuadamente capacitado para promover la ciberdiplomacia.

G) Liderazgo de la UE en la creación de espacios de investigación y discusiones global en materia de ciberseguridad

Se menciona vagamente en la Estrategia de Ciberseguridad de la UE la necesidad de desarrollar la normativa internacional en relación con el ciberespacio, pero la UE debería liderar la creación de foros mundiales para fijar qué se consideran acciones cibernéticas por encima del umbral del uso de la fuerza, y establecer una serie de protocolos complementarios para actuar con eficacia contra los ataques cibernéticos llevados a cabo por "proxys" que actúan para un actor estatal. Para la elaboración de esta normativa la Comisión y el AR deberán reforzar los intercambios regulares de información con todo actor interesado, incluyendo el sector privado, la sociedad civil y la academia. La implicación de todos los interesados en definir la postura de la UE permitirá que estas normas gocen de mayor aceptación, facilitando su reconocimiento a nivel mundial.

H) Inclusión y consideración en las futuras Estrategias de Ciberseguridad los desarrollos del 5G

Debemos incluir en esta Estrategia un enfoque consolidado en relación a las tecnologías 5G. Ya que la UE ha permitido que los EM escojan a sus proveedores con relativa libertad, y esto no puede modificarse, debería centrarse en aprovechar su mecanismo de cooperación internacional para tratar de alcanzar con países afines un consenso sobre la visión, normas y requisitos del espectro de estas redes. Ante el creciente dominio tecnológico de China es muy necesaria una posición transatlántica común para inclinar la balanza hacia un sistema de gobernanza de datos abierto, justo y seguro. Dado que la importancia de los sistemas 5G ha adquirido una dimensión geopolítica, siendo éstas un motor económico y un activo de seguridad nacional, las estrategias y principios actuales no pueden limitarse a las agendas nacionales, y abrir un profundo debate transatlántico

sobre el papel del 5G garantizará una cooperación mutuamente beneficiosa y mayor estabilidad internacional (Chivot, 2020).

I) ***Creación de organismos diplomáticos de la UE centralizados en ciberseguridad, introduciendo este tema de forma transversal en toda acción y desarrollo de su PESC.***

Por último, proponemos que la UE estudie crear sus propias "Embajadas digitales", como realizó Dinamarca en 2017 (Esparza, 2017), inventando el concepto de "diplomacia tecnológica", elevando la tecnología, digitalización y ciberseguridad a una prioridad transversal de su política exterior y de seguridad (Udenrigsministeriet, 2021). La UE debería nombrar a un "embajador digital", que se relacione en nombre de la UE con las principales empresas tecnológicas y en materia de ciberseguridad del mundo. A lo largo de este trabajo hemos mencionado la importancia del mantenimiento de una relación fluida entre los sectores público y privado en este campo, y esta sería una manera de construir lazos entre la UE y compañías que le pueden ofrecer el mejor asesoramiento actualizado en materia de riesgos cibernéticos. La creación de esta embajada digital serviría para plantear las dudas o preocupaciones de la UE en materia de ciberseguridad, para tratar de influir en la dirección en la que se desarrolla la tecnología y aumentar los mecanismos de preparación y prevención de la UE y para tratar de aumentar la influencia de la UE en relación a cuestiones de política tecnológica, promoviendo su visión del ciberespacio con estos actores privados.

6) CONCLUSIONES FINALES SOBRE LA ACTUALIZACIÓN DE LA ESTRATEGIA DE CÍBERSEGURIDAD DE LA UNIÓN EUROPEA.

La principal conclusión que se puede extraer de lo expuesto en este trabajo es que la implementación de estrategias y medidas de ciberseguridad es necesaria tanto para actores estatales como no estatales, ya que la expansión constante del dominio cibernético ha aumentado los potenciales peligros y amenazas a los que se hallan expuestos. Se ha estudiado el panorama actual en la materia, sus condicionantes, sus implicaciones y se han hecho algunos avances sobre el futuro. Las siguientes líneas de investigación estarían relacionadas con los avances técnicos y sus consecuencias estratégicas y geopolíticas, porque esta materia no es estática y su evolución y los retos

a los que habrá que enfrentarse derivan esencialmente de los cambios tecnológicos. También hemos comprobado que la soberanía estratégica está íntimamente relacionada con la soberanía tecnológica. Eso significa que hay que estar preparados para el futuro porque aunque nuestra estrategia de ciberseguridad sea efectiva, la misma necesita un proceso de renovación continua. La UE necesita una visión de futuro que englobe aspectos educativos, empresariales, y formativos para lograr presentar una posición competitiva. Es por tanto necesario aumentar el nivel de inversión en I+D y fomentar la creación de entornos de innovación que faciliten el desarrollo de empresas de futuro.

De cara al futuro habrá que prestar mucha atención a las implicaciones que el desarrollo de la IA tendrá en la ciberseguridad, puesto que sabemos que la misma es esencial para la detección y respuesta ante ataques y consecuentemente quien más avance en dicha tecnología tendrá una ventaja decisiva sobre los demás. De momento EE.UU sigue siendo el líder en la materia en cuanto a patentes y citas de publicaciones científicas, aunque China se está acercando enormemente, pretendiendo convertirse en líder mundial en la materia en 2030 (Rodríguez, 2021). También se deberá estudiar de cara al futuro la evolución de las dinámicas entre los distintos actores estatales en el ciberespacio, ya que, aunque en las estrategias de ciberseguridad que hemos estudiado se fomenta y protege el respeto a los DDHH y la democracia en el dominio cibernético, también hemos comprobado que estos valores no son compartidos por todos los actores operantes en el mismo, por lo que sería conveniente observar de qué forma los actores estatales podrían de forma efectiva cooperar para salvaguardar estos valores y fomentar su protección.

Por último, debemos señalar que nuestro análisis ha demostrado que la guerra cibernética es una realidad, y podemos comprobar que ningún actor, estatal o no estatal está a salvo. Los actores estatales pueden ver sus infraestructuras críticas saboteadas, o la información de sus órganos gubernamentales sustraídas. Pero los actores no estatales, tanto empresas como individuos, también pueden ver sus datos personales robados. A todo esto hay que sumar las tácticas de desinformación *y fake news* que utilizan diversos actores con el fin de desestabilizar las sociedades de naciones enteras. A nivel individual, cada persona debe ser consciente de este problema, y que cualquier publicación que leemos o compartimos puede influir en otros, por lo que nuestras acciones pueden fomentar o limitar la expansión de desinformación. Tratar de

solucionar este problema a nivel individual contribuirá sin duda, a solucionar este gran desafío.

7) BIBLIOGRAFÍA

- Abrams, A. (6/4/2019). *Here's What We Know So Far About Russia's 2016 Meddling*. Time. (Recuperado el 12/4/2021 de https://time.com/5565991/russia-influence-2016-election/).
- Aguilar, L. et al. (2011). *Cuaderno de Estrategia 149: Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio.* Instituto Español de Estudios Estratégicos. (Recuperado el 15/4/2021 de http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2011/Cuaderno_149.html).
- Aguilar, A. (30/11/2020). *Cuenta atrás para Google, Apple, Facebook y Amazon: la nueva regulación europea contempla 'dividir' compañías y abre la puerta a otra disputa en la OMC.* Business Insider. (Recuperado el 12/2/2021 de https://www.businessinsider.es/como-afectara-nueva-regulacion-ue-tecnologicas-764115).
- Aitel, D. (2015). *Iran is emerging as one of the most dangerous cyber threats to the US*. Business Insider UK. (Recuperado el 2/2/2021 de http://uk.businessinsider.com/iran-is-emerging-as-one-of-the-most-dangerous-cyber-threats-to-theus-2015-12?r=US&IR=T).
- Alexander, D. (2017). *Apparent Islamic State backers hack U.S. military Twitter feed.* Reuters. (Recuperado el 12/2/2021 de https://www.reuters.com/article/us-cybersecurity-centcom-hack-idUSKBN0KL1UZ20150113).
- Applegate, S. (2013). *The Dawn of Kinetic Cyber*. En: Podins, K., Stinissen, J., Maybaum, M (eds.): *5th International Conference on Cyber Conflicts*. NATO CCDCOE Publications. Tallinn. Pp.3-6.
- Arauzo, E. (3/10/2020). *Reunión extraordinaria del Consejo Europeo, 1 y 2 de octubre de 2020.*Oficina de Prensa del Consejo Europeo. (Recuperado el 1/4/2021 de https://www.consilium.europa.eu/es/meetings/european-council/2020/10/01-02/).
- Arquilla, J. et al. (1993). *Cyberwar is Coming!*. Comparative Strategy 12(2): 141–65.
- Arteaga, F. (2019). *Capacidades ofensivas, disuasión y ciberdefensa.* CIBER ElCano (Real Instituto El Cano). (Recuperado el 23/3/2021 de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLO

BAL_CONTEXT=/elcano/elcano_es/zonas_es/ari92-2019-arteaga-capacidades-ofensivas-disuasion-y-ciberdefensa).

- Arteaga, F. (2021). *La evaluación y la revisión de la Directiva NIS: la Directiva NIS 2.0.* Real Instituto El Cano. (Recuperado el 12/3/2021 de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari19-2021-arteaga-evaluacion-y-revision-de-la-directiva-nis-2-0).
- Arteaga, F. (2021). *Año Nuevo, nuevo "paquete" de ciberseguridad de la Comisión para 2021*. Real Instituto El Cano. (Recuperado el 23/3/2021 de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-arteaga-nuevo-paquete-de-ciberseguridad-de-comision-para-2021).
- AWS (Amazon Web Services). (2021). Training and Certifications: Build your future in the AWS Cloud. AWS Training. (Recuperado el 12/3/2021 de https://www.aws.training/).
- Ayerbe, A. (10/11/2020). *La ciberseguridad y su relación con la inteligencia artificial.* CIBERElCano. (Recuperado el 2/2/2021 de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari128-2020-ayerbe-ciberseguridad-y-su-relacion-con-inteligencia-artificial).
- Banta, B. (2020). *International Cyberpolitics.* International Studies Association and Oxford University Press. (recuperado el 11/3/2021 de https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-553).
- Beer, F. (2001). *Meanings of War and Peace*. College Station: Texas A&M University Press.
- Bendiek, A. et al. (16/2/2021). *Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy*. German Institute for International and Security Affairs. (Recupeado el 1/3/2021 de https://www.swp-berlin.org/en/publication/revisiting-the-eu-cybersecurity-strategy-a-call-for-eu-cyber-diplomacy/).
- Bird & Bird. (2020). *Who is leading 5G? A transparent assessment of 5G patent leadership.* Two Birds Pattern. (Recuperado 1/3/2021 de https://www.twobirds.com/~/media/pdfs/who-is-leading-5g-development.pdf).

- Bissell, K. et al. (2019). Ninth Annual Cost of Cybercrime Study. Accenture. (Recuperado el 12/2/2021 de https://www.accenture.com/us-en/insights/security/cost-cybercrime-study).
- Bissell, K. et al. (2020). *Innovate for cyber resilience: Third annual state of cyberresilience*. Accenture. (Recuperado el 12/2/2021 de https://www.accenture.com/us-en/insights/security/cyber-threatscape-report).
- Bohmelaer de Leusse, C. et al. (2019). *The Global Internet Report: Consolidation in the Internet Economy*. Internet Society. (Recuperado el 12/3/2021 de https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/).
- Boisen, C. (2020). *Hugo Grotius, Declaration of War, and the International Moral Order*. Grotiana. Vol. 42 (2). Pp. 282-283.
- Brantly A. et al. (2020) *Military Operations in Cyberspace*. En: Sookermany A. (ed.) *Handbook of Military Sciences*. Springer, Berlin. Pp. 1-16.
- Carter, N. (22/1/2018). *Dynamic Security Threats and the British Army*. RUSI Organization. (Recuperado el 12/3/2021 de https://rusi.org/event/dynamic-security-threats-and-british-army).
- Chang, W. (2012). *Warfare in the Cyber Domain*. Air, Space and Power Journal. Vol. 26 (5). Pp. 49-56.
- Chivot, S. (10/9/2020). *The EU's approach to 5G and the reshaping of transatlantic relations.* ELN. (Recuperado el 3/2/2021 de https://www.europeanleadershipnetwork.org/commentary/the-eus-approach-to-5g-and-the-reshaping-of-transatlantic-relations/).
- Choucri, N. (1972). *En busca de sistemas de paz: Escandinavia y los Países Bajos, 1870-1970*. En: Russett, B (ed.), *Paz, guerra y números*, Berkeley: Sage Publications. Pp. 239-74.
- Choucri, Nazli. et al. (1989). *Presión lateral en las relaciones internacionales: concepto y teoría*. En: Midlarsky, M (ed.) *Handbook of War Studies*. Ann Arbor: University of Michigan Press. Pp. 289-326.
- Choucri, N. (2000). *CyberPolitics in International Relations.* International Political Science Review. Vol. 21 (3). Pp. 243-258.

- Clarke, R.A. et al. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper and Collins. Pp. 188-190.
- Clarke, R.A. et al. (2020). *The Fifth Domain.* Nueva York: Penguin Random House. Pp. 102-109.
- CNN-CERT (Centro Criptológico Nacional). (2019). *Ciberamenazas y Tendencias: Edición 2019.* CCN-CERT IA-13/19. Ministerio de Defensa.
- Cocchini, A. (2021). *Ciberdiligencia debida: ¿una actualización necesaria para el Derecho Internacional del ciberespacio?* Real Instituto Elcano: CIBERelcano. (Recuperado el 21/3/2021 de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari27-2021-cocchini-ciberdiligencia-debida-actualizacion-necesaria-para-derecho-internacional-del-ciberespacio).
- Comisión Europea. (2006). *Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas*. /* COM/2006/0786 final */
- Comisión Europea. (2013). *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.* Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.
- Comisión Europea. (9/11/2013). *European Cybercrime Centre (EC3) opens on 11 January*. Comunicados de Prensa de la Comisión Europea. (Recuperado el 1/4/2021 de https://ec.europa.eu/commission/presscorner/detail/en/IP_13_13).
- Comisión Europea. (2018). *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal.* 80COM(2018) 225 and 226; C(2020) 2779 final.
- Comisión Europea. (2020). *The EU's Cybersecurity Strategy for the Digital Decade (JOIN/2020/18 final).* (Recuperado el 1/1/2021 de https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN).

- Comisión Europea. (2020). *El Plan de Acción 2020-2024 para los Derechos Humanos y la Democracia.*
- Connell, M. (2014). *Deterring Iran's Use of Offensive Cyber: A Case Study*. CAN Analysis and Solutions. Arlington, VA.
- Consejo de la Unión Europea. (2014). *EU Human Rights Guidelines on Freedom of Expression Online and Offline.*
- Consejo de la Unión Europea. (6/7/2019). *El Consejo da mandato a la Comisión para negociar acuerdos internacionales sobre pruebas electrónicas en materia penal.* Oficina de Prensa del Consejo de la UE. (Recuperado el 23/3/2021 de https://www.consilium.europa.eu/es/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/).
- Consejo de la Unión Europea. (2021). Un futuro digital para Europa. Políticas-Cronologías del Consejo de la Unión Europea. (Recuperado el 18/3/2021 de https://www.consilium.europa.eu/es/policies/a-digital-future-for-europe/).
- Consejo Europeo. (2008). *Informe sobre la aplicacion de la Estrategia Europea de Seguridad. S407/08.*
- Consejo Europeo. (2010). *Estrategia de Seguridad Interior de la Unión Europea: Hacia un modelo europeo de seguridad.* Publicaciones de la Unión Europea. Luxemburgo
- Cook, S. (30 March 2021). *Beijing Is Getting Better at Disinformation on Global Social Media.* The Diplomat. (Recuperado el 1/4/2021 de https://thediplomat.com/2021/03/beijing-is-getting-better-at-disinformation-on-global-social-media/).
- Cornish, P. (2019). *Report: Military operations in cyberspace.* Wilton Park. (Recuperado el 12/2/2021 de https://www.researchgate.net/publication/330181733_Military_operations_in_cyberspace).
- Cotarelo, J. (2013). Las nuevas formas de acción y comunicación políticas. Valencia: Tirant Humanidades. Pp. 13-31.

- Craig, A. et al. (2016). *Conceptualising Cyber Arms Races*. IEE Proceedings for CCDCOE CyberCon, 8th International Conference on Cyber Conflict: Cyber Power, 141–58.
- Craig, A. et al. (2018). *Realism and Cyber Conflict: Security in the Digital Age.* En Orsi. D. et al., *Realism in Practice: An Appraisal.* Bristol (U.K): E-International Relations.
- CSIS. (2020). *Significant Cyber Incidents.* Strategic Technologies Program. (Recuperado el 1/3/2021 de https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents).
- Daricili, A.B. (03/12/2020). *¿Cuáles son los objetivos de las estrategias de ciberseguridad de los países con más poder del mundo?* Agencia Anadolu. (Recuperado el 2/4/2021 de https://www.aa.com.tr/es/an%C3%A1lisis/-cu%C3%A1les-son-los-objetivos-de-las-estrategias-de-ciberseguridad-de-los-pa%C3%ADses-con-m%C3%A1s-poder-del-mundo/2063747#).
- Defense Science Board. (January 2013). *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.* Defense Science Board. Washington D.C.
- Defsec Media. (2019). *Motivation of cyber terrorists in launching acts of cyber terror.* Line of Defence. Vol. 12. Pp. 44-46.
- Demchak. C. et al. *Thinking Systemically about Security and Resilience in an Era of Cybered Conflict,* en Richet. J.L (ed)., *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*. Hershey, PA.: Information Science Reference. Pp. 367–382.
- Denning, D. (2017). *Following the Developing Iranian Cyberthreat.* The Conversation. (Recuperado el 12/3/2021 de https://www.scientificamerican.com/article/following-the-developing-iranian-cyberthreat/).
- DHS (Department of Homeland Security). (2018). *US Department of Homeland Security Cybersecurity Strategy.*
- Díez-Picazo, L.M. (2008). *La naturaleza de la Unión Europea.* InDret: Revista para el Análisis del Derecho. (Recuperado el 3/2/2021 de https://indret.com/la-naturaleza-de-la-union-europea/).

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Ebert, H. (12/10/2020). *Cyber Resilience and Diplomacy in the Republic of Korea*. EU Cyber Direct: Supporting EU Cyber Diplomacy. (Recuperado el 2/3/2021 de https://eucyberdirect.eu/content_research/cyber-resilience-and-diplomacy-in-the-republic-of-korea/).
- ECA (European Court of Auditors). *Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper).*
- Ehl, D. (2018). *Nueva agencia para la ciberseguridad: Alemania contraataca a los hackers.* DW Made for minds. (Recuperado el 3/2/2021 de https://www.dw.com/es/nueva-agencia-para-ciberseguridad-alemania-contraataca-a-hackers/a-45298258).
- ENISA. (2005). *About ENISA - The European Union Agency for Cybersecurity-Towards a Trusted and Cyber Secure Europe.* ENISA Reports. (Recuperado el 12/3/2021 de https://www.enisa.europa.eu/about-enisa).
- ENISA. (2019). *Annual Report on Trust Services Security Incidents in 2019.* ENISA Reports.
- ENISA. (17/12/2019). *ENISA welcomes the EU Cybersecurity Strategy and Agency's proposed tasks*. ENISA Press Releases. (Recuperado el 13/3/2021 de https://www.enisa.europa.eu/news/enisa-news/enisa-welcomes-the-eu-cybersecurity-strategy-and-agency2019s-proposed-tasks).
- ENISA. (2020). *EU Threat Landscape Report: Cyber attacks are becoming more sophisticated, targeted and widespread.* ENISA Reports. (Recuperado el 21/1/2021 de https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends).
- ENISA. (2021). *2020 Report on CSIRT-LE Cooperation: study of roles and synergies among selected countries.* ENISA Reports. (Recuperado el 12/4/2021 de https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation/).
- Esparza, P. (9/2/2017). *¿Por qué Dinamarca creará la primera embajada digital del mundo para lidiar con Google, Facebook y otros gigantes tecnológicos?* BBC

News. (Recuperado el 3/2/2021 de https://www.bbc.com/mundo/noticias-38917336).

- EU Cyber Direct. (10/10/2019). *Council Conclusions on the Cyber Diplomacy Toolbox*. EU Cyber Direct Project. (Recuperado el 3/3/2021 de https://eucyberdirect.eu/content_knowledge_hu/draft-council-conclusions-on-the-cyber-diplomacy-toolbox/).
- Europol. (2020). *EXPLOITING ISOLATION: Offenders and victims of online child sexual abuse during the COVID-19 pandemic*. EUROPOL Reports. (Recuperado el 8/3/2021 de https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic).
- Europol. (2020). *Written contribution to JPSG The Europol Innovation Lab*. Europol.
- Evans, M. et al. (26/2/2021). *Cyberattacks Cost Hospitals Millions During Covid-19*. The Wall Street Journal. (Recuperado el 2/3/2021 de https://www.wsj.com/articles/cyberattacks-cost-hospitals-millions-during-covid-19-11614346713).
- Feliú Ortega, L. et al. (2012). *El ciberespacio, nuevo escenario de confrontación*. Monografías del Centro Superior de Estudios de la Defensa Nacional. Vol. 26: 28-76.
- Fernández, A. (30/12/2015). *La ciberguerra, un teatro invisible*. El Orden Mundial. (Recuperado el 12/4/2021 de https://elordenmundial.com/la-ciberguerra-un-teatro-invisible/).
- Friedman. A. et al. (2014). *Cybersecurity and Cyberwar*. Oxford: Oxford University Press. Pp. 144-146.
- GoogleActívate. (2021). Preguntas Frecuentes. GoogleActívate Cursos Online. (Recuperado el 12/2/2021 de https://learndigital.withgoogle.com/activate/faqs).
- Government of the United Kingdom. (18/2/2021). *Record year for UK's £8.9bn cyber security sector*. Government of the United Kingdom Press Releases. (Recuperado el 12/3/2021 de https://www.gov.uk/government/news/record-year-for-uks-89bn-cyber-security-sector).

- Guinness, H. (18/7/2015). *What Is GAFA? Why The EU Doesn't Love Large American Internet Companies.* MUO. (Recuperado el 14/2/2021 de https://www.makeuseof.com/tag/gafa-eu-doesnt-love-large-american-internet-companies/).
- Juanes, G. (1/1/2020). *Guía Práctica de Ciberseguridad para pymes.* Cuadernos de Seguridad. (Recuperado el 12/3/2021 de https://cuadernosdeseguridad.com/2020/09/pymes-ciberataques-ciberseguridad/).
- Hassan, A. et al. (2012). *Cybercrime in Nigeria: Causes, Effects and the Way Out*. ARPN Journal of Science and Technology. Vol. 2 (7). Pp. 22-24.
- Hitchens, T. et al. (1/10/2017). *International Cybersecurity Information Sharing Agreements.* Centre for International & Security Studies at Maryland (Recuperado el 21/3/2020 de https://www.jstor.org/stable/resrep20426?seq=1#metadata_info_tab_contents).
- Hobbes, T. (1651). *Leviathan or The Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil.* Londres: Bloomsbury Publishing.
- IBM. (2020). Inteligencia artificial para una clase de ciberseguridad más inteligente. IBM- Services. (Recuperado el 12/3/2021 de https://www.ibm.com/es-es/security/artificial-intelligence).
- IEEE (Instituto Español de Estudios Estratégicos). (19/07/2018). *Estrategia de Seguridad Nacional de EE.UU.* IEEE. (Recuperado el 1/4/2021 de http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2017/Resena_US_Estrategia_Seg.Nacional_Dec2017.pdf).
- INSS (Institute for National Security Studies). (15/10/2012). *Iran's Cyber Warfare.* INSS Insight. Vol. 375. Pp. 2-4.
- International Institute for Strategic Studies: Military Balance 2014. pp. 19-22. Routledge, London. (2014).
- ITU (International Telecommunications Union). *Top countries best prepared against cyberattacks.* ITU Publications. (Recuperado el 23/2/2021 de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Top-countries-best-prepared-against-cyberattacks.aspx).

- Jervis, R. (1978). *Cooperation Under the Security Dilemma*. World Politics 30(2): 167–214.
- Johnson. D. et al. (2010). *Principles of the Defense for Cyber Networks.* Defense Concepts. Vol. 4. Pp. 2-17.
- Joyner, C. (Diciembre 2006). *Coercion.* Oxford International Public Law: Max Planck Encyclopedias of International Law. (Recuperado el 12/3/2021 de https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1749).
- Kaspersky. (2020). *Tips on how to protect yourself against cybercrime*. Kaspersky Resources. (Recuperado el 12/3/2021 de https://www.kaspersky.com/resource-center/threats/what-is-cybercrime).
- Kolet, K. (2001). *Asymmetric Threats to the United States*. Comparative Strategy 20(3): 277–92.
- Kuehl, D. (2009). *From Cyberspace to Cyberpower: Defining the Problem*. en Kramer, F. et al. *Cyberpower and National Security*. Washington (D.C): National Defense UP.
- Lachow, I. (2009). *Cyber Terrorism: Menace or Myth ?* En: F. D. Kramer, S. H. Starr & L. K. Wentz (eds.). *Cyberpower and National Security*. National Defense University Press. Washington, D.C.
- Lango, H. (2016). *Competing Academic Approaches to Cyber Security*. Conflict in Cyber Space: Theoretical, strategic and legal perspectives, 7-26. London: Routledge.
- Lecuit, J. (2021). *El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea.* Real Instituto El Cano. (Recuperado el 2/4/2021 de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari4-2021-alonso-acceso-a-pruebas-electronicas-y-cifrado-dos-puntos-clave-de-agenda-seguridad-europea).
- Lee R. (4/3/2016). *The Problems with Seeking and Avoiding True Attribution to Cyber Attacks.* SANS DFIR. (Recuperado el 3/3/2021 de https://digital-

forensics.sans.org/blog/2016/03/04/the-problems-withseeking-and-avoiding-true-attribution-to-cyber-attacks/).

- Lewis, J. (2010). *A Note on the Laws of War in Cyberspace.* Centre for Strategic & International Studies. (Recuperado el 12/3/2021 de csis.org/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf).
- Lewis, J. et al. (2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. Banco Interamericano de Desarrollo. (Recuperado el 4/3/2021 de https://publications.iadb.org/publications/spanish/document/Experiencias-avanzadas-en-pol%C3%ADticas-y-pr%C3%A1cticas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Rep%C3%BAblica-de-Corea-y-Estados-Unidos.pdf9).
- Lindsay, J.R. (2013). *Stuxnet and the Limits of Cyber Warfare*. Security Studies 22(3): 365–404.
- Lonsdale, D. (2004). *The Nature of War in the Information Age: Clausewitzian Future.* Londres: Routledge.
- Maayan, D. (13/1/2020). *The IoT Rundown For 2020: Stats, Risks, and Solutions.* Security Today. (Recuperado el 13/3/2021 de https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx).
- Machín, N. et al. (2016). *La ciberseguridad como factor crítico en la seguridad de la Unión Europea.* Revista UNISCI. Vol. 42. Pp. 2-16.
- Mancera, J.M. (2014). *La ciberguerra china desde la lógica de la guerra irrestricta.* Ciencia Y Poder Aéreo. Vol. 9 (1). Pp. 89-96.
- Maness, R. et al. (2014). *The dynamics of cyber conflict between rival antagonists, 2001-11*. Journal of Peace Research 51(3): 347–60.
- Maness, R. et al. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press. Oxford.
- Mahnken, T. G. (2018) *Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare*. Center for Strategic and Budgetary Assessments. Washington D.C.
- Martin, N. (7/12/2020). *US-Australia Partnership aims to bolster cyber defense of both countries.* GovConDaily. (Recuperado el 21/3/2021 de

https://www.executivegov.com/2020/12/us-australia-partnership-aims-to-bolster-cyber-defense-of-both-countries/).

- Martin, T. (22nd April 2018). *How North Korea's Hackers Became Dangerously Good*. L'Opinion. (Recuperado el 11/7/2020 de https://www.lopinion.fr/edition/wsj/how-north-korea-s-hackers-became dangerously-good-147906).
- Martinez, J. (16/20/2016). *Normativa de la UE de protección de datos y ciberseguridad (y II)*. Community of Insurance. (Recuperado el 1/4/2021 de https://communityofinsurance.es/2016/11/12/ue-proteccion-datos-ciberseguridad/).
- McNeil, T. (13/7/2019). *Why the United States Is the Only Superpower*. Tufts Now. (Recuperado el 9/2/2021 de https://now.tufts.edu/articles/why-united-states-only-superpower).
- Mearsheimer, J. J. (2006). *Structural Realism*. International Relations Theories: Discipline and Diversity, 71-88. Oxford: Oxford University Press.
- Meier, R. (15/9/2017). *Industry 4.0: New stage of development in the export business.* Switzerland Global Enterprise. (Recuperado el 12/2/2021 de https://www.s-ge.com/pt/node/720).
- Morgenthau, H.J. (1948). *Politics among Nations: The Struggle for Power and Peace.* New York: Alfred A. Knopf.
- Morillas, M. (2020). *La propaganda yihadista y los esfuerzos en contranarrativa.* Observatorio Internacional de Estudios sobre Terrorismo. (Recuperado el 3/2/2021 de https://observatorioterrorismo.com/eedyckaz/2020/08/La-propaganda-yihadista-y-los-esfuerzos-en-contranarrativa.pdf).
- Mueller, R. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* US Department of Justice.
- Mulrine, A. (2016). *How North Korea built up a cadre of code warriors prepared for cyberwar* .Christian Science Monitor. (Recuperado el 12/2/2021 de http://www.csmonitor.com/World/Passcode/2015/0206/How-North-Korea-built-up-a-cadre-ofcode-warriors-prepared-for-cyberwar).
- National Intelligence Council. (2019). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.* Office of the Director of National Intelligence. (Recuperado el 2/2/2021 de https://www.dni.gov/files/documents/ICA_2017_01.pdf).

- NNUU. (23/7/2004). *Report of the Secretary-General.* UN Doc. A/59/116.
- NNUU. (15/7/2011). *Report of the Secretary-General on Developments in the field of information and telecommunication in the context of international security.* UN Doc. A/66/152.
- NNUU. (20/7/2013). *Report of the Secretary-General.* UN Doc. A/65/154, p. 15.
- NSCI. E-Governance Academy. (2012). *What we do.*
- Nichols, M. (5/10/2019). *North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report.* Reuters. (Recuperado el 12/2/2021 de https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX).
- NSOROK (National Security Office of the Republic of Korea). (2019). *National Cybersecurity Strategy (12-1025000-000003-01).* (Recuperado el 1/1/2021 de https://unidir.org › cpp › state-pdf-export).
- Nye, J.S. (2017). *Deterrence and dissusasion in cyberspace.* International Security Vol. 41(3). Pp. 44-71.
- Nye, J.S. (2011). *The Future of Power.* Bulletin of the American Academy of Arts and Sciences. Vol. 64 (3). Pp. 45-52.
- Nye, J.S. (1990). *"Soft Power".* Foreign Policy. Vol. 80: 153–71.
- PAE (Portal de Administración Electrónica). (17/12/2020). *La nueva Estrategia de Ciberseguridad de la UE*. Noticias del PAE del Gobierno de España. (Recuperado el 12/4/2021 de https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2020/Diciembre/Noticia-2020-12-17-Nueva-estrategia-ciberseguridad-UE.html#.YIQi5N3tbX4).
- Park, J. et al. (2016). *South Korea's Options in Responding to North Korean Cyberattacks.* Journal of Information Warfare Vol. 15 (4). Pp. 86-99.
- Park, S. (2017). *Digital Capital.* Londres: Palgrave Macmillan.
- Parlamento Europeo. (2016). *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.* Documento 32016L1148.
- Parlamento Europeo. (2018). *European Parliament resolution of 13 June 2018 on cyber defence* (2018/2004(INI))

- Parsons, E. (2020). *Understanding the Cyber threat from North Korea.* F-Secure. (Recuperado el 12/10/2020 de https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-north-korea).
- Pawlak, P. (2015). *At a glance: Understanding Cyber Threats.* European Parliament Think Tank. (Recuperado el 3/3/21 de https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2015)564355).
- Perlroth, N. et al. (28/3/2013). *Cyberattacks Seem Meant to Destroy, Not Just Disrupt.* The New York Times. (Recuperado el 23/2/2021 de https://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html).
- Potter, R. (27/6/2018). *Is cyberwar politics by other means?.* Asia & the Pacific Policy Society. (Recuperado el 13/2/2021 de https://www.policyforum.net/cyberwar-politics-means/).
- Pzeworski et al. (1987). *Comparative Policy Research: Learning from Experience.* Nueva York: St. Martin's Press.
- Qiao, L. (2007). *Unrestricted warfare: China's master plan to destroy America.* Natraj Publishers, Dehradun.
- Raska, M. (24/9/2020). *North Korea's evolving cyber warfare strategy.* East Asia Forum. (Recuperado el 1/3/2021 de https://www.eastasiaforum.org/2020/09/24/north-koreas-evolving-cyber-warfare-strategy/).
- Reyes, R. (2009). *Diccionario Crítico de Ciencias Sociales: Terminología Científico Social.* Madrid: Plaza y Valdés Ediciones.
- Rodríguez, A. (2019). *Hacktivismo, lucha y protesta en internet.* El Orden Mundial. (Recuperado el 12/2/2021 de https://elordenmundial.com/hacktivismo-lucha-protesta-internet-ciber-geopolitica/).
- Saalbach, K.P. (2019). *Attribution of Cyber Attacks.* In: Reuter C. (eds) Information Technology for Peace and Security. Wiesbaden: Springer Vieweg.
- Sánchez del Campo, A. (8/11/2020). *5G rollout runs into problems in Europe.* Garrigues Digital. (Recuperado el 20/3/2021 de https://www.garrigues.com/en_GB/garrigues-digital/5g-rollout-runs-problems-europe).

- Sánchez Medero, S. (2010). *Los Estados y la Ciberguerra*. Boletín de Información. Vol. 217. Pp. 63-76.
- Scroxton, A. (15/1/2021). *US cyber security agencies get $9bn in Biden plan.* Computer Weekly. (Recuperado el 12/2/2021 de https://www.computerweekly.com/news/252494895/US-cyber-security-agencies-get-9bn-in-Biden-plan).
- Schmidt, B. (2002). *On the History and Historiography of International Relations.* London: Sage Publications.
- Schneier, B. (2003). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* Göttingen: Copernicus Books.
- Schwab. K. (2017). *The Fourth Industrial Revolution.* Nueva York (NY): Crown Publishing.
- Sciarrone, M. (2017). *Cyber Warfare: The New Front.* George. W. Bush Institute. (recuperado el 14/2/2021 from https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.html).
- Sigholm, J. (2013). *Non-State Actors in Cyberspace Operations.* Journal of Military Studies. Vol. 4 (1). Pp. 25-38.
- Singer, P.W. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.
- Smellser, J. (1976). *Comparative Methods in the Social Sciences.* Englewood Cliffs, N.J: Prentice-Hall.
- Staab, P. et al. (2018). *Cómo desafía China a Silicon Valley*. Nueva Sociedad: Tribunal Global. Vol. 275. Pp: 3-5.
- Sultan, O. (2019). *Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s.* The Cyber Defense Review. Vol. 4 (1). Pp. 43-60.
- Tan, A. (1/7/2020). *Australia to invest a record A$1.35bn in cyber security*. Computer Weekly. (Recuperado el 12/2/2021 de https://www.computerweekly.com/news/252485479/Australia-to-invest-a-record-A135bn-in-cyber-security).
- Tate, R. (2010). *Apple's Worst Security Breach: 114,000 iPad Owners Exposed.* Gawker Daily. (Recuperado el 4/3/2021 de https://web.archive.org/web/20100612222852/http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed).

- Tilly, C. (1984). *Big Structures, Large Processes, Huge Comparisons.* Nueva York: Russell Sage Foundation.
- Trend Micro. (2020). *Securing the Pandemic-Disrupted Workplace: Trend Micro 2020 Midyear Cybersecurity Report.* Trend Micro™ Research.
- Tran, D. (2018). *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack.* Yale Journal of Law and Technology. Vol. 20. P. 376.
- Tsagourias, N. (2015). "*The legal status of cyberspace*", en Nicholas Tsagourias y Rusell Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Edward Elgar Pub., pp. 13-29.
- Udenrigsministeriet (Oficina Del Embajador Tecnológico de Dinamarca). *TechPlomacy (technological-diplomacy).* Udenrigsministeriet Presse. (Recuperado el 1/2/2021 de https://techamb.um.dk/en/techplomacy/abouttechplomacy/-).
- United Nations Office on Drugs and Crime (UNODC). (2010). *The Globalization of Crime: A Transnational Organized Crime Threat Assessment.* United Nations Publications. New York.
- UNODC. (2013). *El uso de Internet con fines terroristas.* Nueva York: Naciones Unidas. (Recuperado el 12/3/2021 de https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf).
- Urrutia, O. (2013). *The role of think tanks in the definition and application of defence policies and strategies*. Revista del Instituto Español de Estudios Estratégicos. Vol. 2: 5-8.
- Van der Meer et al. (2015). *US Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations.* Netherlands Institute of International Relations. (Recuperado el 3/2/2021 de https://www.jstor.org/stable/resrep05348?seq=1#metadata_info_tab_contents).
- Van der Meulen, A. et al. (2019). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. RAND. (Recuperado el 14/3/2021 de https://www.rand.org/randeurope/research/projects/eu-cybersecurity-threats-responses.html).
- Van Riper, P. (1997) *La guerra en el siglo XXI.* Parameters. Vol. 27 (3). Pp. 2-4.
- ISSA. (2021). *ISSA Journal: Preparing the next Generation Security Proffesional.* Information Security Systems Association. Vol. 19 (3): 8-10.

- Waltz, K.N. (1979). *Theory of International Politics*. Boston (MA): Addison-Wesley.
- Wilson, C. (2009). *Cyber Crime*. En: F. D. Kramer, S. H. Starr & L. K. Wentz (eds.) *Cyberpower and National Security*. National Defense University Press, Washington D.C.
- Wintour, J. (11/8/2020). *Europe divided on Huawei as US pressure to drop company grows.* The Guardian. (Recuperado el 12/1/2021 de https://www.theguardian.com/technology/2020/jul/13/europe-divided-on-huawei-as-us-pressure-to-drop-company-grows).
- Wortzel, L. (17/11/2009). *Preventing Terrorist Attacks, Countering Cyber Intrusions, and Protecting Privacy in Cyberspace.* Testimony before the Subcommittee on Terrorism and Homeland Security. United States Senate.
- Zerzi, M. (2017). *The Threat of Cyber Terrorism and Recommendations for Countermeasures.* Center for Applied Policy Research. (Recuperado el 3/3/2021 de https://euagenda.eu/publications/the-threat-of-cyber-terrorism-and-recommenda-tions-for-countermeasures).
- Zetter, K. (2009). *Senate Panel: 80 Percent of Cyber Attacks Preventable.* Wired. (Recuperado el 3/3/2021 de 2009, https://www.wired.com/2009/11/cyber-attacks-preventable/).
- Zhang, Li. (2012). *A Chinese perspective on cyber war. International Review of the Red Cross.* Vol. 94, (886). P. 801.