Universitat Autònoma de Barcelona

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIOLOGÍA

GRADO EN CIENCIA POLÍTICA Y GESTIÓN PÚBLICA

TRABAJO FINAL DE ESTUDIOS

El ciberespacio, el poder del siglo XXI

Análisis del impacto de la ciberseguridad en las dinámicas de poder del sistema internacional

ESTUDIANTE: Álvaro Franco, 1604400

TUTOR: Pablo Aguiar Molina

Barcelona, mayo 2024

"*Debemos unirnos ahora, y sin demora, para mitigar esta amenaza y asegurar que las nuevas tecnologías sigan siendo una fuerza para el bien en lugar de una fuerza para el mal.*"

Vladimir Voronkov, Secretario General Adjunto de la
Oficina de las Naciones Unidas de Lucha Contra el Terrorismo

Índice

Resumen

El ciberespacio ha traído consigo un nuevo dominio en el que ejercer el poder y la guerra, en el panorama internacional. Cada día existen miles de ciberataques entre actores internacionales que buscan ampliar su esfera de poder, principalmente con motivos económicos. Por ello, es relevante indagar en las consecuencias que el ciberespacio representa para la lucha por el poder en el panorama internacional y si éste va a ser capaz de desplazar a los viejos campos de batalla. Con el objetivo de aplicar a la realidad todo lo estudiado a lo largo del trabajo, se utiliza un caso real de conflicto cibernético, el caso Stuxnet, que permite ejemplificar la teoría recogida. Estas páginas pretenden contribuir a dicha cuestión y arrojar luz sobre ella.

Palabras clave: Ciberseguridad, ciberespacio, Relaciones Internacionales, poder, sistema internacional, geopolítica.

Abstract

Cyberspace has brought with it a new domain in which to exercise power and war, on the international scene. Every day there are thousands of cyberattacks between international actors seeking to expand their sphere of power, mainly for economic reasons. For this reason, it is relevant to investigate how cyberspace represents a new domain in the struggle for power on the international scene and whether it will be able to displace the old battlefields. In order to apply to reality all that has been studied throughout this project, a real case of cybernetic conflict is used, the Stuxnet case, which exemplifies the theory collected. These pages are intended to contribute to this question and shed light on it.

Key words: Cybersecurity, cyberspace, International Relations, power, international system, geopolitics.

1. Introducción

Con el advenimiento de la era digital, el mundo cibernético ha emergido como un nuevo polo de interacción y competencia entre actores internacionales, en el cual el poder está más presente que nunca. De esta forma, se han liberado debates sobre si ha significado un cambio sustancial en la configuración del poder internacional, con argumentos a favor y en contra.

Es por ello, que el presente trabajo propone explorar este tema crucial, examinando los diferentes aspectos del poder en el mundo cibernético y su impacto en las relaciones internacionales. Para ello, se revisará la historia del sistema internacional cibernético, así como la aplicación de las teorías de las Relaciones Internacionales a las dinámicas de poder en el mismo. Además, se identifican las principales potencias cibernéticas y los elementos más básicos de su uso del poder en el sistema. No solo esto, también se realiza un breve análisis de las regulaciones cibernéticas y se identifica un caso de estudio que sirve de ejemplo para, por último, definir los desafíos y tendencias del sistema internacional cibernético en un futuro.

Así, se podrá no solo comprender cómo ha evolucionado la dinámica del poder en el mundo cibernético, sino también identificar las implicaciones de estos cambios para la estabilidad internacional, la seguridad cibernética y la gobernanza mundial. Estas páginas pretenden contribuir al debate en curso sobre el papel de la tecnología en la configuración del orden internacional y las estrategias que los actores internacionales emplean para usar su poder en la consecución de sus intereses en el mundo cibernético.

2. Objetivos

Las siguientes páginas buscan resolver el debate existente en torno a las implicaciones del sistema internacional cibernético en la balanza de poder: ¿Ha significado un cambio sustancial en las relaciones internacionales? ¿Ha habido una difusión del poder? ¿Han adquirido más poder los actores más pequeños? ¿Se tambalea la posición hegemónica de las principales potencias? ¿Son las regulaciones internacionales una garantía de seguridad?

Para elaborar el análisis, se parte de la hipótesis de que las cuestiones de ciberseguridad tienen un impacto primordial en la dinámica de poder entre las principales potencias cibernéticas mundiales (al influir en la capacidad de estos actores para ejercer influencia y control en el ámbito geopolítico). Esto se manifiesta en el fortalecimiento de su posición estratégica y en la potencial alteración de las relaciones internacionales tradicionales. Esta nueva amenaza digital, por tanto, deriva en una nueva forma de equilibrio de poder digital en el mundo contemporáneo.

3. Marco teórico

3.1. Ciberseguridad en el contexto de las Relaciones Internacionales

3.1.1. Términos y definiciones pertinentes

Las nuevas tecnologías han introducido en nuestro uso habitual nuevos conceptos que todavía no comprendemos íntegramente, como los referentes a las cuestiones de ciberseguridad. Por ello, es necesario primeramente dilucidar algunos conceptos imprescindibles para entender el contenido del presente trabajo. Estos son, principalmente, los términos que se puedan inferir del componente preposicional "*Ciber*" como, por ejemplo, ciberespacio o ciberseguridad.

En primer lugar, "***Ciber***", que deriva del inglés "*cyber*", es un "*Elemento compositivo creado por acortamiento del adjetivo cibernético, que forma parte de términos relacionados con el mundo de las computadoras u ordenadores y de la realidad virtual*" (DPD).

Así pues, cuando hablamos de **ciberespacio**, lo entendemos como "*un entorno virtual de información e interacciones entre personas*" (Kissinger, 2016), que, a su vez, es global y dinámico, apoyado en infraestructuras (físicas y virtuales) y sistemas de información y telecomunicaciones (Quintana, 2016). Diferentes actores pueden participar de este sistema para conseguir sus objetivos, también estados, que pueden llevar a cabo actividades para ejercer su poder en el ciberespacio, como actividades ilícitas o ilegales con fines económicos, políticos o personales (Aguilar et al., 2011).

Finalmente, si hacemos referencia a la **ciberseguridad**, a pesar de que encontramos alrededor de una cincuentena de definiciones (Maurer & Morgus, 2014), puede entenderse que ésta "*incluye las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de dichos sistemas y de otras personas afectadas por las ciberamenazas*." (Parlamento y Consejo Europeo, 2019/881). Esta protección implica perseguir la "*confidencialidad, integridad y disponibilidad de datos, recursos y procesos mediante el uso de controles administrativos, físicos y técnicos*" (Guiora, 2017).

3.1.2. Evolución del sistema internacional cibernético y la ciberseguridad

El ciberespacio se ha consolidado como imprescindible y esencial para nuestras vidas diarias durante las últimas décadas, pues casi la mayoría de nuestras actividades diarias emplean Internet. Consiguientemente, las ciberamenazas también llegaron para quedarse. Veamos la evolución, brevemente, del sistema internacional cibernético.

Siguiendo a Palfrey, podemos identificar 4 fases, principalmente: La primera fase, Era Abierta, que ocurre desde su nacimiento hasta el 2000; la segunda, Acceso Denegado, del 2000 al 2005; la tercera, Acceso Controlado, del 2005 al 2010 y; la cuarta, Acceso en Disputa, del 2010 a la actualidad (Palfrey, 2010).

En la primera de estas etapas, Era Abierta, se construyen las bases de la red global, con vistas a la democratización de la información libre, principalmente en EEUU. Internet representaba, dada su natividad temprana, un espacio imposible o muy difícil de regular (Palfrey, 2010). Su nacimiento suponía que ahora los ordenadores podían proporcionar y recibir información sin conexiones físicas, naciendo así el ciberespacio. Es a principios de los 70 cuando empiezan a aparecer los primeros programas maliciosos en Internet, pero es durante los 80 que aparecen los primeros ataques relevantes en el ciberespacio y la ciberseguridad se generaliza y constituirá un nuevo mercado incipiente. El 2 de noviembre de 1988, el Gusano Morris infectó unos 6000 ordenadores del *Massachusetts Institute of Technology*, el primer *malware* de la historia (Holgado, 2022). Los 90 son, sin embargo, el periodo de máxima consagración de esta etapa, con el *boom* del correo electrónico y la llegada de ordenadores a considerables hogares (Sánchez, 2022).

En la segunda de estas etapas, Acceso denegado, Internet empieza a recibir regulaciones, filtros y bloqueos a la información por parte de muchos estados, primordialmente China (Orozco, 2019). Ante la apertura del ciberespacio, aquí los estados pretenden dibujar sus fronteras mediante controles en el mismo. Aquí, crece el uso de *phishing*, correos maliciosos que suplantan una identidad de confianza (Poitevin, 2023).

La tercera etapa, Acceso controlado, destaca por que los Estados empiezan a utilizar mecanismos legales que pretenden controlar el ciberespacio, como los registros, licencias o métodos de vigilancia (Palfrey, 2010). Aparecen compañías relevantes como McAfee o Panda Security, que traen la ciberseguridad a los dispositivos más convencionales (Crego, 2023).

Por último, en la cuarta etapa, Acceso en Disputa, la regulación empieza a confrontar tanto a ciudadanía como a empresas privadas contra los gobiernos, lo que ha desembocado en una disputa acerca de la gobernanza del ciberespacio (DeNardis, 2009). Es aquí cuando empiezan a ocurrir los ataques más elaborados, a mayor escala y recurrentes, incorporando también la Inteligencia Artificial para mejorar la detección y respuesta (Balleza, 2023). Tal es el nivel que en 2023 alcanzamos a leer titulares como: "*El cibercrimen alcanza niveles inéditos: 90 millones de ataques anuales que cuestan 10,5 billones de euros"* (Limón, 2023).

3.1.3. Aplicación de las teorías de las Relaciones Internacionales a la ciberseguridad

Si una cosa es clara, es que "*Las Relaciones Internacionales están hoy, en todo caso, sobre provistas de teorías de todo tipo imaginable*" (Wendt & Sindal, 2009) y, sin embargo, la ciberseguridad ha sido tratada de forma muy exigua. Es por ello por lo que es conveniente aplicarlas e investigar si se adaptan apropiadamente a la cuestión. Principalmente, nos centraremos en el Realismo y Liberalismo (por ser las teorías hegemónicas) y, para realizar el análisis, el enfoque se centra en los siguientes elementos: actores, sistema internacional cibernético y ciberpoder.

Dada la extensión de perspectivas teóricas, realistas y liberales, es útil identificar unos supuestos comunes en ellas, que permitan partir de ese punto para esclarecer sus conexiones teóricas básicas.

Con referencia al Realismo, encontramos que, de acuerdo con Barbé, 1) El Estado es el actor principal; 2) El interés nacional (de seguridad) guía la acción de los Estados; 3) El sistema internacional es anárquico; y 4) El poder y la seguridad son los valores primarios del Estado (Morgenthau, 1949; Waltz, 1979). Así, partiendo de la base de que el sistema internacional (anárquico) es "*carente de un poder centralizado*" (Barbé, 1987), podemos establecer relaciones con el sistema cibernético, pues no existen tampoco instituciones de gobernanza en él y, por consecuencia, son los Estados los encargados de ejercer su soberanía. Esto implica que se puedan identificar "*Acumulación de capacidades cibernéticas y percepciones mutuas de amenaza y competencia entre estados en un número selecto de casos."* (Craig & Valeriano, 2018). Es decir, se replica el dilema de seguridad como resultado de esta anarquía, pues el incremento de seguridad de un estado es visto como una amenaza para otro estado (Jervis, 1976). Todo esto puede desarrollar una carrera armamentística e, incluso, recurrir a la disuasión en el ciberespacio (Orozco, 2019). Sin embargo, las superpotencias más dependientes de las tecnologías son aquellas más vulnerables a posibles ataques (Kolet, Lambakis, & Kiras, 2002), pero quizás son estas también las que tienen más capacidad de ciberdefensa y, si es necesario, responder.

En cuanto al Liberalismo, se entiende que 1) El Estado no es el único actor internacional relevante; 2) La política interna del Estado guía la política exterior del mismo; 3) La anarquía del sistema se mitiga a través de normas e instituciones; y 4) La cooperación es predominante al conflicto (Jørgensen, 2018). Esta teoría añade, junto al Estado, otros actores no Estatales con capacidad de influencia cibernética transnacional (Keohane, 1984), esto es, el ciberpoder se ha diversificado, pues quien tiene un dispositivo inteligente tiene un arma. Además, se ha

penetrado la soberanía del estado por la relevancia que han adquirido actores no estatales, que interaccionan transnacionalmente, de forma cibernética (Eriksson & Giacomello, 2006). La anarquía realista, por otro lado, se supera porque mediante la normas, instituciones u organizaciones "*compuestas por estados y actores no estatales dedicados al mantenimiento de la seguridad cibernética disminuiría en gran medida la incertidumbre que enfrenta actualmente cada estado*" (Petallides, 2012). Es por ello, que se alza como imprescindible la "*cooperación para mitigar la peligrosidad de las amenazas en el dominio digital, incluyendo la colaboración entre las esferas pública y privada, civil y militar."* (Bartolomé, 2023).

Vemos, por tanto, la aplicabilidad del Realismo y Liberalismo, como teorías de las Relaciones Internacionales, a la nueva era cibernética. Sin embargo, es necesario no caer en el hermetismo teórico, pues puede ser útil entenderlas de forma conjunta, ocasionalmente.

3.2. Las principales potencias cibernéticas mundiales

La disciplina de las RRII, generalmente, entiende las potencias como "*aquellos estados que establecen las reglas del juego y que disponen de recursos y son capaces de movilizarlos para defender dichas reglas*" (Barbé, 1995). Cuando un estado tiene capacidad para definir las reglas del juego, entendemos que tiene poder para ejercer influencia en el sistema internacional. Por consiguiente, en relación con el sistema cibernético, entendemos como una potencia cibernética o ciberpotencia aquellos estados que disponen de ciberpoder, es decir, "*El potencial para usar el ciberespacio a fin de lograr los resultados deseados.*" (Parker, 2014).

Así pues, ¿cuáles son las diferentes ciberpotencias que dominan el sistema internacional cibernético? Podemos distinguir, utilizando el estudio de Gráficos de radar que realiza el estudio National Cyber Power Index[1], diferentes tipos de potencias cibernéticas, pues no todas éstas pugnan en la misma escala.

El primer liderazgo mundial en términos de ciberpoder radica en Estados Unidos, al que vamos a calificar de *hiperpotencia*[2] cibernética y China una *superpotencia*, que le sigue de cerca. Ambos países son las economías tecnológica y económicamente más capaces, además de que disponen del mayor número de usuarios *online* y las empresas más punteras en cuestión de ciberseguridad. No solo esto, la ciberseguridad es prioritaria para ambos gigantes y sus discursos pugnan por ser los conductores de la conversación internacional, es decir, por acercar

[1] Ver anexos para descubrir Gráficos de radar que descomponen el ciberpoder de las potencias (Voo, Hemani, & Cassidy, 2022).

[2] Aprovechando el término introducido por Hubert Védrine, he decidido calificar a EEUU de hiperpotencia cibernética para elevar su categoría por encima de una superpotencia, pues la mayoría de los autores consideran que este país reside en una escala superior a todos los demás. Este término, por tanto, permite distinguir a EEUU sobre las otras superpotencias y potencias, debido a la no existencia de un rival con las mismas capacidades.

la regulación internacional del ciberespacio hacia sus intereses y visiones, pues mientras EEUU tiene una visión más aperturista y liberal del ciberespacio, China cree necesarias las regulaciones y restricciones en él (Seagal, 2016). El resultado de todo esto es que ambos países dominan el espacio internacional en cuanto a capacidades financieras, de vigilancia, inteligencia, comerciales, de control de la información, destructivas y normativas. Siguiendo el estudio de Voo, Hemani y Cassidy, las mayores diferencias entre ambos países residen en que Estados Unidos, tiene mayor capacidad defensiva que China, mientras que ésta última es más capaz financieramente (Voo, Hemani, & Cassidy, 2022).

Completando el pódium encontramos a Rusia, una *gran potencia*, que posee los mejores hackers del mundo, con gran capacidad ofensiva y gran capacidad de control de la información. Rusia ejerce una guerra propagandística en la red, un gran número de hackers afines al régimen (*hacktivistas*) operan en su beneficio (Calzado, 2021). Sin embargo, su infraestructura tecnológica y empresarial no está al nivel. Conocedora de esto, Rusia está invirtiendo en esta lacra y se espera que con los años pueda pugnar con las anteriores superpotencias. Por ejemplo, desde el estallido de la guerra en Ucrania, Rusia ha incrementado en un 300% los ataques cibernéticos a la OTAN (France24, 2023).

Un peldaño debajo, encontramos *potencias cibernéticas* como Reino Unido, Australia, Países Bajos, Corea del Sur, Vietnam o Francia que, sin tener las capacidades, influencia o infraestructura de los 3 grandes, sobresalen por encima de los que les siguen por detrás. Por ejemplo, Reino Unido domina discursivamente al respetar la influencia norteamericana y dispone de servicios de inteligencia potentes (MI5); Australia es pujante en cuanto a defensa; Países Bajos tiene capacidad normativa y buenos servicios de inteligencia (AVID); al igual que Corea del Sur; Vietnam ejerce un gran control en la red y la información; Francia, para acabar, dispone de buenos servicios de inteligencia (DGSE) y capacidades defensivas.

Por último, existen países que ejercen un rol a destacar en el sistema internacional cibernético hasta el punto de calificarlas como *potencias emergentes*. Aquí ingresarían Irán, Corea del Norte e Israel. En primer lugar, Irán es uno de los países con más actividad en el dominio cibernético, centrándose en el control de la información para silenciar a la oposición, así como menoscabar estados rivales (Denning, 2017). Además, es un estado con unos servicios de inteligencia considerados de los mejores del mundo, el ECI, como también posee una gran red de *hacktivistas* (Calzado, 2021). En segundo lugar, Corea del Norte, que colabora con Irán en materia de ciberseguridad, no ha declarado una estrategia concreta de ciberseguridad, aunque podemos evidenciar que sus ataques se dirigen a ser fuentes de ingresos económicos (Iniseg, 2020). Por último, Israel, con uno de los mejores servicios de inteligencia del mundo y un faro

de influencia de EEUU en su región, está desarrollando potentes empresas de ciberseguridad, financieramente crecientes, como Check Point o CyberArk.

En resumen, a través del estudio y las clasificaciones de diferentes autores[3], he identificado diferentes ciberpotencias que, con el objetivo de clasificarlas de forma escalada, he distinguido en diferentes categorías en función de sus capacidades: Una hiperpotencia (Estados Unidos), una superpotencia (China), una gran potencia (Rusia), potencias (Reino Unido, Australia, Países Bajos, Corea del Sur, Vietnam, Francia) y potencias emergentes (Irán, Corea del Norte e Israel).

3.3. Impacto de la ciberseguridad en la dinámica de poder

3.3.1. El poder en el sistema internacional cibernético

La atribución

La guerra, como proyección del poder por parte de los actores internacionales (principalmente Estados), no siempre ha sido igual. Pues a lo largo de siglos la expresión de la guerra fueron batallas terrestres y marinas, hasta llegar a la invención de los vehículos aéreos, que llevaron al cielo las ofensivas. No solo esto, con el arribo del hombre al espacio, podemos concebir que este también es un dominio en el cual los Estados pugnan para ejercer su poder (véase la carrera espacial de la segunda mitad del siglo pasado). Sin embargo, existe un quinto dominio, el cibernético, en el cual también los Estados velan por dominar de diferentes métodos. En este contexto, es esencial examinar cómo se manifiesta y se ejerce el poder en el sistema internacional cibernético.

Las amenazas cibernéticas son con mucha frecuencia perpetradas desde el anonimato, con el objetivo de evitar un posible contrataque. En caso de ataque cibernético, la **atribución** es, por tanto, el primer paso. No solo esto, es un paso relevante para una buena defensa, pues la capacidad de atribución también repele ataques potenciales, por miedo a las consecuencias.

Thomas Rid y Ben Buchanan estudiaron la atribución y llegaron a una serie de conclusiones, partiendo de la base de que, parafraseando a Wendt, "*la atribución es lo que los estados hacen de ella*" (Rid & Buchanan, 2015). La primera de las conclusiones es que la atribución no es una ciencia sino un arte, luego son las habilidades, herramientas y cultura de la organización lo que determina la capacidad de esta. En segundo lugar, la atribución es un procedimiento matizado y de capas múltiples, no una respuesta binaria que puede solucionarse o no. Por último, los daños

[3] (Seagal, 2016), (Singer & Friedman, 2014), (Calzado, 2021), (Mata-Sánchez, 2023), (Jiménez, 2015).

causados son proporcionales a los esfuerzos materiales y políticos consiguientes que un gobierno invierte (Rid & Buchanan, 2015).

No solo esto, argumentan en contra de diferentes posiciones comunes en el debate de la ciberseguridad. Generalmente, se dan cuenta que de una forma u otra los estados son capaces de realizar la atribución con éxito. Asimismo, en contra del pensamiento de que internet ha diversificado el poder sustrayéndoselo a los Estados, argumentan que son los estados los únicos que disponen de recursos y la inteligencia suficiente para, mediante la atribución, atacar con certeza a sus objetivos y, como ya se ha comentado, evadir posibles ataques. Finalmente, argumentan que contrariamente a la creencia de que los países industrializados son los más vulnerables, realmente, son los que disponen de más capacidades defensivas y ofensivas (Rid & Buchanan, 2015). De la mano de la capacidad de atribución, viene la capacidad de disuasión, pues si un estado puede identificar quién le ha atacado, puede emprender represalias (Singer & Friedman, 2014).

Con esto vemos que, el quinto dominio sigue siendo un reflejo de que el poder pertenece a quien tiene capacidades materiales e influencia y, a pesar de que se haya diversificado, todavía son los Estados los que lo poseen principalmente.

Poder blando y poder duro

El ejercicio del poder no es uniforme, tampoco en el sistema internacional cibernético. Existen innumerables formas de ejercer el poder, pero Joseph S. Nye Jr. las clasificó todas en dos concepciones: el **poder duro** y el **poder blando**. Así, entiende que "*el comportamiento del poder duro se basa en la coerción y el pago"* mientras que "*el comportamiento del poder blando se basa en la formulación de agendas, la atracción o la persuasión"* (Nye, Jr, 2010).

Nye entiende el ciberpoder como la capacidad de adquirir resultados beneficiosos y deseables a través de instrumentos, mecanismos e información del quinto dominio. Además, se da cuenta de que el poder cibernético también puede ejercerse en su aspecto "duro" y "blando", dependiendo del método utilizado para ejercer influencia. La siguiente tabla resume estos métodos.

Objetivos del poder cibernético

	Dentro del ciberespacio	Fuera ciberespacio
Instrumentos de la información	Duro: Ataques cibernéticos Blando: Establecimiento de normas y estándares	Duro: Ataques a sistemas electrónicos de control a distancia de la información (SCADA) Blando: Campañas diplomáticas
Instrumentos	Duro: Controles estatales	Duro: Atacar a rúters o cables

físicos	Blando: Activismo cibernético (*Hacktivistas*)	Blando*: Naming and shaming* contra proveedores

Fuente: (Nye, Jr, 2010).

Cabe diferenciar, primeramente, que el ejercicio del poder puede darse dentro o fuera del ciberespacio. No es lo mismo atacar un sistema informático mediante un software malicioso a destruir, físicamente, ordenadores o diferentes dispositivos informáticos. Además, es necesario distinguir entre los instrumentos de la información, que atañe a el uso de la información online; y los instrumentos físicos, que proporcionan recursos de poder para utilizar en el mundo cibernético (Nye, Jr, 2010).

Dentro del ciberespacio, los instrumentos de la información nos pueden permitir ejercer el poder mediante ataques maliciosos que denieguen el servicio del ciberespacio (frecuentemente con fines económicos) o, por contra, mediante la capacidad de influencia se puede dominar la agenda, las normas y las instituciones que dominan las ideas sobre el ciberespacio. De hecho, cabe destacar que los actos más frecuentes son aquellos destinados a ejercer influencia (Pernik, 2018). En cuanto a los instrumentos físicos, los estados pueden establecer controles y normativas, incluso supraestatales, que mitiguen la anarquía del ciberespacio y, no solo esto, los *hacktivistas* están recibiendo importancia recientemente porque son medios propagandísticos, con fines políticos, de los Estados (como por ejemplo Rusia).

Fuera del ciberespacio, el poder de la información permite ejercer poder duro dañando infraestructura física de otros países que sustenta el ciberespacio en los mismos. El poder blando podría ejercerse mediante la atracción de ciudadanos de otros países mediante campañas diplomáticas publicitadas por internet (Corea del Sur lo está ejerciendo últimamente). Los instrumentos físicos implican, primero, los ataques y sabotajes a los sistemas de comunicación y, segundo, el uso del *naming and shaming* contra empresas y proveedores que se consideren abusivos (manifestaciones contra Yahoo en 2006).

Para acabar, Nye también dibuja una triple capa del poder en el dominio cibernético. En primer lugar, hablamos de que A incita a B a realizar algo que B propiamente no haría. Segundo, A imposibilita la elección de B al descartar opciones de esta última (control de agenda). Tercero, A moldea las preferencias de B para que obvie algunas no deseadas.

Se ha podido ver, para concluir, que el Sistema Internacional Cibernético, aunque difunde el poder entre nuevos actores diferentes a los Estados, "*es poco probable que cambie las reglas del juego en las transiciones de poder*" (Nye, Jr, 2010), pues la difusión del poder no es equivalente a la paridad ni la sustitución, porque el poder relativo sigue perteneciendo a los más grandes, a las potencias. Sin embargo, se espera que el ejercicio de la influencia, el poder blando, se anteponga al poder duro en el ciberespacio (Bejarano, 2013).

3.3.2. La regulación del ciberespacio

Actualmente no existen regulaciones vinculantes efectivas que normalicen el uso del poder en el ciberespacio o sirvan para reclamar responsabilidad internacional. Sin embargo, éste mitiga su anarquía mediante mecanismos expresos y tácitos, resultado de las iniciativas de diferentes actores internacionales de emprender un camino hacia la regulación del sistema internacional cibernético.

Podemos identificar, entonces, 4 tipos de regulaciones que afectan al ciberespacio: la ley, las normas sociales, el mercado y el código (Lessig, 1998).

En primer lugar, las leyes de los propios estados o de organizaciones supranacionales de estados. Por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea[4] o el Convenio sobre cibercriminalidad de Budapest[5]. En segundo lugar, las normas sociales son reglas que regulan conductas y, en caso de inobservancia, exponen sanciones sociales. Por ejemplo, el rechazo social hacia la pornografía infantil ha conllevado a su penalización, es decir, a convertirla en un delito. En tercer lugar, el mercado también es un condicionante al resultar una barrera de entrada a diferentes actores, porque limita mediante los precios los actores que participan en el sistema cibernético, por ejemplo, a determinados precios solo una pequeña cantidad de actores pueden permitirse desarrollar buenos sistemas de defensa o programas de ataque. Por último, el código, entendido como el *software* y *hardware*, es *"el conjunto de protocolos, de reglas, implementadas o codificadas en el software del propio ciberespacio, que determinan cómo las personas interactúan, o existen, en este espacio."* (Lessig, 1998). En resumen, el código es la estructura tecnológica del ciberespacio, que los individuos no podemos escoger, simplemente nos viene dada por los creadores de este. Un ejemplo es que, en ocasiones, debemos identificarnos para acceder a determinados portales y no podemos resignarnos a ello, por lo que este tipo de mecanismos determinan la arquitectura del ciberespacio y el uso que hacemos de él.

Sin embargo, ¿por qué no existe ningún tratado internacional en este ámbito? Rex Hughes, asesor de la OTAN, fue preguntado acerca de si Estados Unidos y sus aliados querrían un *cibertratado* y su respuesta fue: "*la respuesta oficial es sí, queremos que haya reglas de tránsito y que se aplique el derecho de los conflictos armados. Pero extraoficialmente la respuesta es*

[4] Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

[5] Convenio del Consejo de Europa, con 56 firmantes, por el cual se busca la cooperación internacional en contra de ciberdelitos como la pornografía infantil, delitos de odio, fraude o derechos de autor. Es un precedente sobre el que trabajar.

no. Los países que tienen capacidades avanzadas quieren preservarlas" (Singer & Friedman, 2014). La respuesta es clara, pues las ciberpotencias no quieren atarse las manos mientras que sus rivales pueden seguir progresando. No solo esto, no existe consenso en las visiones que tienen los países acerca del uso del ciberespacio. Como se ha mencionado anteriormente, las visiones de los países occidentales no concuerdan con las que propugnan China o Rusia, por ejemplo.

En cuanto a Naciones Unidas, desde 1998, a raíz de un proyecto de resolución presentado por la Federación Rusa, se presentan informes anuales a la Asamblea General con las opiniones de los Estados Miembros en materia de ciberseguridad. Además, a partir de 2004 han existido 6 Grupos de Expertos Gubernamentales (GEG) con la labor de identificar y estudiar los retos y amenazas que presenta la ciberseguridad a escala internacional (Naciones Unidas, 2022).

El resultado han sido informes con definiciones, conclusiones y recomendaciones, pero en ningún caso un marco normativo vinculante sino una serie de principios generales (Andover Llinás & Shore, 2023):

1. Cooperación entre estados para aumentar la estabilidad y la seguridad cibernética, con el objetivo de desalentar prácticas hostiles para la paz internacional.
2. Obligación de proteger, es decir, es necesario siempre solventar el problema de la atribución antes de tomar conclusiones precipitadas.
3. Los Estados no deben permitir, de forma consentida, que se lleven a cabo prácticas cibernéticas maliciosas en su territorio.
4. Multilateralismo con el objetivo de contrarrestar el terrorismo y delincuencia en el ciberespacio.
5. Primacía en el ciberespacio de los Derechos Humanos.
6. Respetar la infraestructura crítica y tecnológica de los Estados.
7. Proteger de manera proactiva la infraestructura crítica propia contra posibles ciberataques.
8. Deber de responder mediante apoyo a la infraestructura crítica, bajo ataque, de otros Estados bajo.
9. Tomar medidas que se centren en proteger la cadena de suministros de tecnología, con el fin de evitar sabotajes y posibles tentaciones de perturbar el sistema.
10. Cooperación que tenga como objetivo compartir información para resolver posibles vulnerabilidades en la ciberseguridad.
11. No incentivar ni sustentar la acción cibernética maliciosa.

Esta serie de principios pretenden conducir el comportamiento de los actores en internet. Sin embargo, clara es la evidencia de que "*La falta de un marco jurídico determinado que esté*

claramente aceptado por los Estados provoca la existencia de vacíos legales y situaciones de desamparo que son aprovechadas con fines ilícitos por otros Estados y actores no estatales." (García, 2021). El resultado de esto es que la amplia interpretación de estas normas dificulta la reclamación de responsabilidad internacional de los actores del sistema y, con ello, la aplicación de consecuencias legales pertinentes (Ambos, 2015).

4. Caso práctico

4.1. Stuxnet y sus consecuencias en el poder global

Con el objetivo de ejemplificar lo anteriormente expuesto y mostrar la evidente y estrecha relación entre ciberseguridad y geopolítica, en este apartado se pretende explicar brevemente el caso de Stuxnet.

La relevancia de esta cuestión recae en que fue a partir de aquí que "*se dio a conocer un virus informático que marcó un hito por sus efectos que cruzan la línea entre lo virtual y el mundo real, y por conjugar además elementos tecnológicos y geopolíticos, dando luz de lo que podrían ser las próximas guerras.*" (Silva, 2018). Cabe obviar que la complejidad del caso escapa del límite del presente trabajo.

4.1.1 Contexto histórico y político

El ataque se enmarca en un conflicto geopolítico extenso entre Estados Unidos (e Israel) contra Irán, por su emergencia como potencia regional con capacidades nucleares en Oriente Medio (Gyuris, 2018). Es necesario recordar que la relación entre los dos aliados con Irán ha sido compleja, desde que este empezó a mostrarse hostil contra occidente (sobre todo a raíz de la revolución islámica de 1979). Tal fue, que cuando las ambiciones nucleares de Irán se consideraban ya amenazantes, EEUU comenzó en 2005 a planear estrategias de limitación de los desarrollos nucleares de Irán, afirmando en 2008 que defenderían "*vigorosamente a sus amigos e intereses*" en la región (Rice, 2008).

4.1.2 Stuxnet, la primera ciberarma

Stuxnet fue la primera ciberarma de la historia, de tal manera que mediante el espacio virtual pudo infligir daños en el espacio físico. Concretamente, el objetivo fue la planta de enriquecimiento de uranio de la ciudad iraní de Natanz.

Este ataque se llevó a cabo contra 3 capas: la capa tecnológica (dispositivos electrónicos Siemens S7-417, Windows) por la que se propaga el *malware* o *gusano*; la capa del sistema informático por el cual se lleva a cabo la manipulación (controladores industriales) y la capa física en la que se ejerce el daño real (rotores-centrífugos de la central) (Scheneier, 2013). Así, el ataque se materializó de dos formas: sobrepresurizando las centrifugadoras y sobreacelerando

los rotores[6]. Seguramente, Stuxnet fue introducido en la central mediante un USB (Delgado, 2020-2021).

A pesar de que podrían haber volado por los aires la central, se prefirió su asfixia, porque el sistema estaba diseñado de tal forma que mostraba que no existían errores en la central, siendo así un rompecabezas para los ingenieros iraníes (Bueno, 2019). Además, el *malware* se propagó en 2010 por los sistemas de internet hacia otros países, afectando a todos los dispositivos Siemens S7-417. Sin embargo, el gusano estaba configurado para únicamente dañar a los que respondían a una configuración exacta a la de la central de Natanz. Por ello, se sospecha la participación de "espías nucleares" (Silva, 2018).

En definitiva, Stuxnet supuso la destrucción y el daño, entre los años 2009 y 2010, de hasta 1000 equipos de planta de enriquecimiento de uranio de Natanz (Albright, Brannan, & Walrond, 2010).

4.1.3 Atribución y motivos

A pesar de que la atribución no es clara, existe un consenso generalizado entorno a la responsabilidad de Israel y EEUU. David Sanger, periodista del New York Times encontró "*entre cinco y diez funcionarios (de EEUU) gubernamentales de alto rango deseosos de alardear de la operación*" (Gyuris, 2018). Esta operación, con el nombre de Juegos Olímpicos, fue llevada a cabo con la colaboración necesaria de Israel, según la misma revista. Además, no existen muchos actores capaces de un ataque de tal magnitud.

Ahora, ¿por qué se llega a tal punto? La teoría de las RRII puede ayudar a entenderlo y el Neorralismo es realmente pertinente. Así, se han de tener en cuenta cinco supuestos (Mearsheimer, 2006); (Balsalobre, 2016):

1. El sistema internacional es anárquico: Las potencias interactúan, con sus capacidades, compiten (lo que uno gana, el otro lo pierde) en un sistema incierto. La estructura del sistema será su único constreñimiento y la principal causa del conflicto.
2. Las potencias tienen capacidades militares ofensivas: Las utilizan para defender sus intereses.
3. No existe certeza en las intenciones: Las potencias desconocen si existen pretensiones ofensivas o defensivas, que busquen alterar o mantener el balance de poder, respectivamente.
4. Los estados buscan su supervivencia.
5. Las potencias son racionales: buscan maximizar sus beneficios y son calculadoras.

[6] Ver anexos para profundizar en las cuestiones técnicas del ciberataque Stuxnet, puesto que no es el objeto principal del trabajo.

En primer lugar, partimos de la base de que las pretensiones de Irán entorno a la proliferación nuclear representan un aumento de sus capacidades ofensivas y, por tanto, una amenaza para Israel, el principal potencial perjudicado. Por ello, lo verdaderamente importante es "*el cambio de status quo a partir del incremento de capacidades por parte de Irán con el desarrollo del programa nuclear, y la amenaza que representa para Israel*" (Llinas, 2017).

En segundo lugar, aprovechando de su amistad con EEUU y su enemistad con Irán, Israel busca apoyo del gigante norteamericano para contrarrestar el desarrollo del arma (Gamero-Garrido, 2017). Lo que claramente se vislumbra aquí es la necesidad de seguridad, como consecuencia a una situación de incertidumbre, por parte de Israel, equilibrando la balanza de poder.

Finalmente, el ciberataque, representó la satisfacción del interés de seguridad a partir de sofocar la amenaza. La estructura empujó a Israel y EEUU a actuar ante un aumento de capacidades de un actor que escalaba en su posición dentro de la misma, acaparando poder relativo. Con todo ello, a través de Stuxnet "*los gobiernos de EEUU e Israel lograron efectivamente ralentizar el programa nuclear iraní, alterando el balance de poder en medio oriente y en el sistema internacional*" (Gyuris, 2018).

5. Desafíos emergentes y tendencias futuras

Con todo esto, ¿qué podemos esperar en el futuro? El profesor Josep Ibáñez lo tiene muy claro. Él argumenta que se espera que "*se mantenga e incluso se refuerce la presencia de la política y el poder en internet del mismo modo que lo hará la utilización de internet con fines políticos y como instrumento de poder*" (Ibáñez, 2010). Además, es consciente de que el ciberespacio es un campo más en disputa y, por ello "*las instituciones internacionales que ejercen autoridad más allá de los Estados necesitan estrategias de legitimación de sus actividades de gobernanza global pero estas estrategias son tanto o más necesarias si nos referimos a los actores y autoridades de tipo privado.*" (Ibáñez, 2010).

Por otro lado, P.W. Singer y Allan Friedman identifican 5 principales tendencias en relación con la ciberseguridad (Singer & Friedman, 2014). En primer lugar, la computación "en la nube" comporta una acumulación ingente de información en aquellas compañías que la proporcionan. Es decir, como "subir los archivos a la nube" es menos costoso y ocupa menos espacio que almacenarlos físicamente, estas compañías acaban acumulando toda la información de los individuos. Ligado a esto, la segunda tendencia es la gestión del *Big Data* y la vulnerabilidad de la privacidad, pues estas compañías operan con nuestros datos e información, con el objetivo de obtener rédito económico, muchas veces sin el conocimiento del usuario, derribando así "*fronteras humanas sociales, legales y éticas que aún no estamos preparados para cruzar.*". En

tercer lugar, los autores hablan de la "revolución móvil", es decir, los cada vez más pequeños ordenadores que a diario utilizamos y transportamos son más vulnerables que un PC ordinario, son objetivos móviles para los ciberdelincuentes. No solo esto, en países subdesarrollados, el uso del móvil es mucho más frecuente para las gestiones diarias que en el mundo occidental, a pesar de que lo disponen de la misma seguridad informática. En cuarto lugar, se hace referencia a la pugna entre diferentes narrativas acerca del funcionamiento de internet, esto es, se puede prever una disputa entre visiones opuestas acerca de cuestiones como la libertad de expresión, la libertad de uso o la privacidad. Debemos recordar que la visión de China, cada vez más pujante en internet, no es la misma que la de EEUU, y todo dependerá del poder de convicción de las potencias. Por último, el "Internet de las Cosas (*IoT*)" representa la interconexión de los aparatos de nuestro día a día, con el objetivo de acomodar nuestra rutina mediante la tecnología. Puede resultar obvio el peligro que se deriva de esto, pues ¿qué perjuicios supondría el sabotaje de la domótica o infraestructura crítica a nivel nacional?

Como se ha mencionado anteriormente, es necesario reafirmar la relevancia del multilateralismo para dar respuesta internacional a todos estos desafíos, con el objetivo de mantener la paz y la seguridad internacional.

6. Conclusiones

A lo largo de estas páginas se ha podido estudiar brevemente lo que supone el ciberespacio para la configuración actual del poder a nivel internacional. El sistema internacional cibernético es un campo de batalla más, cada vez más relevante y cada vez más pugnado entre las diferentes potencias, pues ven aquí una vía más para aumentar su poder. Como ya se ha visto, se prevé que cada vez más este dominio sea utilizado por las autoridades como instrumento de poder, con fines políticos o geoestratégicos.

Asimismo, el ciberespacio no ha alterado sustancialmente las relaciones de poder a nivel internacional, pues los poderosos siguen siendo poderosos y los débiles, si bien han podido acumular cierto poder, no pueden contrarrestar a los más grandes, tal como se ha visto en el caso de Stuxnet. La anarquía del sistema internacional cibernético todavía perdura, pues no existen aún suficientes normas internacionales relevantes que la mitiguen. Según el realismo, bajo este contexto, la emergencia del ciberespacio, pues, no ha cambiado las dinámicas de poder instauradas bajo los otros dominios.

El cambio sustancial radica entonces, según en liberalismo, en la necesidad de cooperación y multilateralismo para dar lugar a normas internacionales que atenúen la anarquía, que limiten el uso del ciberpoder de forma perjudicial y castiguen a los agresores a la vez que proteja a las víctimas. Debe, además, encontrar respuesta al problema de atribución y sistematizarlo, para

que existan estándares comunes en esta cuestión. Es importante, empero, no equivocarse. La regulación no debe castigar el uso libre de internet a los individuos ni a actores pequeños, porque esto así se difunde el poder, lo que debe hacer es limitar el libre uso, sin consecuencias, a los más grandes.

El objetivo, por tanto, debe ser regular y normativizar para desescalar y difundir el poder entre los estados y actores privados, mitigar la anarquía del sistema con el objetivo de dar seguridad a las naciones. No obstante, no será hasta que los más grandes abandonen su egoísta lucha personal, que finalmente decidan atarse las manos y así poder empezar a regular con sensatez y justicia. Por ello, como se ha recalcado anteriormente, el uso del poder blando en el ciberespacio es muy relevante, los Estados con poder normativo deben dar el paso hacia la regulación.

En definitiva, el ciberespacio llegó para quedarse y es quimérico desprenderse de él, por ello, debemos avanzar, mediante cooperación internacional y multilateralismo, hacia su limitación como instrumento de poder para los más capaces y su impulso para los más pequeños, porque solo así se puede diversificar el poder.

7. Bibliografía

Aguilar, L. J. (2011). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. *Instituto Español de Estudios Estratégicos*. Obtenido de https://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2011/Cuaderno_149.html

Albright, D., Brannan, P., & Walrond, C. (2010). Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? *Institute for science and International Security*. Obtenido de https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

Ambos, K. (2015). *Responsabilidad penal internacional en el ciberespacio.* barcelona: Georg August Universität Göttingen.

Andover Llinás, A., & Shore, M. (18 de Octubre de 2023). *Fundamentos de ciberseguridad: Introducción a las normas cibernéticas de las Naciones Unidas*. Obtenido de LinkedIn Learning: https://www.linkedin.com/learning/fundamentos-de-ciberseguridad/introduccion-a-las-nomas-ciberneticas-de-las-naciones-unidas

Balleza, J. C. (2 de Septiembre de 2023). *De la Guerra Fría a la Guerra Cibernética: La Épica Evolución de la Ciberseguridad y su Desafío en el 2030.* Obtenido de LinkedIn: https://www.linkedin.com/pulse/de-la-guerra-fr%C3%ADa-cibern%C3%A9tica-

%C3%A9pica-evoluci%C3%B3n-y-su-en-paris-balleza/?trk=public_post&originalSubdomain=es

Balsalobre, J. P. (18 de 1 de 2016). *Kenneth Waltz: Neorrealismo y estructura de poder*. Obtenido de Kosmos-Polis: https://kosmospolis.com/2016/01/kenneth-waltz-neorrealismo-y-estructura-de-poder/

Barbé, E. (1987). El papel del realismo en las relaciones internacionales. *Revista de Estudios Políticos (N*(57), 149-156.

Barbé, E. (1995). *Relaciones Internacionales.* Madrid: Tecnos.

Bartolomé, M. (Maig de 2023). *Ciberseguridad, Geopolítica y Relaciones Internacionales*. Obtenido de Global Strategy: https://global-strategy.org/ciberseguridad-geopolitica-y-relaciones-internacionales/

Bejarano, M. J. (2013). Poder blando frente a poder duro en el ciberespacio. *Instituto Español de Estudios Estratégicos*(33).

Bueno, L. F. (15 de 8 de 2019). *Stuxnet, así es la nueva guerra del virus*. Obtenido de Espaciomisterio: https://www.espaciomisterio.com/conspiraciones/virus-stuxnet-guerra_40595

Calzado, C. (2021). La importancia del dominio cibernético en el contexto internacional actual como 5º dominio de la guerra. *Universidad Pontificia Comillas*.

Craig, A., & Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. *E-International Relations*, 1-11. Obtenido de https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

Crego, A. P. (8 de mayo de 2023). *¿Cuál es la historia de la ciberseguridad?* Obtenido de Deusto Formación: https://www.deustoformacion.com/cursos/programacion-tecnologia/curso-ciberseguridad/historia

Delgado, A. N. (2020-2021). *El Caso Stuxnet: Especial atención a los desafíos y las conductas que se presentan en los ciberdelitos.* León: Universidad de león.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance.* Cambridge: MA: MiT Press.

Denning, D. (2017). *Following the Developing Iranian Cyberthreat.* The Conversation. Obtenido de https://www.scientificamerican.com/article/following-the-developing-iranian-cyberthreat/

Diccionario Panhistórico de Dudas. (s.f.). *Versión Provisional, Segunda Edición*. Obtenido de Diccionario panhispánico de dudas [En línea]: https://www.rae.es/dpd/ciber-

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review, 27*(3), 221-244. Obtenido de https://www.jstor.org/stable/20445053

France24. (16 de Febrero de 2023). *Los ciberataques rusos aumentaron un 300% en 2022 en países de la OTAN*. Obtenido de France24: https://www.france24.com/es/minuto-a-minuto/20230216-los-ciberataques-rusos-aumentaron-un-300-en-2022-en-pa%C3%ADses-de-la-otan

Gamero-Garrido, A. (2017). *Cyber Conflicts in International relations.* Massachusets: Massachusets Institute of Tecnology.

García, J. R. (2021). *La aplicación del derecho internacional al ciberespacio en las ciberoperaciones realizadas por actores no estatales desde el territorio de un estado.* Madrid: Universidad Pontificia de Comillas.

Guiora, A. N. (2017). *Cybersecurity: Geopolitics, law, and policy.* New York: Routledge.

Gyuris, E. N. (2018). *La influencia de la Seguridad Informática en las Relaciones Internacionales.* Tandil: Universidad Nacional del Centro de la Provincia de Buenos Aires.

Holgado, R. (2 de Noviembre de 2022). *20 minutos*. Obtenido de "Estamos bajo ataque": se cumplen 34 años del 'gusano Morris', el primer malware de la historia: https://www.20minutos.es/tecnologia/ciberseguridad/estamos-bajo-ataque-se-cumplen-34-anos-del-gusano-morris-el-primer-malware-de-la-historia-5073273/

Ibáñez, J. (2010). Internet, política y poder en la sociedad postinternacional. 323-378.

Iniseg. (11 de Mayo de 2020). *Corea del Norte y el Ciberespionaje: búsqueda de piratas informáticos*. Obtenido de Iniseg: https://www.iniseg.es/blog/ciberseguridad/corea-del-norte-y-el-ciberespionaje-busqueda-de-piratas-informaticos/

Jervis, R. (1976). *Perception and misperception in International Politics.* New Jersey: Princeton University Press.

Jiménez, C. M. (2015). *El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia.* Madrid: Universidad Pontificia de Comillas.

Jørgensen, K. E. (2018). *International Relations Theory.* London: Palgrave.

Keohane, R. O. (1984). *After Hegemony.* Princeton, NJ: Princeton University Press.

Kissinger, H. (2016). *World Order*. Barcelona: Debate.

Kolet, K., Lambakis, S., & Kiras, j. (2002). *Understanding "Asymmetric" Threats.* Comparative Strategy.

Lessig, L. (1998). Las leyes del ciberespacio. *THEMIS*(44), 171-179.

Limón, R. (20 de Junio de 2023). El cibercrimen alcanza niveles inéditos: 90 millones de ataques anuales que cuestan 10,5 billones de euros. *El País*.

Llinas, D. A. (2017). *Análisis del ciberataque para la seguridad de los estados y su incidencia en la transformación del status quo: Stuxnet el virus informático.* Bogotá: Universidad del Rosario. doi:https://doi.org/10.48713/10336_13705

Mata-Sánchez, G. (2023). Relaciones Internacionales y Geopolítica: conflicto y poder en el ciberespacio. *Revista Relaciones Internacionales del mundo actual, 3*(41), 542-562.

Maurer, T., & Morgus, R. (2014). *Compilation of Existing Cybersecurity and Information Security Related Definitions.* Suiza: Departamento Federal de Asuntos Exteriores.

Mearsheimer, J. (2006). Structural Realism. 71-88.

Morgenthau, H. J. (1949). *Politics amongst Nations.* New York: Alfred A. Knopf.

Naciones Unidas. (2022). *Novedades en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional*. Obtenido de Oficina de Asuntos de Desarme de las Naciones Unidas: https://disarmament.unoda.org/ict-security/

Naciones Unidas. (s.f.). *Oficina de la Lucha contra el Terrorismo*. Obtenido de Ciberseguridad: https://www.un.org/counterterrorism/es/cct/programme-projects/cybersecurity

Nye, Jr, J. S. (2010). *Cyberpower*. Harvard Kennedy School: Belfer Center for Science and Intenrational Affairs.

Orozco, G. A. (2019). El sistema internacional cibernético: elementos de análisis. *OASIS, 30*, 163-186. doi:https://doi.org/10.18601/16577558.n30.10

Palfrey, J. (2010). Four Phases of Internet Regulation. *Limiting Knowledge in a Democracy, 77*(3), 981-996. Obtenido de https://www.jstor.org/stable/40972303

Panda Security. (18 de Octubre de 2013). *Los virus más famosos de la historia: Melissa*. Obtenido de https://www.pandasecurity.com/es/mediacenter/virus-melissa/

Parker, C. K. (2014). El uso del ciberpoder. *Military Review*, 50-59. Obtenido de https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20140831_art009SPA.pdf

Parlamento y Consejo Europeo. (2019/881). Reglamento sobre la Ciberseguridad de la UE.

Pernik, P. (2018). *Hacking for Influence - Foreign Influence activities and Cyber-attacks.* Tallin: International Centre for Defence and Security.

Petallides, C. J. (2012). Cyber Terrorism and IR Theory: Realism, Liberalism and Constructivism in the New Security Threat. *Inquiries Journal/Student Pulse, 4*(3). Obtenido de http://www.inquiriesjournal.com/a?id=627

Poitevin, V. (27 de Junio de 2023). *Breve historia del phishing*. Obtenido de Stormshield: https://www.stormshield.com/es/noticias/breve-historia-del-phishing/

Quintana, Y. (2016). *Ciberguerra.* Madrid: Ediciones de la Catarata.

Rice, C. (2008). *Rethinking the National Interest. American Realism for a New World*. Obtenido de Foreign Affairs: https://www.foreignaffairs.com/articles/2008-06-01/rethinking-national-interest

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Strategic Studies, 38*(1-2), 4-37. doi:http://dx.doi.org/10.1080/01402390.2014.977382

Sánchez, L. O. (25 de Diciembre de 2022). *NordVpn*. Obtenido de La historia de la ciberseguridad: https://nordvpn.com/es/blog/historia-ciberseguridad/

Scheneier, B. (2013). El análisis definitivo de Stuxnet: Matar una centrífugadora. *Ralph Langner*.

Seagal, A. (2016). *The Hacked World Order.* New York: Public Affairs.

Silva, F. (2018). Stuxnet - El software como herramienta de control geopolítico. *Revista Puce*(106), 297-314.

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What everyone needs to know.* New York: Oxford University Press.

Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index.* Harvard kennedy School, Science and International Affairs. Cambrigde: Belfer Center.

Waltz, K. N. (1979). *Theory of International politics.* Berkley: Addison-Wesley.

Wendt, A., & Sindal, D. (2009). Why there is International Theory now. *International Theory*, *1*(1), 1-14. doi:https://doi.org/10.1017/S1752971909000062

8. Anexos

1. **Principales potencias del sistema internacional cibernético** (Voo, Hemani, & Cassidy, 2022)

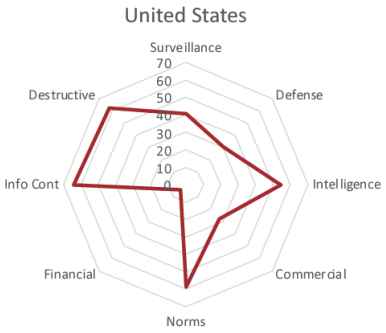

Ilustración 1: *Gráfico de radar de EEUU.*

Ilustración 1: *Gráfico de radar de China.*

Ilustración 3: *Gráfico de Radar de Rusia.*

Ilustración 2*: Gráfico de Radar de Reino Unido.*

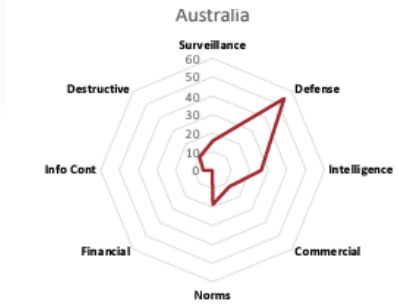

Ilustración 5: *Gráfico de Radar de Australia.*

Ilustración 6: *Gráfico de Radar de Países Bajos.*

Ilustración 7: *Gráfico de Radar de Corea del Sur.*

Ilustración 8: *Gráfico de Radar de Francia.*

Ilustración 9: *Gráfico de Radar de Vietnam.*

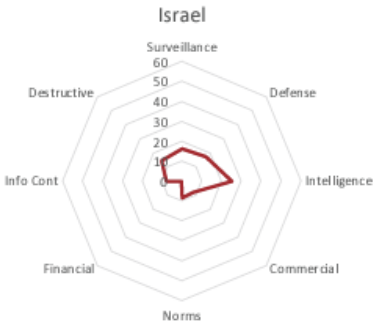

Ilustración 10: *Gráfico de Radar de Israel.*

Ilustración 11: *Gráfico de Radar de Irán.*

Ilustración 12: *Gráfico de Radar de Corea del Norte.*

2. **Stuxnet: cuestiones técnicas del ciberataque** (Scheneier, 2013)**.**

Capas del ciberataque:

CAPA TECNOLÓGICA	
Afectación: Redes, sistemas operativos y aplicaciones.	Objetivo: propagar.
CAPA DEL SISTEMA DE CONTROL INDUSTRIAL	
Afectación: Controladores industriales, subcontroladores.	Objetivo: manipulación.
CAPA FÍSICA	
Afectación: Válvulas, centrifugadoras, accionamientos eléctricos, etc.	Objetivo: Daño por explotación de vulnerabilidades físicas.

Métodos de afectación: