Facultad de Ciencias Económicas y Empresariales

Ciberseguridad y diplomacia digital en perspectiva comparada: Unión Europea y Estados Unidos

Autor: Claudia García García
Director: Juan Gonzalo Lugo Sanchiz

Resumen

En un contexto internacional, el poder ya no se mide únicamente en términos militares o económicos, sino también en la capacidad de dominar el ciberespacio. La digitalización ha transformado las dinámicas internacionales, convirtiendo el concepto de ciberseguridad como protagonista en la seguridad y proyección exterior de los Estados.

La Unión Europea y Estados Unidos emergen como actores clave con visiones distintas, aunque interdependientes, sobre cómo gobernar, proteger y aprovechar el entorno digital. El siguiente análisis estudia cómo ambas potencias reflejan concepciones divergentes del poder y la soberanía en la era digital. Para ello, se emplea una metodología cualitativa basada en el análisis de documentos oficiales, informes estratégicos y casos relevantes, estructurando el estudio en un marco teórico de Relaciones Internacionales que incorpora perspectivas realistas liberales y constructivistas.

En el caso de la Unión Europea, se destaca su apuesta por una soberanía digital compartida, basada en la regulación, la cooperación multilateral y la defensa de valores como la privacidad y los derechos digitales. Por otro lado, Estados Unidos prioriza el liderazgo tecnológico y la seguridad nacional, apoyándose en la innovación, la disuasión estratégica y la cooperación con aliados.

Lejos de ser excluyentes, ambos modelos interactúan en una relación compleja donde convergen intereses comunes, como la defensa de un entorno digital seguro o la protección de infraestructuras críticas, y divergencias en ámbitos como la protección de datos o la autonomía estratégica. Esta tensión refleja no solo distintas culturas políticas, sino también una competencia implícita por definir las reglas del orden digital global.

En última instancia, se concluye que la capacidad de equilibrar rivalidad y colaboración será determinante para configurar un ciberespacio estable, seguro y alineado con principios democráticos en las próximas décadas.

Palabras clave: ciberespacio, rivalidad geopolítica, diplomacia digital, ciberseguridad, soberanía digital.

Abstract

In an international context, power is no longer measured only in military or economic terms, but also in the ability to dominate cyberspace. Digitalization has transformed international dynamics, making the concept of cybersecurity a protagonist in the security and external projection of States.

The European Union and the United States emerge as key actors with different, although interdependent, visions on how to govern, protect and take advantage of the digital environment. The following analysis studies how both powers reflect divergent conceptions of power and sovereignty in the digital age. To this end, a qualitative methodology based on the analysis of official documents, strategic reports and relevant cases is used, structuring the study in a theoretical framework of International Relations that incorporates liberal and constructivist realist perspectives.

In the case of the European Union, its commitment to shared digital sovereignty, based on regulation, multilateral cooperation and the defence of values such as privacy and digital rights, stands out. On the other hand, the United States prioritises technological leadership and national security, relying on innovation, strategic deterrence and cooperation with allies.

Far from being mutually exclusive, the two models interact in a complex relationship where common interests, such as the defence of a secure digital environment or the protection of critical infrastructures, converge and divergences in areas such as data protection or strategic autonomy. This tension reflects not only different political cultures, but also an implicit competition to define the rules of the global digital order.

Ultimately, it is concluded that the ability to balance rivalry and collaboration will be decisive in shaping a stable, secure cyberspace aligned with democratic principles in the coming decades.

Keywords: cyberspace, geopolitical rivalry, digital diplomacy, cybersecurity, digital sovereignty.

Índice de Contenidos

1. Introducción

1.1 Relevancia del tema

La intensificación de los procesos de digitalización en el sistema internacional ha reconfigurado las dinámicas tradicionales de poder, otorgando al ciberespacio una relevancia estratégica creciente en los ámbitos de la seguridad, la economía y la política global. En este marco, la ciberseguridad y la diplomacia digital han adquirido un papel central y estrechamente vinculado en la configuración de la acción exterior tanto de los Estados como de los actores supranacionales.

La ciberseguridad puede definirse como una disciplina centrada en asegurar sistemas, redes, *software* y datos frente a ataques digitales, garantizando la confidencialidad, integridad y disponibilidad de la información (Daim et al., 2024). Por su parte, la diplomacia digital hace referencia al uso de herramientas digitales y tecnologías de la información en la formación y ejecución de la política exterior, así como a la gestión de las Relaciones Internacionales en el entorno digital.

La relevancia de este tema radica en que el ciberespacio ha dejado de ser un ámbito meramente técnico para convertirse en un escenario donde los Estados y otros actores compiten por poder e influencia, igual que ocurre en otros ámbitos tradicionales como la economía o seguridad militar. Fenómenos como los ciberataques contra infraestructuras críticas, la manipulación de la información, el control de los flujos de datos y la regulación de las grandes plataformas tecnológicas evidencian que la seguridad digital se encuentra actualmente vinculada en su totalidad a la estabilidad internacional. En este contexto, la creciente competitividad geopolítica entre la UE y EEUU no solo refuerza la importancia del ciberespacio como ámbito estratégico, sino que también condiciona la respuesta occidental ante conflictos recientes, como la invasión rusa en Ucrania. La retirada de la ayuda norteamericana a Ucrania durante la guerra no constituye un elemento aislado, sino que se inscribe en estas tensiones, generando fricciones en la cooperación transatlántica y generando posibles efectos sobre el equilibrio geopolítico global.

La Unión Europea y Estados Unidos destacan como dos de los principales actores globales en la gobernanza del ciberespacio, aunque con enfoques diferenciados. La primera potencia ejerce el poder digital principalmente a través de la regulación y el liderazgo normativo, mientras que el segundo actor aborda el ciberespacio desde una lógica más estratégica y de poder, combinando seguridad, tecnología y alianzas. Realizar un análisis comparativo de ambos

modelos resulta especialmente relevante para comprender las dinámicas actuales del poder digital y las posibilidades de cooperación transatlántica.

En definitiva, el estudio de la relación entre ciberseguridad y diplomacia digital permite aportar una perspectiva innovadora al campo de las Relaciones Internacionales, al articular enfoques tradicionales de la seguridad con nuevas modalidades de acción exterior propias de la era digital.

1.2 Objetivos de estudio

La finalidad del siguiente trabajo es realizar un análisis sobre la interdependencia entre ciberseguridad y diplomacia digital, entendidas como dimensiones fundamentales de la acción exterior en el contexto internacional contemporáneo. A partir de una perspectiva comparada, el estudio examina los casos de la Unión Europea y de Estados Unidos, con el propósito de comprender cómo ambos actores configuran sus estrategias, marcos normativos y políticos en el ciberespacio. Asimismo, pone de manifiesto que estas estrategias no se limitan a la protección frente a amenazas, sino que trascienden el ámbito estrictamente técnico o defensivo para proyectarse en su acción exterior.

A partir de este objetivo general, se plantean los siguientes objetivos específicos:

1. Estudiar los principales enfoques teóricos y marcos analíticos de las Relaciones Internaciones que explican la relación entre la ciberseguridad y la diplomacia digital.
2. Analizar la evolución y consolidación de la diplomacia digital de la Unión Europea como un instrumento central de su acción exterior para influir y cooperar internacionalmente en el ámbito del ciberespacio.
3. Examinar la diplomacia digital estadounidense como herramienta de poder y gestión internacional, especialmente en un entorno marcado por tensiones y conflictos en el ciberespacio.
4. Comparar los enfoques adoptados por la Unión Europea y Estados Unidos, identificando las principales convergencias y divergencias en sus políticas de ciberseguridad y diplomacia digital, así como las implicaciones de dichas diferencias para su proyección internacional.

5. Valorar críticamente los principales retos y perspectivas futuras derivados de la creciente conflictividad en el ciberespacio, examinando sus implicaciones para la cooperación transatlántica y la articulación de respuestas conjuntas.

1.3 Metodología y estructura del trabajo

El presente trabajo de fin de grado emplea un enfoque cualitativo, basado principalmente en una revisión bibliográfica exhaustiva, análisis documental y la comparación de políticas públicas. Este enfoque se justifica por su capacidad para proporcionar una compresión profunda y contextualizada de cómo la Unión Europea y Estados Unidos abordan la ciberseguridad y la diplomacia digital. Además, se hace uso de un enfoque interdisciplinar que integra aportaciones de las Relaciones Internacionales, los estudios de seguridad y el derecho digital, permitiendo identificar convergencias, divergencias y desafíos comunes en un contexto marcado por nuevas amenazas híbridas y la creciente disputa por la soberanía digital.

La estructura del trabajo sigue una lógica secuencial y comparativa. En primer lugar, se desarrolla un marco teórico y conceptual que define los conceptos fundamentales de ciberseguridad y diplomacia digital y se presentan las principales ideas de las teorías del realismo, liberalismo y constructivismo en el marco del ciberespacio en la política global. La perspectiva realista, concibe la ciberseguridad como instrumento de poder y defensa; el liberalismo permite examinar la cooperación internacional y los regímenes de gobernanza digital; y el constructivismo facilita el estudio de los valores, normas y narrativas que configuran el ciberespacio.

A continuación, el trabajo se articula en dos capítulos empíricos, cada uno dedicado a uno de los actores principales estudiados. Se analiza la evolución de las políticas de ciberseguridad de la Unión Europea con organismos, directivas y estrategias que permiten observar el creciente papel como actor de la diplomacia digital. Asimismo, es necesario ilustrar el uso de la regulación como expresión de su poder normativo a través de ejemplos de respuestas del actor a ciberincidentes recientes. Por otro lado, el capítulo relativo a Estados Unidos estudia la evolución de sus estrategias nacionales de ciberseguridad, su apuesta por las alianzas y coaliciones en el ámbito digital. Es complementado con la revisión de casos emblemáticos que han marcado su doctrina y el papel determinante del sector privado en su política digital.

Estos capítulos permiten tener una base sobre la que se elabora un apartado comparativo que contrasta los enfoques europeo y estadounidense, identificando diferencias estructurales, puntos de convergencia y tensiones persistentes, especialmente en materia de protección de datos y soberanía digital. Finalmente, el trabajo concluye con una reflexión sobre los retos globales donde se sintetizan los principales resultados, se responden a las preguntas de investigación y la viabilidad de una diplomacia transatlántica sólida, ofreciendo recomendaciones para fortalecer la cooperación internacional en ciberseguridad.

2. Marco teórico y conceptual

El análisis de la relación entre ciberseguridad y diplomacia digital requiere partir de un marco teórico que combine elementos de las Relaciones Internacionales (RR.II), los estudios de seguridad y de gobernanza global de Internet. “Las Relaciones Internacionales enfrentan desafíos epistemológicos y prácticos sin precedentes en la era digital, caracterizada por la incertidumbre, la complejidad y la volatilidad” (Hernández Mendoza & Hernández Martínez, 2025, p.1)., lo que lleva a reconsiderar las nociones de poder, soberanía y cooperación en un contexto profundamente tecnológico y de rápida transformación. Más que un asunto técnico, la digitalidad implica cambios en infraestructuras y en correlaciones de poder que generan nuevas modalidades de disputa, crisis interconectadas y competencia estratégica, con impactos directos en la seguridad y en la proyección exterior de los Estados.

Bajo esta lógica, la ciberseguridad se ha consolidado como un concepto multidimensional. Según la Unión Internacional de Telecomunicaciones (UIT), la ciberseguridad es “la recopilación de herramientas, políticas, conceptos de seguridad, salvaguardias, directrices, enfoques de gestión de riesgos, acciones, formación y buenas prácticas destinadas a proteger los activos de información frente a amenazas en el ciberespacio” (International Telecommunication Union [ITU], s. f., sección “Definition of cybersecurity”, traducción propia). Esto comprende la prevención de confidencialidad, integridad y disponibilidad de la información en el ciberespacio, así como la resiliencia de las infraestructuras digitales. La ciberseguridad debe entenderse como un fenómeno político material y normativo-diplomático a la vez. Ello se aprecia en que “la digitalidad tensiona los marcos teóricos tradicionales, genera dilemas ético-legales en torno a la privacidad y los datos, y amplifica sesgos algorítmicos y asimetrías de poder Norte-Sur" (Hernández Mendoza & Hernández Martínez, 2025, p.1). La comparativa entre UE-EE.UU refleja este diagnóstico, puesto que mientras la primera enfatiza

regulación y derechos, EE.UU prioriza su seguridad nacional, alianzas y liderazgo tecnológico, siendo dos respuestas diferentes ante un mismo ecosistema de riesgos y capacidades.

Por su parte, la diplomacia digital representa la adaptación de la práctica diplomática al entorno digital. Según el *Foreign and Commonwealth Office* (2012), la diplomacia digital se refiere al uso de Internet y herramientas digitales para alcanzar objetivos de política exterior (Foreign and Commonwealth Office, 2014). Esto incluye desde el uso de plataformas digitales para la comunicación pública *(e-diplomacy)*[1] hasta la negociación de normas internacionales sobre ciberseguridad, gobernanza de Internet o inteligencia artificial. Sin embargo, es algo más que la simple utilización de las herramientas digitales para la consecución de objetivos diplomáticos, puesto que implica cambios organizativos y funcionales en las prácticas diplomáticas. Además, la diplomacia digital también se manifiesta en la creación de foros multilaterales, como el *Internet Governance Forum,* y en estrategias de poder blando digital, donde la narrativa, la reputación y la influencia simbólica juegan un papel central.

El vínculo entre ambos conceptos se encuentra en la interdependencia entre seguridad y diplomacia en el entorno digital. La ciberseguridad requiere cooperación internacional, intercambio de información y construcción de confianza entre Estados, con ejemplos como las Medidas de Fomento de la Confianza (CBMs) que convierten la confianza en procedimientos (canales verificados, criterios comunes, protocolos de respuesta). Esto convierte la diplomacia digital en una herramienta indispensable para activar y sostener estas medidas. Al mismo tiempo, los objetivos de la diplomacia digital como la proyección de valores o la promoción de la regulación global se ven condicionados por las capacidades tecnológicas y por los intereses estratégicos de ciberseguridad de cada actor, pues la competencia geopolítica gira cada vez más en torno al aprovechamiento de las tecnologías emergentes, donde la definición de estándares se convierte en un elemento clave.

En este sentido, el marco conceptual del estudio puede organizarse en torno a tres dimensiones. La primera, la dimensión político-estratégica que se centra en como los Estados diseñan políticas para proteger su soberanía digital y preservar su capacidad de poder en el ciberespacio (reducción de dependencias tecnológicas, fortalecimiento de infraestructuras críticas, desarrollo de capacidades). En el caso europeo, la soberanía digital ha pasado de ser un lema político para convertirse en eje estructural del modelo digital de la UE, con una arquitectura

[1] La e-diplomacy se refiere al uso estratégico de tecnologías digitales por parte de actores diplomáticos para comunicar o negociar asuntos internacionales en el entorno digital.

normativa y programática que orienta estrategias sobre datos. Por otro lado, la segunda dimensión, la normativa, centrada en la creación de marcos legales y éticos que regulen la seguridad digital, la privacidad y la cooperación internacional. La UE tiende a codificar derechos y obligaciones, a través de la protección de datos (RGDP) y marcos horizontales sobre servicios/plataformas (DSA). Mientras que en EE.UU, el enfoque combina estrategia nacional, orden ejecutiva con regulación financiera (SEC) o *reporting* de incidentes (CIRCIA). Por último, la dimensión diplomática, examina como los Estados emplean la diplomacia digital para gestionar conflictos, promover nomas y fortalecer su influencia global mediante foros y procesos multilaterales como CBMs de la OSCE comentados anteriormente o GGE/OEWG de la ONU sobre conducta responsable.

El caso comparado de la Unión Europea y Estados Unidos permite observar la coexistencia de distintos modelos de gobernanza digital. Ambos enfoques, lejos de ser excluyentes, se entrecruzan en la práctica mediante acuerdos, fricciones y alineamientos sectoriales, donde la cooperación y la competencia coexisten.

2.1 Enfoques desde las Relaciones Internacionales

El estudio de la ciberseguridad y la diplomacia digital puede abordarse desde diferentes teorías y enfoques de las Relaciones Internacionales, ya que cada una ofrece una manera distinta de interpretar cómo los Estados, actores no estatales y organismos internacionales actúan en el ciberespacio. Estos marcos no son excluyentes, ofrecen un repertorio complementario para explicar cómo se comportan los Estados en el entorno digital y que estrategias emplean para proteger sus intereses, gestionar riesgos y proyectar influencia.

En primer lugar, el realismo ha sido un paradigma dominante en el campo de las relaciones internacionales y “enfatiza las limitaciones que la naturaleza humana y la ausencia de un gobierno internacional imponen a la política. En conjunto, hacen de las Relaciones Internacionales un ámbito dominado por el poder y el interés” (Donnelly, 2000, p. 9, traducción propia). Por eso, cada uno debe protegerse por su cuenta, guiado por el poder y el interés nacional.

Aplicado al ciberespacio, este enfoque caracterizado por la anarquía y la competencia entre Estados por el poder y la supervivencia parece ser la teoría más apropiada para dilucidar los problemas acuciantes de ciberseguridad. Por lo tanto, esta mirada parte de la idea de que el

ciberespacio no constituye un ámbito radicalmente nuevo, sino la extensión de una lógica ya conocida, puesto que los Estados siguen desconfiando unos de otros y tratan de proteger sus infraestructuras críticas y desarrollar capacidades ofensivas y defensivas, solo que ahora también lo hacen mediante redes, datos y ciberataques.

En este sentido, el realismo ayuda a entender por qué los gobiernos destinan cada vez más recursos a la ciberdefensa y por qué se observa una creciente militarización del ciberespacio. Solo en Estados Unidos, "el presupuesto del presidente para el año fiscal 2024 destinado a las actividades cibernéticas del Departamento de Defensa es de 13.5 mil millones de dólares en 2024 lo que supone un aumento de 1.8 mil millones de dólares (15.4%) respecto a la solicitud presupuestaria del año fiscal 2023" (Goss, 2023, párr. 3, traducción propia).

La ciberseguridad se interpreta como extensión de la seguridad nacional, convirtiendo los ciberataques o el espionaje digital en instrumentos de poder estatal. De ahí que los Estados den ciertos pasos instituciones como la creación de organismos como el *U.S Cyber Command* para centralizar y sincronizar operaciones de ciberdefensa y ciberofensiva. Por ejemplo, en 2016, *U.S. Cyber Command* creó la Joint Task Force (JTF) para coordinar las operaciones en el ciberespacio contra ISIS. A su vez, el reconocimiento del ciberespacio como dominio de operaciones, por parte de la OTAN en la Cumbre de Varsovia de 2016, materializan la idea de que la seguridad digital se ha integrado como componente central de la seguridad nacional y defensa colectiva.

Desde el marco realista, la diplomacia digital cumple una función instrumental para asegurar aliados, gestionar la rivalidad y disuadir conductas adversarias mediante acuerdos, normas y coaliciones. No son expresiones de altruismo normativo, sino herramientas para gestionar la rivalidad y reforzar la propia seguridad. Al aprobar reglas y mecanismos de sanción frente a actividades cibernéticas maliciosas, los Estados intentan que los ciberataques resulten más costosos y arriesgados para sus posibles adversarios.

Mientras que la teoría realista ofrece un enfoque más pesimista respecto a la cooperación, el liberalismo tiende a ofrecer una visión mucho más positiva puesto que no se centra solo en la anarquía del sistema internacional, sino que considera que la cooperación y las instituciones como ONG o OIG pueden reducir la inseguridad y hacer el comportamiento de los Estados más previsibles. El enfoque liberal ofrece una panorámica sobre las bases posibles para construir cooperación en el ámbito de la ciberseguridad y el ciberespacio. En general, el liberalismo sostiene que la política internacional es un proceso en transformación, en el que la

creciente interdependencia entre los Estados impulsa dinámicas de cooperación. Por lo tanto, los Estados no actúan únicamente movidos por la búsqueda de poder, sino también por la existencia de ciertos intereses comunes en ámbitos como la ciberseguridad o gobernanza del ciberespacio.

"El liberalismo considera el ciberespacio como un espacio global que debe ser accesible a todos y regirse por normas comunes" (Saaid, 2025, traducción propia), precisamente por su carácter transnacional y su dependencia de infraestructuras distribuidas que atraviesan fronteras estatales. Esta infraestructura interconectada hace que cualquier fallo o riesgo se comparta entre múltiples actores, de manera que la seguridad de cada Estado depende del nivel de protección, las prácticas y las capacidades de los demás actores con los que está interconectado. Desde esta óptica, la diplomacia digital se convierte en un instrumento central para desarrollar mecanismos de gobernanza compartida, orientados a armonizar estándares técnicos y jurídicos dentro de un entorno digital seguro y pacífico.

Se aboga por una gobernanza multiactor que refleja la creencia liberal de que los problemas del entorno digital pueden abordarse mediante acuerdos cooperativos y regímenes internacionales. Con multiactor se refiere a la incorporación de forma activa de organizaciones internacionales, empresas tecnológicas, sociedad civil y comunidad experta, con el objetivo de reducir asimetrías y gestionar riesgos compartidos con el foco en tener una responsabilidad compartida.

Por lo tanto, esta teoría ofrece un marco teórico que ayuda a comprender por qué los Estados recurren a la diplomacia, crean alianzas y fortalecen instituciones para gestionar amenazas digitales de espionaje, desinformación o ciberataques. En contraste con lo que defiende la teoría realista, el liberalismo subraya las posibilidades de una gobernanza digital basada en la cooperación, la regulación y la gestión correcta de las amenazas.

El constructivismo aporta una tercera mirada para analizar la ciberseguridad y la diplomacia digital, "al ser la teoría de las Relaciones Internacionales que comprende la importancia de las ideas y las estructuras en la política mundial, especialmente en lo relativo a las cuestiones de seguridad" (Manili, 2019, p. 24, traducción propia). A diferencia de las teorías, el constructivismo defiende que las acciones y comportamientos de los Estados, es decir, la política internacional, se construye a partir de significados e ideas compartidas entre actores. Sus acciones están basadas en cómo buscan ser percibidos e integrados en el orden internacional, sin responder mecánicamente a condiciones objetivas.

Desde esta perspectiva, “el ciberespacio es un terreno fértil para la aplicación del constructivismo, hasta el punto de considerar el ciberespacio como una construcción social” (Saaid, 2025, traducción propia), donde se incluyen reglas, discursos y representaciones colectivas. Por lo tanto, los conceptos de seguridad, amenazas o incluso ciberespacio no tienen un significado fijo por sí mismos, sino categorías que se construyen socialmente a través de la interacción entre actores. En este sentido, la forma en la que los Estados perciben el ciberespacio no depende únicamente de su capacidad ofensiva, sino que está profundamente condicionada por significados, valores y proyectos políticos que cada Estado proyecta en el ciberespacio. De este modo, la definición de ciberseguridad es contingente, lo que implica que clasificar un incidente digital como espionaje o acto de guerra depende de discursos, normas e interpretaciones, no solo de hechos técnicos.

Las normas internacionales y estructuras del entorno digital no existen de forma predeterminada, por lo que la diplomacia digital desde la perspectiva constructivista puede entenderse como un espacio donde los Estados buscan moldear reglas y expectativas compartidas sobre la mejor forma de usar el ciberespacio. No se busca solo responder a amenazas objetivas, lo importante, es cómo se interpreta eso políticamente. En este proceso, su identidad influye en la respuesta de sus decisiones, por ejemplo, un Estado puede presentar sus capacidades cibernéticas como puramente protectoras si se considera una potencia responsable y defensiva. Mientras que puede interpretar las acciones de otro como más agresivas si lo define como rival estratégico.

En conjunto, tras el análisis de estas tres teorías de las Relaciones Internacionales se puede comprender la complejidad del ciberespacio y de la diplomacia digital como ámbitos en los que conviven dinámicas de poder y cooperación. Mientras que el realismo ayuda a explicar la centralidad de la seguridad nacional con un ciberespacio que aparece como un reflejo de la rivalidad entre Estados. El liberalismo ofrece una lectura orientada hacia la cooperación con el empleo de la diplomacia digital como herramienta para generar confianza, debido a la propagación de amenazas que supera la capacidad de cada Estado para abordarlas de forma individual. Por último, el constructivismo defiende la importancia de los discursos, valores y percepciones para interpretar los términos de amenazas que definen las normas que regulan el comportamiento de los Estados en el ciberespacio.

Estas aproximaciones teóricas permitirán la comprensión de la posición de la Unión Europea y EE.UU en materia de ciberseguridad y diplomacia digital. El análisis se centrará en

determinar hasta qué punto cada una de las potencias encarna un modelo liberal o si, por el contrario, tienden hacia esquemas más restrictivos y securitizados. Ello permitirá determinar si sus estrategias digitales buscan sostener un orden digital basado en normas comunes con la participación de múltiples actores, o si se prefiere adoptar un enfoque con un control regulatorio estricto sin interdependencia.

2.2 Contexto geopolítico actual

El análisis del ciberespacio debe situarse en el actual contexto geopolítico, caracterizado por una creciente inestabilidad, fragmentación del orden internacional y competencia entre grandes potencias. En este marco, surge una cuestión clave: ¿es posible una gobernanza multiactor eficaz en un mundo geopolítico inestable, en el que potencias como China y Rusia actúan como actores de disrupción?

Mientras que actores occidentales, como la UE y EE.UU, han promovido un modelo de Internet más abierto, interoperable y con participación de múltiples actores, sus enfoques presentan matices relevantes. Estados Unidos ha defendido tradicionalmente este modelo como parte de su liderazgo tecnológico y estratégico global, mientras que la Unión Europea lo ha desarrollado de forma más progresiva desde una perspectiva normativa, centrada en la protección de derechos fundamentales.

Frente a este modelo, China y Rusia impulsan modelos más estatocéntricos, con un control soberano de la información y de las infraestructuras digitales. Esta divergencia dificulta la gobernanza multiactor defendida por el enfoque liberal, generando una fragmentación normativa y técnica del internet global, denominada *splinternet*[2]. En este sentido, China y Rusia pueden considerarse actores de disrupción, no tanto por generar inestabilidad de forma caótica, sino por promover de forma deliberada un modelo alternativo de gobernanza digital que prioriza la seguridad nacional y la estabilidad interna.

Esta tensión debe entenderse en un contexto geopolítico caracterizado por la transformación del sistema internacional, desde un orden relativamente cooperativo hacia otro más competitivo y fragmentado. En este sentido, el analista geopolítico Robert D.Kaplan (Anexo 1), describe un mundo caracterizado por una situación de crisis permanente, marcada por la inestabilidad,

[2] Splinternet hace referencia al proceso de fragmentación del internet global en diferentes espacios digitales según los países, con distintas normas, acceso a contenidos o niveles de control.

la competencia estratégica y la erosión de los marcos de cooperación tradicionales (Hurst Publishers, 2024).

Aplicado al ciberespacio, este diagnóstico sugiere que la gobernanza multiactor enfrenta importantes limitaciones. Los países utilizan el ciberespacio para competir y obtener ventajas políticas, económicas o miliares, lo que reduce los incentivos para compartir información, coordinar políticas o establecer normas comunes. No obstante, la naturaleza global del ciberespacio hace inevitable cierto nivel de cooperación, lo que implica que las amenazas digitales llegan a traspasar fronteras, lo que obliga a mantener al menos mecanismos básicos de cooperación como la participación en foros multilaterales como la OTAN.

En consecuencia, la gobernanza de la ciberseguridad en el contexto de una creciente rivalidad geopolítica debe entenderse como un proceso de constante tensión entre conflicto y cooperación.

3. La Unión Europea: hacia una soberanía digital compartida

3.1 Evolución de la política de ciberseguridad

La política de ciberseguridad en la Unión Europea ha evolucionado hasta convertirse en un elemento central de la gobernanza contemporánea puesto que el contexto tecnológico y geopolítico en el que se insertan las sociedades europeas ha cambiado radicalmente. En sus orígenes, la ciberseguridad se concebía como un asunto sectorial y predominante técnico, centrado en garantizar el correcto funcionamiento de redes informáticas y sistemas de información. No se entendía como un asunto que afectase a toda la sociedad o a la política, sino como algo que recaía casi exclusivamente en expertos informáticos, ingenieros o agencias técnicas especializadas.

Sin embargo, el aumento de las amenazas cibernéticas, la ausencia de fronteras del ciberespacio y la progresiva digitalización de las sociedades europeas han impulsado hacia el desarrollo de un marco normativo e institucional cada vez más complejo y coordinado. Los ciberataques ya no se limitan a fallos técnicos o delitos aislados, sino que incluyen prácticas de espionaje, coacción política, sabotaje o manipulación de opinión pública, en muchos casos llevadas a cabo por actores estatales o grupos organizados transnacionales. Han pasado de ser un problema técnico, a una amenaza real contra la estabilidad política, la confianza de los ciudadanos o la soberanía de los Estados miembros de la UE.

En los primeros años, la agenda europea se centraba en proteger la "integridad, confidencialidad y disponibilidad de las redes y sistemas de información mediante medidas técnicas de seguridad perimetral" como antivirus o sistemas de detección de intrusos. Esta visión era tecnológica y defensiva, pensada para responder a ciberincidentes tradicionales, tales como accesos no autorizados, *malware*[3] o interrupciones del servicio, pero insuficiente para afrontar amenazas de carácter estratégico y político. La cooperación entre los Estados miembros era fragmentaria y esencialmente voluntaria, careciendo de un marco jurídico sólido que permitiese una estrategia europea integrada de seguridad y defensa. La intervención de la UE se orientó principalmente a facilitar el intercambio de buenas prácticas y a reforzar capacidades técnicas, sin instrumentos de coordinación obligatorios a escala europea.

No obstante, está visión comienza a resultar claramente limitada a medida que los Estados y otros actores emplean el escenario del ciberespacio para ganar poder o influencia. A partir de 2013, la UE reconoce explícitamente que "la Red se ha convertido en un escenario de competición geopolítica y económica entre Estados donde se entremezclan ciberataques, ciberdelitos y desinformación con un propósito desestabilizador" (Alonso Lecuit, 2018, p. 1)., es decir, se ha convertido en un dominio de conflicto y competencia estratégica.

Esta transformación del ciberespacio en un ámbito de confrontación híbrida evidencia que los riesgos cibernéticos transcienden lo puramente tecnológico, las amenazas cibernéticas son cada vez más complejas, transfronterizas y con impactos que superan la capacidad de respuesta individual de los Estados, por lo que justifica la intervención de la UE como actor coordinador y regulador. En el contexto actual, la UE integra la ciberseguridad en sus grandes políticas generales especialmente en ámbito de la seguridad interior y en la agenda digital global. Las amenazas se manifiestan en el plano digital obligando a reconsiderar las políticas clásicas de seguridad interior. Los ciberataques contra infraestructuras críticas afectan directamente a la vida cotidiana de los ciudadanos y al orden social, lo que hace necesario integrar la ciberseguridad en el núcleo de las políticas de seguridad interior.

Este cambio de enfoque político va acompañado de un proceso de institucionalización progresiva, que ha redefinido los actores implicados, los objetivos perseguidos y los recursos movilizados por la Unión Europea. La ciberseguridad deja de ser una reacción puntual a crisis o ataques y pasa a entenderse como una política pública permanente con reglas, actores y

[3] Un malware es un software malicioso diseñado para dañar o alterar la información de un sistema informático sin autorización

procedimientos propios. Uno de los elementos centrales de esta institucionalización es la creación y el fortalecimiento de agencias especializadas, que actúan como nodos técnicos y políticos dentro del ecosistema europeo de ciberseguridad.

En este contexto, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), creada en 2004 con un mandato inicialmente limitado y de carácter principalmente técnico-consultivo, refleja claramente esta evolución. ENISA nació como una agencia que asesoraba y compartía conocimientos técnicos para mejorar la ciberseguridad en Europa. Tras el reforzamiento normativo de la UE, su papel se ha consolidado y fortalecido puesto que "contribuye a la política de seguridad cibernética de la UE, refuerza la confianza en productos, servicios y procesos digitales mediante esquemas europeos de certificación de la ciberseguridad" (Unión Europea, s. f.). Por lo tanto, este fortalecimiento de la agencia refleja el proceso de institucionalización, al transformar una agencia técnica secundaria en un actor central de coordinación y apoyo capaz de influir en las políticas nacionales de los Estados miembros.

El verdadero punto de inflexión se produjo en 2013, con la publicación de la Estrategia de Ciberseguridad de la Unión Europea, el primer marco político integral en esta materia. Se trata de un documento de orientación estratégico-política impulsado por la Comisión Europea y el Alto Representante para Asuntos Exteriores y Política de Seguridad para establecer una visión común y prioridades compartidas para todos los Estados miembros de la UE. Esta es una visión más integral de la ciberseguridad, que deja de entenderse como un problema exclusivamente técnico, para incorporarse plenamente a una agenda política transversal, conectada con la seguridad interior, la defensa, la política exterior y la protección de los valores democráticos, como la integridad electoral, la libertad de información y la protección de datos personales. Por lo tanto, la ciberseguridad se convierte en un instrumento clave para salvaguardar los modelos de convivencia democrática.

Esta visión estratégica se materializó jurídicamente en 2016 en la Directiva NIS (*Network and Information Security*) elaborada por la Comisión "para establecer unas capacidades comunes de apoyo, coordinación y respuesta entre los Estados miembros ante ciberincidentes" (Alonso Lecuit, 2018, p. 3). Esta supuso el primer intento de la UE por establecer requisitos mínimos de seguridad, mecanismos obligatorios de notificación de incidentes y estructuras formales de cooperación. Con esta normativa vinculante la UE pasó de un enfoque voluntario a uno regulatorio y armonizador, reforzando la resiliencia colectiva frente a ciberamenazas. Sin embargo, con el paso del tiempo se pudo observar ciertas limitaciones en su aplicación como

asimetría de aplicación entre Estados miembros. El ataque de *ransomware*[4] *WannaCry,* constituye un ejemplo paradigmático de las limitaciones del primer marco europeo de ciberseguridad. Este ciberataque se propagó de forma masiva aprovechando una vulnerabilidad en sistemas Windows y "afectó aproximadamente a 230.000 ordenadores en todo el mundo" (Kaspersky, s. f.), siendo su impacto más significativo el registrado en el sistema sanitario del Reino Unido. Un tercio de las fundaciones hospitalarias del Servicio Nacional de Salud (NHS) se vieron afectadas sufriendo la paralización de hospitales, cancelaciones de operaciones y graves disrupciones en servicios esenciales. "Se estima que este cibercrimen provocó pérdidas por valor de 4.000 millones de dólares en todo el mundo" (Kaspersky, s. f.).

El alcance sectorial de la Directiva NIS era insuficiente, ya que muchas de las entidades afectadas no se incluían como operadores de servicios esenciales según las definiciones nacionales. Esta situación fue uno de los factores que impulsó a la UE a integrar la ciberseguridad de forma definitiva como elemento central de la agenda estratégica, geopolítica y de seguridad de la Unión Europea, lo que desembocó posteriormente en la adopción de la Directiva NIS 2. Esta amplia significativamente el ámbito de aplicación hacia más sectores, subsectores y tipos de entidades, además de endurecer los requisitos de gestión de riesgos y establecer un régimen sancionador más homogéneo y disuasorio. A diferencia de la primera, se introducen responsabilidades directas para los órganos de dirección que pueden enfrentarse a sanciones personales si no cumplen. Por lo tanto, desde una perspectiva política se demuestra que la NIS 2, adoptada formalmente en 2022, consolida la ciberseguridad como elemento central del mercado interior, la seguridad y soberanía digital. En conjunto, este periodo de 2020-2022 refleja la securitización de la ciberseguridad en la UE, puesto que deja de ser un asunto técnico cuando la UE reconoce que las amenazas digitales afectan a la soberanía, la democracia y la seguridad económica.

En la etapa actual, aunque la Directiva NIS 2 entró en vigor en 2023, su transposición por los Estados miembros ha continuado avanzando durante 2024 y 2025. Cada Estado miembro tiene que ser adaptada a su propio sistema jurídico. Aunque muchos ya han aprobado normas para aplicar la directiva, no todos lo han hecho al mismo ritmo ni de forma completa. Esto refleja el desafío de armonizar un nivel elevado de ciberseguridad en toda la UE. No obstante, lo importante es que su aplicación y transposición supone el paso de un marco político y jurídico

[4] Un ransomware es un tipo de malware que retiene los datos confidenciales de un usuario, amenazando con mantenerlos bloqueados.

a un régimen de cumplimiento operativo donde la ciberseguridad pasa a formar parte de la agenda cotidiana tanto de los gobiernos como de las empresas.

Por otro lado, la UE ha anunciado avances con nuevos instrumentos regulatorios como *Cyber Resilience Act* (CRA), que refuerzan la capacidad de resistir y recuperarse de ataques. Con el CRA se pretende cambiar el momento en el que se exige la seguridad, por ello se introducen requisitos obligatorios de ciberseguridad para productos con componentes digitales como *hardwares*[5] y *softwares*.[6] "El objetivo de la normativa es garantizar que una amplia gama de productos, como cámaras domésticas conectadas, frigoríficos, televisores, juguetes y también máquinas, sean seguros antes de su comercialización" (IBF Solutions, s. f.). Esta medida amplía el alcance de la política de ciberseguridad puesto que entra directamente en el mercado y en la industria tecnológica, lo que refleja una clara decisión regulatoria y política.

Además, la Ley de Cibersolidaridad de la UE (*Cyber Solidarity Act*) entró en vigor el 4 de febrero de 2025. El reglamento pretende reforzar las capacidades de la UE para detectar amenazas y ataques con una propuesta de Sistema Europeo de Alerta de Ciberseguridad, compuesto por centros cibernéticos nacionales y transfronterizos interconectados en toda la UE. Mientas que la directiva NIS 2 se centra en la regulación y tratamiento cotidiano de los riesgos cibernéticos, esta última ley se concibe como un instrumento destinado a articular una respuesta colectiva frente a crisis cibernéticas, reflejando que la ciberseguridad es un bien común europeo y requiere una respuesta coordinada cuando se produce una crisis grave.

Otros marcos como el Reglamento de Resiliencia Operativa Digital (DORA) que entró en vigor el 16 de enero de 2023 y su aplicación se produjo a partir del 17 de enero de 2025, fortalecen la resiliencia operativa de sectores específicos como el sector financiero. "Su objetivo es reforzar la seguridad informática de entidades financieras como bancos, compañías de seguros y empresas de inversión" (Ministerio de Economía, Comercio y Empresa, s. f.), que son especialmente vulnerables a los riesgos digitales. Se exige la gestión de riesgos tecnológicos de forma continua y la revisión de sistemas para que el sistema financiero pueda seguir operando y recuperarse rápidamente cuando se produzcan incidentes digitales graves.

En definitiva, la evolución de la política de ciberseguridad en la Unión Europea refleja un proceso de progresiva politización y consolidación institucional, mediante el cual la

[5] El hardware es el conjunto de elementos físicos que componen un dispositivo informático.
[6] Un software es un conjunto de programas que dan instrucciones al dispositivo para que realice tareas específicas.

ciberseguridad ha dejado de ser tratada como un ámbito técnico y sectorial para convertirse en una posición fundamental en las prioridades políticas europeas. Este desarrollo de marco normativo ha permitido sentar las bases de una concepción compartida de la seguridad digital y ha impulsado el desarrollo de una acción europea coordinada frente a los desafíos del entorno digital.

3.2 Diplomacia digital europea

La diplomacia digital no es un ámbito separado de la ciberseguridad, sino su dimensión en el exterior, puesto que la progresiva consolidación de la política de ciberseguridad de la Unión Europea no solo ha reforzado su capacidad interna de protección y resiliencia digital, sino que también ha proyectado estas prioridades hacia el ámbito internacional. Es necesario que actúe en el plano internacional para que el entorno digital global sea más seguro al existir amenazas digitales de carácter transfronterizo y vinculadas a intereses geopolíticos, por ello, la UE ha reconocido esa necesidad de completar sus instrumentos normativos internos con una acción exterior coherente basada en la cooperación internacional, la diplomacia y el establecimiento de normas comunes en el ciberespacio. Una acción exterior con un rasgo claro de defensa de poder normativo.

En este contexto, la diplomacia digital también conocida como eDiplomacia o ciberdiplomacia se entiende como “el motor de las relaciones internacionales”. Es el conjunto de estrategias, políticas y acciones exteriores desarrolladas por los Estados para articular sus objetivos de política exterior y organización internacional a través del uso de internet, redes sociales y tecnologías digitales. La diplomacia digital surge como respuesta al impacto de las tecnologías de la información y la comunicación en el nuevo escenario de las Relaciones Internacionales, transformando las formas tradicionales de interacción, comunicación e influencia entre los actores internacionales.

En el caso de la UE, la integración del ciberespacio en la acción exterior de la UE surge motivada por la combinación del avance tecnológico global y la expansión de Internet como espacio público transnacional donde los ciudadanos interactúan de forma simultánea y en tiempo real. “La diplomacia se ha adaptado al nuevo contexto tecnológico en el que se enmarcan muchas de las relaciones entre diferentes actores políticos, sociales y económicos” (Castro Martínez, 2019, p. 45), subrayando que los canales online han pasado de ser soportes técnicos para la comunicación a convertirse en canales estratégicos para el desarrollo de la

comunicación institucional y diplomática a escala global. A diferencia de otros ámbitos de seguridad internacional donde la responsabilidad de un Estado queda relativamente limitada, en el ciberespacio ocurre que hay una elevada ambigüedad técnica que dificulta saber quién está detrás de un ataque, obligando a presentar la atribución política de ciberataques como una herramienta central de la diplomacia digital europea.

Asimismo, otro factor que influye en el desarrollo de la diplomacia digital es el cambio institucional tras el Tratado de Lisboa, que entra en vigor en diciembre de 2009 y supuso la creación de del Servicio Europeo de Acción Exterior (SEAE) como cuerpo diplomático propio de la Unión Europea encargado de coordinar y ejecutar la política exterior europea. Su objetivo es desarrollar una política exterior de la UE más coherente y eficaz, superando la fragmentación previa entre las distintas instituciones y Estados miembros, creando las bases institucionales necesarias para desarrollar una ciberdiplomacia propia y representando a la UE en foros multilaterales donde se debaten cuestiones relacionadas con la gobernanza digital.

Las primeras prácticas digitales del SEAE se orientaron fundamentalmente hacia la diplomacia pública y la comunicación estratégica, mediante la presencia activa en sus cuentas oficiales en plataformas como X y LinkedIn, donde se promovían los valores y la política exterior de la UE. Estas prácticas buscaban una comunicación más directa con los ciudadanos de diferentes audiencias externas y reforzaba la imagen y legitimidad de la Unión Europea. Además, al promover el diálogo internacional se refleja la preferencia europea por soluciones basadas en reglas, facilitando una comunicación en línea que mejora las alianzas estratégicas gracias a la difusión de posiciones comunes o declaraciones conjuntas.

No obstante, estas primeras iniciativas comunicativas constituyen solo una fase inicial del desarrollo de la diplomacia digital europea. A medida que el entorno digital se convirtió en un espacio de competencia estratégica, donde proliferan los ciberataques o la desinformación, el SEAE se consolidó como el actor central en la articulación de una diplomacia digital europea con un enfoque más estratégico y vinculada a la gestión de crisis y lucha contra la desinformación.

Además, la atribución política se inserta en una estrategia diplomática más amplia mediante la cual, la Unión Europea busca reforzar un orden internacional basado en normas en el ámbito digital. La UE afirma que la estabilidad internacional en el entorno digital no puede garantizarse sin un marco normativo común, por ello, la acción diplomática europea se basa en la Declaración aprobada por el Consejo de la UE y sus Estados miembros en noviembre de

2024. En esta se manifiesta “el respeto del marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio” (Consejo de la Unión Europea, 2024). Dicho marco se fundamenta en el Derecho Internacional existente y en principios multilaterales como la soberanía estatal, la prohibición del uso de la fuerza y el respeto a la Carta de los Derechos Humanos. Asimismo, en el marco de la ONU existen procesos específicos sobre ciberseguridad y normas de comportamiento estatal con grupos de expertos y grupos de trabajo abiertos, apoyados activamente por la UE para evitar la militarización descontrolada del entorno digital.

Esta misma lógica normativa y multilateral se extiende al caso de Internet, entendido su gobernanza como una cuestión diplomática y no solo técnica, donde la comunidad ha defendido de manera consistente un modelo de gobernanza global basado en el multilateralismo, la cooperación internacional y la participación de múltiples actores. Este modelo se distingue con otros actores internacionales que promueven modelos alternativos de control del ciberespacio como será explicado posteriormente en el caso de Estados Unidos o países como China cuyo enfoque es hacia una soberanía cibernética con un control estatal fuerte sobre Internet. Se concibe la diplomacia digital en materia de ciberseguridad orientada al refuerzo de resiliencia colectiva y no de disuasión o confrontación directa.

Para articular respuestas políticas coordinadas ante ciberincidentes graves con implicaciones internacionales, la UE ha desarrollado herramientas como el marco oficial para responder diplomáticamente a actividades maliciosas en el ciberespacio, conocido como *Cyber Diplomacy Toolbo*x, enmarcado dentro de la Política Exterior y de Seguridad Común (PESC). Esta herramienta demuestra que la UE ha institucionalizado respuestas políticas y diplomáticas frente a las ciberamenazas, puesto que articula un enfoque coordinado entre Estados miembros, el SEAE y la Comisión, como un vehículo de legitimación normativa. Aunque en ocasiones este proceso de coordinación de mensajes entre instituciones puede resultar lento debido a la necesidad de consenso interno y precisión institucional que puede reducir la capacidad para generar impacto emocional en la audiencia, al competir en redes sociales con mensajes emocionales, simples y polarizados.

En conjunto, la diplomacia digital de la Unión Europea en materia de ciberseguridad refleja la importancia de una identidad normativa y multilateral en el sistema internacional. Esta ha optado por un enfoque basado en la proyección de normas, valores y estándares compartidos promoviendo principios de los Estados democráticos como la protección de los derechos

fundamentales y comportamientos responsables por parte de los Estados miembros en el ciberespacio. Es un modelo de ciberseguridad basado en la estabilidad, la resiliencia y el respeto del orden internacional basado en normas. Aquello que empezó como una herramienta de comunicación, evolucionó como un instrumento estratégico como respuesta a amenazas híbridas, desinformación y proyección de valores digitales.

3.3 Casos destacados

El análisis de incidentes concretos ocurridos en el ciberespacio ofrece una base empírica para comprender como ha ido evolucionando la UE en el ajuste de mecanismos de ciberseguridad y diplomacia digital frente a un contexto internacional marcado por el aumento de la conflictividad e interconectado tecnológicamente. Como ha sido explicando en capítulos anteriores, el ciberespacio forma parte de la política exterior y de seguridad combinando instrumentos técnicos de protección con marcos normativos y diplomáticos.

Uno de los primeros casos de ciberincidentes de gran escala contra un Estado moderno se produce en la primavera de 2007 en Estonia. Consistió en una campaña sostenida durante 22 días de ataques con una motivación política no técnica al formar parte "de un conflicto político más amplio entre Estonia y Rusia sobre la reubicación de un monumento de la era soviética" (Ottis, 2008, p. 1, traducción propia), conocido como *Bronze Soldier*. Este monumento representaba el inicio de la ocupación soviética, mientras que para la Federación Rusa en Estonia simbolizaba la victoria contra el nazismo.

El país fue objeto de una oleada masiva de ataques de denegación de servicio distribuida (DDoS), un tipo de ciberataque que no pretende robar información, sino que satura el sistema con una cantidad enorme de peticiones al mismo tiempo impidiendo al servicio digital funcionar con normalidad. Los ataques no se dirigieron solo a una institución, sino a todo el sistema estatal y económico. Aunque Estonia era entonces un país altamente digitalizado, carecía de mecanismos sólidos de defensa frente a este tipo de amenazas y provocó la paralización en infraestructuras críticas, como páginas web del gobierno, bancos y medios de comunicación.

Uno de los aspectos más complejos de este acontecimiento fue saber quién era el autor detrás de los ataques. Muchos indicios apuntaban a hackers rusos o grupos nacionalistas rusos, sin embargo, no se logró demostrar de forma concluyente la implicación directa del Estado ruso.

Esto explicaba la ambigüedad en la autoría de los ataques, entendida como la dificultad para identificar de forma clara y concluyente al responsable de un ciberataque debido a las características que definen el ciberespacio. En primer lugar, los atacantes en el ciberespacio disponen de diversas técnicas que les permiten ocultar su identidad utilizando ordenadores ubicados en otros países para lanzar las operaciones maliciosas. Además, pueden dificultar el rastreo técnico y forense del responsable con redes privadas virtuales (VPN) o sistemas de enrutamiento que ocultan la verdadera dirección IP[7] original. "Pruebas indirectas como la coincidencia temporal entre los ciberataques y las declaraciones públicas de funcionarios rusos, junto con el hecho de que muchos ataques provenían de direcciones IP vinculadas a Rusia" (Observatorio de Ciberseguridad, 2024) hicieron poner de forma indirecta el foco en este país.

Esta falta de atribución clara tiene importantes implicaciones en el ámbito internacional, complicando la respuesta política, jurídica y militar. Si un Estado no puede probar quién lo ha atacado, surgen varios problemas, entre los que destaca la dificultad de aplicación de las normas tradicionales del derecho internacional, porque estas normas se construyeron pensando en conflictos donde el autor de la agresión era visible y fácil de identificar.

El caso de Estonia actúa como una señal de alarma estratégica, puesto que un Estado podía ser objeto de ataques sistemáticos en el ciberespacio sin recurrir al uso de la fuerza militar convencional. Este tipo de acciones se enmarcan en lo que se denomina conflictos híbridos, caracterizados por el empleo de distintas herramientas tecnológicas, diplomáticas o informativas que debilitan a otro estado. Dentro del contexto de Estonia, el ciberataque no ocurrió de forma aislada, sino en un período de fuertes tensiones políticas con Rusia por el traslado del monumento. Esto demuestra como el ciberespacio forma parte de un escenario más amplio de confrontación, donde el ámbito digital se conecta con el ámbito geopolítico para generar inestabilidad política, social y comunicativa.

Las consecuencias del episodio fueron significativas tanto para Estonia como para las organizaciones internacionales a las que pertenece, especialmente para la OTAN y la UE. En primer lugar, Estonia solicitó apoyo a la OTAN porque consideró que no se trataba solo de un problema técnico interno, sino de una posible agresión externa, una amenaza a la estabilidad del Estado y un asunto de seguridad nacional y militar. Esto generó un debate interno sobre cómo debería de ser considerado un ataque digital. Si se podía considerar como un ataque militar tradicional y, por tanto, activarse el principio de defensa colectiva establecido en el

[7] La dirección IP es una etiqueta numérica que identifica un dispositivo en Internet o en una red local.

artículo 5 del Tratado del Atlántico Norte. Este artículo establece que "un ataque armado contra una o más de ellas (las naciones firmantes), que tengan lugar en Europa o en América del Norte, se considerará como un ataque dirigido contra todas ellas" (Organización del Tratado del Atlántico Norte [OTAN], 1949), y por ello, los demás aliados deben ayudarle. No obstante, cada país decide cómo ayudar, según lo que considere necesario. Este solo se ha activado una vez en la historia cuando se produjeron los atentados del 11 de septiembre de 2001. Sin embargo, cuando se produjeron los ciberataques contra Estonia en 2007, no estaba claro si este tipo de ataques podían considerarse como una agresión que permitiese activar el principio de defensa colectiva.

En ese contexto en 2008, se asentaron las bases para el desarrollo posterior de una política europea de ciberseguridad y diplomacia digital. Se creó en Tallin el *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), un organismo internacional de investigación, formación y cooperación en materia de ciberdefensa. "Su objetivo era fortalecer las capacidades de ciberdefensa de los países miembros de la OTAN, promoviendo la investigación, el intercambio de conocimientos y la cooperación en la lucha contra las amenazas cibernéticas" (Observatorio de Ciberseguridad, 2024). Entre sus principales aportaciones destaca la elaboración del llamado Manual de Tallin, un estudio sobre cómo se aplican las leyes de la guerra y del derecho internacional en el ciberespacio. Aunque no es una ley obligatoria, sino una guía jurídica, ha tenido mucha influencia práctica.

Su creación convirtió a Estonia en un referente internacional en materia de ciberseguridad. La importancia de este centro y del trabajo realizado en Tallin se refleja en casos posteriores de ciberataques a gran escala, como el ataque a la red eléctrica de Ucrania en 2015. Es uno de los primeros ejemplos documentados de una operación cibernética que afectó a varias compañías distribuidoras de energía en el oeste del país y provocó costes de electricidad que dejaron sin suministro a aproximadamente 225.000 personas durante varias horas.

El ataque se desarrolló mediante una operación compleja y coordinada que combinó técnicas de ingeniería social, *malware* especializado y manipulación remota de sistemas industriales. Los atacantes entraron en los sistemas informáticos de tres compañías regionales de distribución eléctrica y otras tres organizaciones de distintos sectores críticos, tomando el control de los paneles digitales que gestionaban la electricidad (Estrella Digital, 2025). Una vez dentro de los sistemas, los intrusos utilizaron un *malware* denominado *BlackEnergy* que

les permitió recopilar información durante meses y preparar el ataque final que culminó con la interrupción del suministro eléctrico.

Uno de los elementos más relevantes del caso fue su carácter híbrido y coordinado, una estrategia que combina el uso de tácticas convencionales y no convencionales para desestabilizar a los oponentes. Estos ataques no se limitaron a interrumpir el suministro de energía, sino que llevaron a cabo ataques de denegación de servicio (DDoS) contra los centros de atención telefónica de las compañías eléctricas. Además del impacto técnico, miles de ciudadanos intentaron llamar a las compañías eléctricas, aumentando la sensación de caos entre la población por la falta de coordinación de respuesta. Esta combinación de técnicas evidenció un alto nivel de planificación y conocimiento de los sistemas industriales, así como la intención de maximizar el impacto social y psicológico del ataque.

De ambos casos, se observa que la UE actúa principalmente a través de la cooperación y el fortalecimiento de capacidades. La cooperación global en ciberseguridad se ha convertido en una cuestión clave ante las crecientes amenazas cibernéticas. En el caso de Estonia, mostró solidaridad política y técnica con el reconocimiento del problema como asunto que afectaba a toda Europa. Asimismo, comenzó a desarrollar estrategias comunes de ciberseguridad como la Estrategia Europea de Ciberseguridad o la Directiva NIS, que mejorasen la resiliencia colectiva y el reconocimiento del ciberespacio como ámbito clave de seguridad. Por otro lado, en ambos casos se muestra como la UE actúa dentro de un marco multilateral e institucional, colaborando estrechamente con otras organizaciones internacionales y con los propios Estados miembros. Una preferencia por instrumentos diplomáticos, económicos y tecnológicos en lugar de respuestas militares directas. Esta forma de actuación se basa en el principio de seguridad cooperativa, con instrumentos no militares que responden a la naturaleza de la Unión Europea con un “poder blando y normativo”:

4. Estados Unidos: seguridad nacional y liderazgo tecnológico

4.1 Evolución de la estrategia de ciberseguridad

La estrategia de ciberseguridad de Estados Unidos ha evolucionado de forma progresiva y reactiva, al ir desarrollándose poco a poco, en distintas etapas, conforme Internet y las tecnologías digitales se volvieron más complejas. La prosperidad y la seguridad de Estados Unidos se han vuelto más dependientes de un ciberespacio seguro, al depender de manera

directa en como el país responde a los desafíos y oportunidades del ciberespacio. (The White House, 2018, pp. 1–2). Esto rompe la idea de que la ciberseguridad es un asunto técnico y sostiene que se ha convertido en una infraestructura esencial comparable con sistemas de defensa tradicionales como carreteras, ferrocarriles o puertos. Su evolución ha estado marcada por hitos como el fortalecimiento de organismos dedicados exclusivamente al ciberespacio en la proyección de poder y liderazgo global de EEUU.

En 1969 nació ARPANET, "una red de ordenadores creada durante la Guerra Fría cuyo objetivo era eliminar la dependencia de un Ordenador Central" (Sevilla Robles, 2020, p. 9), formada por universidades, centros de investigación y organismos gubernamentales. En los primeros años de la informática en red, la sociedad no era consciente de los riesgos asociados al acceso no autorizado puesto que había pocos usuarios en la red, los cuales utilizaban los sistemas con fines académicos o científicos. Sin embargo, a medida que los sistemas informáticos se volvieron más complejos y valiosos, fue necesario implantar una ley federal de gran alcance destinada a combatir los delitos informáticos en EEUU. Se aprobó el *Computer Fraud and Abuse Act* (CFAA) para combatir el *hacking*, a través de la prohibición de acceso a un ordenador "sin autorización" o "excediendo autorización" (National Association of Criminal Defense Lawyers, s. f.). No obstante, el principal problema de esta ley reside en deficiencias estructurales derivadas de su vaguedad conceptual y su expansión normativa, lo que compromete la seguridad jurídica y favorece aplicaciones desproporcionadas del régimen sancionador.

Durante los años 90, Internet experimentó un crecimiento exponencial y dejó de ser una tecnología técnica, confinada a círculos de investigación y militares, y empezó a filtrarse en la vida cotidiana de la sociedad como infraestructura pública esencial. En ese contexto, se produjo uno de los primeros incidentes graves de ciberseguridad conocido como Morris Worm que evidenció la falta de preparación frente a incidentes informáticos y demostró que incluso redes utilizadas por universidades y organismos gubernamentales podían ser vulnerables a ataques. Esto generó una creciente preocupación por la aparición de vulnerabilidades en los sistemas computacionales, porque cuanto más se digitaliza una sociedad, más expuesta queda a interrupciones, sabotajes o manipulaciones externas. Los ataques y fallos informáticos se gestionaban de manera improvisada y aislada, lo que aumentaba los daños y el tiempo de recuperación. Se trataba de una etapa que reforzaba la idea de una evolución progresiva, mediante ajustes parciales y sin una reforma profunda del Estado.

Uno de los primeros hitos fue la creación de equipos de respuesta a incidentes informáticos, conocidos como CERT (*Computer Emergency Response Team)* (Centro Criptológico Nacional, s. f.). Se trata de una organización especializada en detectar, analizar y mitigar ataques o fallos relacionados con la seguridad de las redes o los equipos. Estos equipos fueron fundamentales para el intercambio de información y alertas tempranas para asentar las bases de la ciberseguridad moderna a nivel nacional e internacional, demostrando que las amenazas digitales no respetan fronteras. No obstante, la ciberseguridad aún no se concebía como un componente central de la estrategia de seguridad nacional, pues términos como "ciberseguridad" o "ciberamenaza" no estaban consolidados. Las respuestas institucionales en Estados Unidos durante la década de 1990 siguieron siendo predominantemente técnicas y defensivas. La preocupación principal era asegurar los sistemas críticos del gobierno y del ejército, en lugar de en el desarrollo de una estrategia integral que abarcara al sector privado y a la sociedad en su conjunto.

El punto de inflexión lo marcaron los atentados del 11 de septiembre de 2001, que trasformaron la visión estadounidense hacia la seguridad. Aunque no fueron ataques cibernéticos, sus consecuencias demostraron que actores no estatales podían causar daños catastróficos utilizando medios no convencionales. "Uno de los aprendizajes fue la necesidad de establecer medidas de protección estrictas e innovar en tecnología especializada en defensa, seguridad de las infraestructuras y protección de las comunicaciones" (IT User, 2021), puesto que, si se trasladaba al ámbito digital, podría tener efectos similares.

La creación del *Department of Homeland Security* (DHS) en 2002-2003 simboliza este cambio. Este se encarga de la protección y resiliencia de infraestructuras críticas, incluidas las digitales, y funciona bajo la coordinación de más de 260.000 perfiles profesionales, lo que subraya como la ciberseguridad deja de concebirse de forma aislada a la seguridad nacional, y se convierte en una función esencial del Estado (Department of Homeland Security, 2026). Sobre esta base institucional, en ese período se publicó la *National Strategy to Secure Cyberspace*, considerada como el primer intento de articular de manera sistemática una política nacional de ciberseguridad. Cuenta con tres objetivos estratégicos que consisten en la prevención de ciberataques contra las infraestructuras críticas, la reducción de la vulnerabilidad nacional frente a los ciberataques y reducción de los daños y tiempo de recuperación tras los ataques (The White House, 2003). Se trata de una etapa que se caracteriza por la comprensión de la ciberseguridad como una cuestión de defensa interna y emergencia de la dimensión

internacional de esta, al identificarse a Estados hostiles como posibles responsables de ciberataques contra intereses estadounidenses.

Por lo tanto, con la llegada de Barack Obama a la presidencia, su Plan de Ciberseguridad estaba basado en tres factores fundamentales que describían la necesidad de otorgar al ciberespacio de un carácter estratégico que ejerce poder y proyecta fuerza. Se refiere a la digitalización masiva de la sociedad y las infraestructuras críticas, el aumento visible y sofisticado de ciberataques como el que sufrió personalmente, cuando los sistemas de la campaña demócrata para la elección presidencial de 2008 que fueron hackeados y la constatación de que la respuesta estatal existente era fragmentada e insuficiente. A partir de este diagnóstico, la administración Obama reconoce que la vulnerabilidad el Estado crece a un ritmo superior a su capacidad defensiva si no se actúa de forma coordinada y era una forma de poder mantener seguro al pueblo. Un modelo que priorizaba la prudencia política y la coordinación internacional, aun a costa de una menor rapidez operativa.

Por ello, ese mismo año, se creó el *U.S Cyber Command* (USCYBERCOM), dependiente del Departamento de Defensa, para coordinar y ejecutar operaciones militares en el ciberespacio y proteger las redes del Pentágono. Las redes del Pentágono son uno de los objetivos más valiosos en el ciberespacio, puesto que son los sistemas digitales que permiten funcionar a las Fuerzas Armadas de EE.UU. Su compromiso podría afectar directamente la operatividad militar y la capacidad de respuesta ante amenazas, lo que hace que su protección deje de ser una tarea técnica y pasa a ser una misión estratégica y militar. Esta decisión supuso un cambio doctrinal que implica que la ciberseguridad deja de ser únicamente reactiva y defensiva para incorporar capacidades ofensivas que interrumpan sistemas adversarios o degradar capacidades militares enemigas. En el modelo promovido por Obama, las ciberoperaciones se concebían como acciones con potenciales implicaciones estratégicas, lo que justificaba la intervención directa de la Casa Blanca y del Consejo de Seguridad Nacional.

En el plano estratégico, se impulsaron planes y marcos nacionales de actuación entre los que desataca el *Cybersecurity National Action Plan* (CNAP), presentado en 2016, para mejorar la seguridad cibernética del gobierno federal y de toda la nación mediante inversión, modernización tecnológica y colaboración entre gobierno, empresas y ciudadanos para enfrentar las amenazas digitales. Mientras que Obama priorizó la construcción de marcos normativos, institucionales y de cooperación, con la llegada de la administración Trump, la

estrategia de ciberseguridad se reorientó hacia una lógica de competencia estratégica entre grandes potencias.

Uno de los rasgos distintivos de la política de ciberseguridad de Trump fue la reconfiguración de los mecanismos de supervisión política y control civil sobre las ciberoperaciones. A diferencia del enfoque adoptado durante la presidencia de Barack Obama, caracterizado por un alto grado de centralización al tomar las decisiones sobre ciberseguridad desde niveles altos del gobierno y por procesos de autorización complejos, la administración Trump optó por ampliar la autonomía del ámbito militar y operativo, especialmente del *U.S. Cyber Command.* Este cambio se materializó en 2018 con la *National Cyber Strategy* que enfatizó la necesidad de "defender hacia adelante", de intervenir en redes externas donde se detecta actividad maliciosa en su origen, no solo cuando ya ha cruzado la frontera defensiva. Por un lado, se fortaleció la capacidad del Estado para actuar con rapidez y persistencia en el ciberespacio, pero también se generaron riesgos asociados a la reducción de la supervisión política.

La *National Cybersecurity Stategy* de 2023 de la administración Biden introduce un enfoque más estructural al redistribuir la responsabilidad de la ciberseguridad entre el Estado, el sector privado y otros actores, y establecer estándares mínimos de ciberseguridad. Sin embargo, este énfasis regulatorio y civil no implica el abandono de las capacidades ofensivas que actualmente se observa en la política de ciberseguridad de los Estados Unidos. En 2025, la presidencia de Trump presenta una clara continuidad doctrinal con respecto a la aplicada durante su anterior mandato caracterizado por operacionalizar la ciberguerra, pero dentro de un contexto donde el ciberespacio ya no es un dominio emergente ni experimental. La prioridad actual es gestionar el riesgo sistémico derivado de la profunda dependencia de la sociedad respecto al ciberespacio, no demostrar su capacidad ofensiva.

En conjunto, la evolución de la estrategia de ciberseguridad de Estados Unidos se caracteriza por una transformación progresiva, pasando de un enfoque limitado y reactivo a un planteamiento en el que el ciberespacio se consolida como un ámbito central de la seguridad nacional y competencia geopolítica. Esta evolución sienta las bases para el desarrollo de una diplomacia digital estadounidense orientada a la promoción de normas, alianzas y estándares internacionales que reflejen sus intereses estratégicos.

4.2 Diplomacia digital estadounidense

En el discurso estratégico estadounidense, aunque el país ya se había involucrado en la diplomacia digital bajo la presidencia de George W. Bush, no sería hasta 2009 cuando se institucionalizó la diplomacia digital como un componente central de su política exterior, dotándola de estructuras, recursos y objetivos estratégicos claros.

A diferencia de la Unión Europea, en la primera estrategia integral del gobierno de EE.UU enfocada específicamente en el ámbito internacional de ciberespacio, se establece que este tiene que ser abierto, interoperable, seguro y confiable y que, en consecuencia, el país trabajará internacionalmente para promover estas características. Por ello, el gobierno estadounidense concibe su estabilidad como esencial para el crecimiento económico, la seguridad, y el ejercicio de libertades fundamentales. Esta estrategia otorga a la diplomacia digital un papel que se despliega de forma transversal en distintos ámbitos de la acción exterior del Estado.

La diplomacia digital estadounidense y los esfuerzos diplomáticos en el ciberespacio no dependen de una sola institución, sino que cuenta con una arquitectura institucional compleja y descentralizada. Es el resultado de la interacción entre agencias federales civiles, militares y de inteligencia, con el Departamento de Estado como núcleo diplomático formal, pero sin una autoridad única que concentre todas las competencias. En primer lugar, el Departamento de Estado (DoS) es la agencia que maneja la política exterior y desempeña un papel central en la articulación de la diplomacia digital, mientras que las oficinas especializadas en el ciberespacio y tecnologías emergentes son estructuras internas creadas dentro del propio Departamento. Su objetivo principal es liderar los esfuerzos de la política exterior de EEUU, representando al país ante otros Estados y organismos internacionales, y negociar acuerdos, normas y compromisos multilaterales. No obstante, el Departamento de Estado no actúa de forma aislada. La Casa Blanca, es el centro político que ejerce el poder ejecutivo, sin embargo, no ejerce funciones diplomáticas directas, define y coordina las grandes prioridades que guían la acción exterior en el ámbito digital. Esto se plasma en documentos como *National Cybersecurity Strategy,* que sirve de marco para la acción del Departamento de Estado y del resto de agencias implicadas.

A medida que el ciberespacio comenzó a consolidarse como dominio estratégico, resultó evidente que el país carecía de un órgano único encargado de articular una respuesta diplomática coherente. Por ello, Estados Unidos crea el *Bureau of Cyberspace and Digital Policy (CDP)* en abril de 2022, como oficina interna del Departamento de Estado. “El Estado

creó la oficina para elevar el ciberespacio como concepto organizativo de la diplomacia estadounidense, consolidando los esfuerzos y el liderazgo de las actividades relacionadas con el ciberespacio en una sola unidad" (U.S. Government Accountability Office, 2025). Asimismo, el Departamento de Defensa y el *U.S Cyber Command* contribuyen a la dimensión disuasoria y de seguridad, frente a amenazas procedentes de otros países.

En la práctica, la diplomacia digital estadounidense se materializa a través de un conjunto amplio de instrumentos que combinan herramientas diplomáticas clásicas, como la negociación entre Estados, con herramientas nuevas propias del mundo digital. Entre los instrumentos más importantes se encuentra la promoción activa de 11 normas internacionales consensuadas a nivel de Naciones Unidas y recogidas en un documento acordado por los Estados miembros sobre el comportamiento de los Estados en el ciberespacio. Estas no son legalmente vinculantes ni obligatorias, pero representan un consenso internacional para reducir riesgos a la paz y seguridad internacionales. El país emplea estas normas consensuadas a nivel de la ONU, como punto de partida para su propia diplomacia digital para negociar con otros países normas de conducta cibernética (UNODA, 2022). Asimismo, el país reconoce la aplicabilidad del derecho internacional al ámbito cibernético. Por ejemplo, el uso de la fuerza en el ciberespacio se rige por el derecho internacional y el Artículo 2(4) de la Carta de las Naciones Unidas, "las actividades cibernéticas que tienen como resultado inmediato muerte, lesiones o destrucción significativa probablemente se considerarían uso de la fuerza" (Theohary, 2024).

Otro instrumento clave es la atribución respecto a etapas anteriores de la política estadounidense en el ciberespacio es la atribución pública de ciberataques a Estados u otros actores maliciosos. En un primer momento, el Estado prefería no revelar públicamente quien estaba detrás de un ciberataque con el objetivo de evitar escalar conflictos y no revelar capacidades sensibles para tratarlo por vías diplomáticas privadas. Sin embargo, a medida que el ciberespacio se convirtió en un dominio más hostil y central para la seguridad nacional, mantener el silencio reforzaba la impunidad y animaba más ataques.

Por ello, existen informes publicados por el Congreso de Estados Unidos titulado *"Cybersecurity: Selected Cyberattacks*, 2012-2024" en el que se describen y se recopilan una selección de ciberataques importantes contra entidades dentro de EEUU. En el informe Rusia figura como actor presuntamente responsable en materia de ciberseguridad contra entidades estadounidenses. El país "utiliza una amplia gama de tácticas, que incluyen diplomacia antiestadounidense, tácticas de coerción energética, desinformación, espionaje, operaciones de

influencia, intimidación militar, ciberataques y herramientas de zona gris" (Cybersecurity and Infrastructure Security Agency [CISA], s. f., traducción propia). El caso más emblemático se produjo en 2016 con la interferencia de Rusia en las elecciones de EE.UU para influir en el resultado de las elecciones presidenciales entre Donald Trump y Hillary Clinton. Según el informe del Comité de Inteligencia del Senado de Estados Unidos, Rusia ha empleado la *Internet Research Agency* (IRA), una empresa privada, para realizar operaciones de influencia en redes sociales con cientos de personas organizadas en turnos de 12 horas (SPYSCAPE, 2023). Se creaban perfiles falsos en redes sociales como Facebook y foros de noticias, produciendo contenidos coordinados para generar desconfianza en el sistema político y amplificar mensajes a favor o en contra de candidatos.

Por otro lado, tras el regreso a la presidencia de Donald Trump en 2025, el país ha realizado un cambio de estrategia política de EE.UU hacia Rusia. Ese mismo año, ciertas agencias de EE.UU como el FBI o el Departamento de Seguridad Nacional, redujeron esfuerzos coordinados para contrarrestar sabotaje, desinformación y ciberataques rusos, al mismo tiempo que la administración Trump presionaba para que se pusiese fin a la guerra entre Rusia y Ucrania. El presidente ha argumentado que el conflicto en Ucrania podría escalar a una Tercera Guerra Mundial y que mejorar las relaciones con Rusia es de interés estratégico para EEUU, lo cual encaja con un enfoque clásico de realismo geopolítico (Kirchgaessner, 2025). En este marco, Rusia es concebida como una potencia nuclear, al disponer de uno de los mayores arsenales nucleares del mundo, cuya confrontación directa con Estados Unidos podría escalar hacia un conflicto de gran intensidad con riesgos sistémicos para la seguridad internacional. Por lo tanto, reducir el apoyo en el ciberespacio se puede justificar como intento de bajar la tensión directa con Rusia.

Asimismo, la reducción del apoyo a Ucrania forma parte de una reconfiguración geopolítica del ciberespacio donde EE.UU está redistribuyendo su atención hacia otras regiones, incluido Oriente Medio. "De acuerdo con *Microsoft Threat Intelligence*, Irán fue responsable de al menos 17% de los ciberataques atribuidos a actores estatales en Medio Oriente en 2024" (Reyes, 2025), convirtiéndose en el principal vector geopolítico digital. En este contexto, Oriente Medio se ha consolidado como un escenario prioritario debido a la creciente actividad cibernética iraní sobre infraestructuras digitales poco protegidas. Por ello, la política digital de Washington en Oriente Medio desde 2018, se ha basado en la implantación de una estrategia que combina sanciones económicas y tecnológicas, "que restringen la exportación de

semiconductores avanzados, inteligencia artificial y componentes para drones y armas inteligentes", con aliados regionales como Israel y los países del Golfo.

EE.UU coopera estrechamente con Israel, siendo su principal aliado cibernético al ser líder en tecnología militar digital, con el objetivo común de contener a Irán. Desde 2017, existe un U.S-Israel *Cyber Working Group,* para compartir intereses estratégicos comunes y defenderse frente a ataques iraníes. Esta relación incluye cooperación operativa observada en 2024 cuando realizaron el ejercicio *CYBERDOME IX,* que fue una operación cibernética ofensiva que permitió imponer costes a Irán y enviar señales disuasorias sin recurrir a una escalada militar directa. Su cooperación se basa en una alianza tecnológica y militar de máximo nivel, mientras que, si se compara con su cooperación con Marruecos, se puede observar una relación estratégica regional y de estabilidad regional. Este último, en un análisis sobre *Defense 5.0* se explica cómo está evolucionando para convertirse en un socio estratégico y cibernético emergente (Roudani, 2025). Esta cooperación refleja el creciente papel de la diplomacia digital como instrumento de seguridad regional y proyección de poder en el ciberespacio.

4.3 Casos destacados

El estudio de incidentes concretos en el ciberespacio sirve de base para comprender como ha sido adaptada su estrategia ante amenazas concretas. Cada incidente relevante muestra vulnerabilidades estructurales en los sistemas de defensa digital que deben ser analizados dentro de un entorno internacional marcado por la independencia digital y la intensificación de la competencia geopolítica en el ciberespacio. A diferencia de la Unión Europea, cuyo enfoque en materia de ciberseguridad se ha orientado más hacia la regulación y coordinación normativa, la respuesta estadounidense a episodios significativos en el ciberespacio se clasifica por una lógica de seguridad nacional, disuasión y proyección de poder.

Uno de los casos más paradigmáticos fue el ciberataque conocido como *SolarWinds,* considerado como un ciberataque silencioso, masivo y estratégicamente significativo en la evolución reciente de la política de ciberseguridad y diplomacia digital de EE.UU. Este fue un ataque ocurrido entre finales de 2019 y 2020, que afectó a la cadena de suministro de software de múltiples agencias gubernamentales estadounidenses como el Departamento de Justicia (DOJ) y empresas privadas. *SolarWinds,* fue un actor clave en la esfera del software, sobre el que se originó el incidente al ser introducido en su producto principal, un código malicioso dentro de una actualización oficial del programa. Esta empresa sería objetivo ideal para los

piratas informáticos porque contaban con acceso privilegiado para recopilar datos de estratégicos del gobierno y grandes empresas. Las autoridades estadounidenses atribuyeron el ataque a actores vinculados al servicio de inteligencia exterior ruso (SVR), siendo uno de los impactos más notables la consecuencia financiera del ataque, con más de 18.000 clientes de la empresa afectados por la actualización instalada. Esta atribución estatal evidenció que las operaciones cibernéticas pueden formar parte de estrategias de influencia y competencia internacional, lo que impulsó la integración de la ciberseguridad en la política exterior y de de defensa.

El ataque fue detectado tras 9 meses, gracias a la empresa de ciberseguridad *FireEye* y sería la agencia federal CISA (*Cybersecurity and Infraestructure Security Agency*) la encargada de emitir alertas urgentes para todo el país para la desconexión de *SolarWinds Orion* y mitigar accesos persistentes. Asimismo, EE.UU respondió como ante una acción hostil internacional, impulsando un cambio de paradigma hacia el modelo z*ero trust* en los modelos de ciberseguridad y el desarrollo de equipos de respuesta rápida (CSIRT) para "minimizar los daños a los sistemas y los datos, erradicar la amenaza y restaurar rápidamente el estado operativo de los sistemas" Akamai (s. f.) . Incluso las actualizaciones firmadas y verificadas pueden ser peligrosas para el usuario.

Uno de los impactos más notables, fue la consecuencia financiera de este, "en promedio el ataque les costó a las empresas el 11% de sus ingresos anuales" Fortinet (s. f.), recibiendo el impacto más dramático las empresas estadounidenses. No obstante, también se observó un profundo cambio en la política de ciberseguridad estadounidense. En primer lugar, el caso de *SolarWinds* "mostró que la ciberseguridad ya no es solo técnica, sino estratégica y geopolítica", dejando en evidencia que los ataques más devastadores no serán necesariamente los más ruidosos.

Un rasgo particularmente distintivo de la diplomacia digital estadounidense es la interdependencia estructural entre el Estado y el sector privado, especialmente entre las grandes corporaciones tecnológicas que influyen en la configuración de normas, estándares y prácticas internacionales en materia digital. Tras el alcance de este incidente, se revelaron vulnerabilidades críticas en la protección de infraestructuras digitales, ya que un solo proveedor fue capaz de comprometer la gestión de la cadena de suministro de software de todo un Estado. Por ello, el gobierno estadounidense impulsó reformas orientas a reforzar la cooperación entre el sector público y el sector privado. Asimismo, se impuso sanciones económicas y

diplomáticas a entidades vinculadas al SVR y reforzó la estrategia de EE.UU conocida como *"naming and shaming"* comentada en capítulos anteriores, con el objetivo de erosionar la reputación del Estado atacante y colocarlo en una posición defensiva ante la comunidad internacional.

Por otro lado, en un contexto de preocupación sobre la vulnerabilidad cibernética de las infraestructuras críticas, el caso Colonial Pipeline consiste en otro ejemplo significativo para comprender la evolución de la política de ciberseguridad de EE.UU sobre infraestructuras críticas. Este ataque tuvo lugar en 2021 y su criticidad es tan elevada porque afectó a "uno de los oleoductos más largos de Estados Unidos, que transportaba alrededor de tres millones de barriles de combustible al día a través de 8,850 kilómetros de Houston a Nueva York" (Jorge Ricart, 2021, p. 3)

Colonial Pipeline es una de las principales empresas de transporte de suministro de gasolina, diésel y combustible del que depende la mayoría de los aeropuertos del este de EE.UU. Su ataque se atribuye al grupo criminal DarkSide que implantó un *ransomware,* entendido como "un código malicioso que tomó el control de las computadoras del entorno de la tecnología de la información (TI)" (Rockwell Automation, s. f.). Esta organización de ciberdelincuencia operaba desde Europa del Este e utilizó un software malicioso que afectaba a los sistemas informáticos de gestión de Colonial Pipeline, buscando el robo de datos del sistema del oleoducto para posteriormente pedir una cantidad económica por su rescate. Aunque los sistemas industriales no fueron directamente destruidos, el cierre temporal del oleoducto provocó un impacto inmediato en la economía estadounidense, ocasionando, "retrasos en el suministro de combustible a lo largo de la costa este, lo que disparó el coste de la gasolina un 4%" (Pankov, 2021). Este corte escaló con rapidez, registrando su pico más alto en seis años, puesto que la población reaccionó con compras compulsivas que generaban grandes colas en las estaciones en varios estados como Georgia, Virginia o Carolina del Norte. Además, su origen en un entorno geográfico vinculado a un rival estratégico para Estados Unidos contribuyó al incremento de tensiones diplomáticas y se exigió a Rusia una mayor cooperación para combatir a los grupos criminales que operaban desde su territorio.

Estos efectos inmediatos en la economía y en la vida cotidiana de los ciudadanos hicieron que la Administración Biden respondiese declarando el estado de emergencia apenas un día después del ataque. Como consecuencia, la Administración de Seguridad en el Transporte (TSA), tradicionalmente encargada de seguridad física como el terrorismo, emitió normas

obligatorias de ciberseguridad para operadores de oleoductos, exigiendo la notificación inmediata al gobierno federal ante cualquier ciberataque. Además, la OFAC (O*ffice of Foreign Assets Control*), perteneciente al Departamento del Tesoro de EE.UU, se encarga de la gestión de sanciones económicas y financieras. Tras este acontecimiento, introdujo una dimensión financiera y jurídica en la respuesta estatal ante un ciberataque de *ransomware*. Esta advirtió sobre posibles sanciones a aquellos que pagasen rescates a grupos de *ransomware* vinculados a actores sancionados. Se trata de una estrategia deliberada que trata de no incentivar pagos que aumenten el negocio del *ransomware*, estableciendo una zona gris que no impide el pago, pero tampoco lo respalda y protege abiertamente. Asimismo, el caso consolidó la integración de la ciberseguridad en la política exterior y de seguridad nacional, con un fortalecimiento del papel de agencias como *Cybersecurity and Infraestructure Security Agency (CISA)* y el Departamento de Seguridad Nacional.

En definitiva, este acontecimiento impulsó nuevas iniciativas destinadas a reforzar la protección de infraestructuras críticas y a mejorar la resiliencia frente a ataques de *ransomware.* La dependencia de sistemas centralizados y la falta de un marco internacional eficaz, hizo que el país entero experimentase como un ataque informático es capaz de trastocar su economía diaria, lo que hizo que se considerase como una amenaza a la seguridad nacional con implicaciones geopolíticas. Por ello, se hizo necesario el cambio de mentalidad desde una concepción de ciberseguridad como fusión técnica limitada al ámbito informático hacia su reconocimiento como un elemento transversal que afecta a toda la organización.

5. Análisis comparado: UE vs EEUU

El análisis comparado entre la Unión Europea y Estados Unidos en materia de ciberseguridad y diplomacia digital constituye un enfoque esencial para comprender las diversas estrategias mediante las cuales los principales actores internacionales abordan la gobernanza del ciberespacio en un contexto caracterizado por una sociedad que depende de los sistemas digitales. Esto implica que la tecnología digital deje de ser un mero instrumento económico para convertirse en un recurso estratégico vinculado a la seguridad, la autonomía y la proyección internacional de los Estados. El objetivo de este análisis no es determinar qué modelo es más eficaz, sino identificar las lógicas que orientan la acción de cada actor y sus implicaciones. Comparar ambos modelos permite comprender similitudes y diferencias en sus

estructuras políticas, capacidades tecnológicas y prioridades estratégicas en sus políticas de ciberseguridad y en el desarrollo de la diplomacia digital.

Ambos actores constituyen referentes globales que permiten obtener un valor analítico significativo del sistema internacional digital. Sin embargo, sus enfoques se basan en tradiciones políticas e institucionales diferentes, lo que explica la divergencia en sus enfoques regulatorios y estratégicos. La principal divergencia radica en la forma en la que ambos actores conciben el ciberespacio y su función dentro del sistema internacional.

La Unión Europea concibe el ciberespacio desde una perspectiva normativa y de gobernanza global, un espacio regulado gracias a la construcción de marcos normativos comunes. En este sentido, la UE afirma que "seguirá promoviendo y defendiendo sus valores a nivel multilateral en todo el mundo" (European Commission, s. f.) , con una gobernanza digital global como área clave donde poder seguir desarrollando normas y estándares de acuerdo con valores comunes basados en los derechos humanos. Un modelo mucho más orientado hacia los valores democráticos, los derechos fundamentales y un enfoque regulatorio coherente. La concepción de la seguridad digital se articula en torno a la noción de "*security as resilience*", entendida como la capacidad de las instituciones, infraestructuras y sociedades para resistir, adaptarse y recuperarse frente a amenazas cibernéticas persistentes. Así, el ciberespacio es interpretado como un ámbito de regulación, cooperación internacional y construcción de un orden digital basado en reglas y valores compartidos.

Por otro lado, "el ejército estadounidense se refiere al ciberespacio como un dominio o sector de acción (como tierra, mar, aire y espacio)", siendo un componente creciente de la seguridad nacional estadounidense, dado su papel en infraestructuras críticas y sistemas militares. El país depende estructuralmente del ciberespacio para el funcionamiento de su defensa militar, su economía digital o sus infraestructuras críticas. Además, le influye la creciente exposición a amenazas procedentes de otros Estados con los que mantiene rivalidad estratégica como Rusia o China. Por ello, este último ha priorizado una lógica de seguridad nacional, liderazgo tecnológico y proyección geopolítica del poder en el ciberespacio. Esta diferencia responde, en parte, a la naturaleza supranacional de la UE, al no ser un Estado único, sino una unión de muchos Estados (27) que comparten reglas e instituciones, pero mantienen su soberanía y tiende a actuar mediante regulación y coordinación interna. Asimismo, la condición de superpotencia global de EE. UU hace que todo lo que afecte a su poder global se considere un asunto de seguridad.

Esta concepción del ciberespacio como componente esencial de la seguridad nacional ha favorecido una evolución rápida y securitaria de la política de ciberseguridad estadounidense, caracterizada por un desarrollo más temprano y rápido en comparación con el modelo europeo. Desde principios de los 2000, en EE. UU ya se conocían ciertos términos como "*cyberwar,* "*cyber threats*" o "*cyber deterrence*" y tras el 11-S, la seguridad se convirtió en prioridad absoluta. La creación de organismos especializados como el *U.S Cyber Command,* la *Cybersecurity and Infraestructure Security Agency (CISA)* y el *Department of Homeland Security (DHS)* en materia de protección digital e infraestructuras críticas, reflejan esta evolución y evidencian la creciente institucionalización de la seguridad digital en la estructura estatal estadounidense.

En contraste, la evolución europea siguió una trayectoria distinta. La incorporación del ciberespacio a su doctrina de seguridad y defensa ocurre de forma gradual, sobre todo entre 2013 y 2022, puesto que antes el enfoque europeo era más regulatorio y económico que militar o estratégico. Asimismo, su evolución también estaba condicionada por su estructura institucional y por la necesidad de coordinar las políticas de los Estados miembros. Aunque desde 2013 comenzó a reconocerse su dimensión estratégica, fue a partir de la Estrategia Global de la UE de 2016, y de forma más consolidada, con el *Strategic Compass* de 2022 cuando el ciberespacio se integró plenamente como dominio relevante para la seguridad y defensa europeas.

Instrumentos jurídicos como la Directiva NIS o el Reglamento General de Protección de Datos (RGDP) reflejan esta prioridad regulatoria, orientada a fortalecer la resiliencia digital y la confianza en el entorno tecnológico. Estos instrumentos forman parte de lo que se denomina armonización normativa, cuyo objetivo es que todos los países tengan reglas similares para evitar fragmentaciones y asegurar que el mercado digital funcione de manera segura y coherente. La estabilidad y seguridad del ecosistema digital se logra gracias a la coordinación entre los Estados miembros, lo que explica la evolución más lenta de la política europea en comparación con el modelo estadounidense.

Además del marco normativo, la Unión Europea ha desarrollado redes de cooperación, agencias especializadas y mecanismos de respuesta conjunta. Entre ellos destaca la red de equipos de respuesta a incidentes, conocida como CSIRT (C*omputer Security Incident Response Teams*), que permite el intercambio de información en tiempo real entre los Estados miembros y facilita la coordinación técnica ante ciberataques de gran escala. Un ejemplo

significativo del papel de los equipos CSIRT fue su actuación durante el ataque global de *ransomware WannaCry,* donde se evidenció como este tipo de elementos eran de especial importancia para la resiliencia digital y la gestión coordinada de crisis en el ciberespacio.

Desde una perspectiva comparada, puede afirmarse que la Unión Europea ha politizado e institucionalizado la ciberseguridad al incorporarla progresivamente a su agenda política, económica y normativa, lo que significa convertirla en tema de políticas públicas, regulación y gobernanza. Esto se evidencia en la adopción de marcos regulatorios específicos sobre ciberseguridad para coordinar a los Estados miembros, como *Digital Services Act* o *Cybersecurity Act.* Otro indicador de politización es la creación de organismos como ENISA (Agencia Europea De Ciberseguridad) o incorporación de centros nacionales de ciberseguridad en cada país miembro. Así como, la asignación de recursos presupuestarios que refuerzan la institucionalización de la ciberseguridad dentro de la agenda política europea.

El principal instrumento financiero de la Unión Europa en este ámbito es el *Digital Europe Programme* (DIGITAL) (European Commission, s. f.). Se trata de un programa de financiación aprobado oficialmente en 2021 y vigente hasta 2027, con el objetivo de acelerar la transformación digital de Europa y reforzar su autonomía tecnológica. En materia de ciberseguridad, el programa financia el desarrollo y despliegue de centros de operaciones de seguridad (SOC) y sistemas de detección de amenazas para conseguir una tecnología propia de ciberseguridad, expertos e infraestructura, sin tener que depender tanto de proveedores externos. Por lo tanto, la politización refleja un enfoque en el que la ciberseguridad se integra en la construcción del mercado digital europeo y en la consolidación de un orden digital basado en reglas y valores compartidos. Una evolución hacia un enfoque regulado y coordinado, dejando atrás uno fragmentado y voluntario, puesto que el concepto de ciberseguridad se concibe como bien público colectivo que requiere una respuesta conjunta.

En el caso de Estados Unidos, ha securitizado la ciberseguridad al situarla en el centro de de su estrategia de defensa y seguridad nacional, tras concebir el ciberespacio como ámbito con potencial de amenaza estratégica y confrontación. Esto implica que el país eleva el nivel de prioridad estratégica, puesto que las amenazas cibernéticas se perciben no solo como riesgo técnicos o económicos, sino como desafíos estratégicos que pueden afectar a la soberanía nacional. La secularización requiere medidas excepcionales y una respuesta estratégica, como la creación del *U.S Cyber Command,* en 2009, un mando militar del Pentágono dedicado solo al ciberespacio. Esta diferencia no implica que uno de los actores ignore la dimensión presente

en el otro, sino que refleja prioridades estratégicas distintas de gestionar la seguridad. Ambos han transitado desde enfoques técnicos hacia concepciones más amplias e integrales de la ciberseguridad, pero la lógica que ha guiado este proceso ha sido diferente en cada caso.

La diplomacia digital constituye otro ámbito en el que se evidencian diferencias significativas entre la Unión Europea y Estados Unidos. En el caso de la UE, la promoción de normas y estándares internacionales en materia digital se manifiesta en su participación en foros multilaterales como las Naciones Unidas y el *Internet Governance Forum*. A través de estos espacios internacionales de diálogo y cooperación donde se negocian normas, principios y estándares se ejerce principalmente su diplomacia digital, al ser parte del proceso de la llamada gobernanza internacional de la ciberseguridad.

En primer lugar, en el marco de las Naciones Unidas, se debaten cómo debe aplicarse el derecho internacional al ciberespacio. El 16 de diciembre de 2020, la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y la Política de Seguridad presentaron una nueva Estrategia de Ciberseguridad de la UE que es defendida en este foro (European Commission, 2020). La UE defiende que el ciberespacio no es un espacio sin reglas, sino que debe regirse por el derecho internacional público, la protección de los derechos humanos y el respeto a la soberanía estatal.

A través de distintos grupos de trabajo, como el *Group of Govermental Experts* (GEE) creado por la ONU en 2004, se definen las normas internacionales sobre el uso del ciberespacio por los Estados. Se trata de un grupo reducido de expertos gubernamentales como diplomáticos y especialistas nombrado por la ONU para debatir sobre la aplicación del derecho internacional en el entorno digital. “El derecho internacional es la base del compromiso compartido por los Estados de prevenir conflictos y mantener la paz y la seguridad internacionales”, (United Nations General Assembly, 2021, p. 20), también en el ciberespacio, donde su aplicación se configura como un elemento esencial para garantizar la estabilidad, la confianza mutua y la previsibilidad en un dominio cada vez más central para la seguridad y las relaciones internacionales. La UE y sus Estados miembros defienden en estos foros la idea de que el derecho internacional existente incluido el respeto a la soberanía estatal debe aplicarse también al ámbito digital.

Por otro lado, el *Internet Governance Forum* (IGF), fue creado en 2006 como resultado de la Cumbre Mundial sobre la Sociedad de la Información (WSIS) y está formado por gobiernos, organizaciones internacionales, empresas tecnológicas y sociedad civil. A diferencia de otros

foros más centrados en seguridad o defensa, este se trata del "principal espacio de las Naciones Unidas para el diálogo inclusivo y multilateral sobre la gobernanza de Internet" (Forus, 2025) . La UE utiliza este foro como plataforma de diálogo multilateral para promover un modelo de internet abierto, seguro y basado en reglas, en el que se garantiza la protección de datos, la libertad de expresión y la transparencia en el uso de tecnologías digitales. Se defiende que el ciberespacio es un espacio global e interconectado, cuya gobernanza deber ser multilateral y multiactor.

Al igual que la UE, Estados Unidos promueve normas y estándares en foros multilaterales, pero su enfoque está más vinculado a la seguridad nacional y a la competencia geopolítica. Uno de los foros más relevantes donde la UE no participa es el Quad (*Quadrilateral Security Dialogue)*. Se trata de una asociación diplomática entre Estados Unidos, Japón, India y Australia que defendía que la ciberseguridad es uno de los ámbitos clave de cooperación estratégica. Dentro del foro, la ciberseguridad se trata como tema central de seguridad y tecnología.

En este contexto, se observa como EE.UU utiliza la diplomacia digital como instrumento para defender su liderazgo tecnológico, gestionando amenazas procedentes de actores rivales. Este enfoque se traduce en el uso de instrumentos como la atribución pública directa de ciberataques. Estados Unidos realiza declaraciones directas desde la Casa Blanca, el Departamento de Justicia o el Departamento del Tesoro, identificando explícitamente a los responsables de ciberataques, como en los casos de *SolarWinds* o *Microsoft Exchange*, para aumentar los costes políticos de las actividades hostiles y reforzar la disuasión frente a futuros ataques. Estos ataques que han afectado a agencias gubernamentales o infraestructuras críticas han reforzado la percepción del ciberespacio como un ámbito de confrontación estratégica. En consecuencia, la respuesta estadounidense ha combinado medidas de refuerzo interno, llegando a destinar más de 20.400 millones de dólares en ciberseguridad federal (Deltek GovWin, 2024). El país invierte significativamente más que la Unión Europea en ciberseguridad, la inversión europea se encuentra más fragmentada entre la Comisión Europea y los Estados miembros y es globalmente inferior.

A pesar de las diferencias estructurales entre ambos actores en su concepción del ciberespacio y en sus instrumentos de actuación, ambos actores presentan importantes convergencias que han favorecido el desarrollo de una cooperación transatlántica en materia de ciberseguridad. Ambos coinciden en la importancia de "preservar un Internet, abierto, libre, conectado

globalmente, interoperable, no fragmentado y estable" (Internet Governance Forum, s. f.) , sin embargo, este modelo de Internet abierto se enfrenta al modelo basado en la soberanía digital estatal, promovido por potencias como China y Rusia.

Por un lado, el modelo abierto se fundamenta en la idea de que el ciberespacio es un bien público cuya estabilidad depende del mantenimiento de estándares comunes, del libre flujo de información y de la cooperación multilateral. Muchas empresas tecnológicas funcionan globalmente porque Internet está interconectado, por ejemplo, Amazon, Microsoft o Netflix operan simultáneamente en Europa y Estados Unidos gracias a la interoperabilidad de las redes digitales. Para ello, se creó en 2021 un foro de cooperación entre la Unión Europea y Estados Unidos conocido como *Trade and Technology Council* (TTC). Este constituye un mecanismo de coordinación destinado a armonizar estándares tecnológicos y regulatorios para garantizar la interoperabilidad de productos digitales. Asimismo, ambos actores defienden que los datos deben poder circular internacionalmente para el comercio y economía digital de forma segura, dejando constancia de esto en el acuerdo firmado entre ambos actores en 2023 sobre *EU-US Data Privacy Framework* (U.S. Department of Commerce, s. f.). Se trata del principal acuerdo transatlántico en materia de transferencia de datos personales, que cuenta con estándares comunes de protección de datos y mecanismos de supervisión y reclamación.

El modelo de soberanía digital parte de la premisa de que el ciberespacio debe estar bajo el control del Estado dentro de sus fronteras, igual que el territorio físico. Debe de estar sometido de manera similar a otros ámbitos tradicionales de la soberanía digital, lo que se traduce en la regulación de contenidos, el control de los flujos de información y la supervisión de los datos dentro de sus fronteras. Este modelo puede contribuir a la fragmentación del ciberespacio global, un fenómeno que "recibe el nombre de *Splinternet* y consiste, principalmente, en que las autoridades restringen el acceso a ciertas páginas web o servicios" (El Economista, 2023) .

La coexistencia de estos dos modelos refleja una creciente competencia normativa en el ámbito internacional, que se mantiene de forma visible en diversos foros internacionales como en el *Open-Ended Working Group* (OEWG) de la ONU. En él, Rusia tiene una posición muy clara sobre el control soberano de su espacio digital y, para ello, propone negociar una Convención Internacional de la ONU sobre seguridad de la información, que establezca normas vinculantes y un mayor control estatal del entorno digital.

La cooperación en materia de ciberseguridad se ha intensificado en el marco de alianzas políticas y de seguridad ya existentes. La Organización del Tratado del Atlántico Norte

(OTAN) ha incorporado de manera progresiva el ciberespacio como un ámbito relevante de actuación. Al principio durante los años 2000, la OTAN veía la ciberseguridad como un asunto técnico vinculada a la protección de redes informáticas y sistemas de comunicación. Sin embargo, los diversos incidentes explicados en capítulos anteriores como el caso de Estonia en 2007, mostraron como un ciberataque podía tener consecuencias comparables a las de una crisis de seguridad tradicional, afectando no solo a la infraestructura tecnológica, sino también a la estabilidad política y económica del país. Como respuesta, la OTAN comenzó a reconocer la necesidad de incorporar la ciberdefensa a su agenda estratégica, lo que llevó a la creación del Centro de Excelencia de Ciberdefensa Cooperativa en Tallin, destinado a la investigación, formación y cooperación en materia de seguridad digital. Desde 2010, la organización ha reconocido oficialmente el ciberespacio como un dominio de operaciones, iniciando así un proceso de adaptación progresiva a las nuevas amenazas del entorno digital.

Otro ámbito de convergencia es la creciente preocupación por la protección de procesos democráticos frente a la desinformación, la manipulación informativa y otras formas de interferencia digital. Tras las acusaciones de injerencia rusa en las elecciones estadounidenses de 2016, se reforzaron sus sistemas electorales y se promovió una mayor supervisión de las plataformas digitales. Entre las medidas destaca la declaración del Departamento de Seguridad Nacional (DHS) del sistema electoral como infraestructura crítica nacional para evitar hackeos o manipulación electoral y su refuerzo de coordinación con NSA, FBI y CISA.

Posteriormente, otra medida adoptada por la *European Commission* en 2018 fue la creación del Código de Buenas Prácticas contra la Desinformación, destinado a la lucha contra la desinformación en Internet. Se trata de un acuerdo voluntario entre las grandes compañías tecnológicas como Meta, Google, X o TikTok y la Comisión Europea que incentiva a asumir mayor responsabilidad en la protección del ecosistema informativo digital. Un instrumento de autorregulación voluntaria empleado especialmente para prevenir campañas de desinformación y manipulación electoral online.

Un caso destacado fue durante las elecciones al Parlamento Europeo de 2019, cuando las principales plataformas digitales implementaron medidas de transparencia publicitaria, eliminación de cuentas falsas o *bots*[8] y cooperación con verificadores de datos. Las plataformas debían enviar informes sobre las campañas y contenido eliminado, concluyendo que estas respondían más rápido a la desinformación y mejoraban la transparencia de anuncios públicos.

[8] Un bot es una aplicación de software que efectúa automáticamente tareas repetitivas en una red.

Sin embargo, se la Comisión Europea señaló la necesidad de medidas más fuertes y reforzó el código posteriormente en 2022. La gran medida fuerte fue la *Digital Services Act* aprobada por la Unión Europea, de carácter obligatorio por ley para crear un entorno digital seguro, transparente y responsable.

Asimismo, ambas potencias han desarrollado en los últimos años varios proyectos conjuntos en ciberseguridad y diplomacia digital, especialmente desde 2021, con el objetivo de coordinar respuestas antes las ciberamenazas. La principal iniciativa conjunta es el *Trade and Technology Council* (TTC) establecido durante la Cumbre UE-EE.UU que tuvo lugar el 15 de junio de 2021 en Bruselas para "impulsar la transformación digital y colaborar en el desarrollo de nuevas tecnologías a partir de los valores democráticos que comparten, especialmente el respeto de los derechos humanos" (European Commission, 2024). Es una plataforma institucionalizada de diálogo y coordinación de alto nivel con reuniones organizadas y periódicas. Se encuentra dividido en grupos de trabajo especializados que abordan ámbitos como la seguridad de las tecnologías de la información y la comunicación o la lucha contra la desinformación.

El objetivo principal es evitar la fragmentación normativa, buscar evitar divergencias y promover marcos interoperables que preserven un espacio digital transatlántico coherente. Un ejemplo de potencial fragmentación normativa se observa en las diferencias entre el Reglamento General de Protección de Datos Europeo (GDPR) y el sistema estadounidense de protección de datos. En EE.UU no existe una ley federal única equivalente al GDPR, sino que cuentan con un sistema más flexible, fragmentado por sectores, priorizando a la innovación y mercado. Para evitar que estos sistemas digitales sean incompatibles ha creado un marco transatlántico de transferencia de datos personales, conocido como *Data Privacy Framework,* que permite restablecer flujos de datos entre ambas economías bajo garantías de protección de la privacidad. Con ello se consigue un orden digital global con el liderazgo de ambos actores en la gobernanza tecnológica internacional, alineado con principios democráticos.

6. Retos y perspectivas futuras

En la era digital actual, la ciberseguridad y la diplomacia digital han dejado de ser en una preocupación exclusiva de los departamentos de TI para convertirse en un elemento clave en la estabilidad política, económica y social de los Estados. La creciente dependencia hacia los sistemas interconectados y tecnologías de la información ha generado importantes

oportunidades de desarrollo e innovación, pero también ha dado lugar a nuevas amenazas complejas que trascienden fronteras y desafían los mecanismos tradicionales de gobernanza internacional.

Uno de los principales retos es el incremento en la complejidad y sofisticación de las amenazas en el ámbito de la ciberseguridad. Los ataques informáticos han evolucionado desde acciones aisladas distribuidas por accidente o como prueba de habilidad técnica hacia operaciones altamente estructuradas y tecnológicamente complejas. Entre las amenazas más relevantes se encuentra el *ransomware*, un tipo de software malicioso que bloquea el acceso a los sistemas, exigiendo un pago económico a cambio de su recuperación. El 81,1% de los ciberincidentes contra organizaciones europeas en 2025 estuvieron relacionados con *ransomware*, seguido de brechas de datos (15.2%), lo que evidencia el uso creciente de tácticas de extorsión digital complejas y coordinadas (Philpot, 2025). Esto demuestra que el cibercrimen ya no es una actividad aislada, sino una industria organizada y rentable. Funcionan como si fueran empresas organizadas, con estructuras jerarquías y con servicios como el denominado *Ransomware as a service* (RaaS), mediante el cual desarrolladores especializados crean y comercializan herramientas de ataque que pueden ser adquiridas o alquiladas por otros delincuentes.

Esto se encuentra alineado con otro desafío para los Estados que consiste en reforzar la ciberseguridad y la vigilancia frente a amenazas digitales sin vulnerar derechos fundamentales como la privacidad y la libertad individual. El problema no reside únicamente en la existencia de instrumentos de vigilancia, sino en los límites de su utilización y en la legitimidad de su aplicación. Por lo tanto, es necesario la existencia de controles judiciales, supervisión parlamentaria y organismos independientes para garantizar que las capacidades de vigilancia no se utilicen de manera arbitraria.

En este contexto, otro de los principales retos a los que se enfrentan los Estados y las organizaciones es la escasez de profesionales especializados en ciberseguridad. En el ámbito europeo, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) presenta un estudio oficial basado en datos de 1.080 profesionales de organizaciones europeas, principalmente de sectores críticos como energía, transporte o salud (ENISA, 2025). Este advierte de la persistencia de una brecha de talento y de competencias en ciberseguridad, lo que limita la detección de amenazas y la capacidad de respuesta ante incidentes. El incremento constante de ciberataques agrava esta situación, puesto que, en 2023, “el promedio mundial alcanzó 1.984 ataques semanales por organización, un 21% más” (GÉANT, 2025). Este crecimiento

evidencia que la demanda de especialistas en ciberseguridad aumenta a un ritmo superior al de la formación y disponibilidad de profesionales. La falta de profesionales dificulta la implementación de programas de formación y concienciación en materia de seguridad, lo que provoca que empelados y usuarios carezcan de los conocimientos necesarios para identificar y prevenir riesgos. Como consecuencia, el factor humano continúa siendo uno de los elementos más vulnerables dentro de la ciberseguridad, que producen fallos como el uso de contraseñas débiles o mala configuración de sistemas.

La Unión Europea se enfrenta actualmente a importantes retos de naturaleza tecnológica, política y geoestratégica que condicionan su capacidad para actuar como un actor global sólido y autónomo. “El 69% del mercado europeo de servicios en la nube está controlado por Amazon, Microsoft y Google” y “el 92% de los datos occidentales se almacenan en infraestructuras estadounidenses” (Forbes, 2025). Esta situación genera una dependencia tecnológica significativa de proveedores externos, lo que limita la autonomía europea en sectores clave para la economía digital y la seguridad. Como respuesta a la creciente dependencia tecnológica externa, la Unión Europea ha impulsado iniciativas como GAIA-X, orientadas a desarrollar una infraestructura *cloud* europea que protege datos europeos. No obstante, este proyecto en desarrollo resulta insuficiente para reducir de forma sustancia la dependencia tecnológica de la Unión Europea.

Por otro parte, Estado Unidos cuenta con un reto de competencia tecnológica con China. El país ha llevado a cabo una estrategia sistemática para convertirse en líder mundial con programas como el 14º Plan Quinquenal, donde se establecen objetivos claros para dominar industrias estratégicas como la IA, los semiconductores o telecomunicaciones 5G. Para Estados Unidos, esto supone el riesgo de perder su posición dominante en la economía digital global, por ello, se imponen restricciones a la exportación de chips avanzados y maquinaria tecnológica. Los chips son la base material de casi toda la economía digital contemporánea, son imprescindibles para el funcionamiento de dispositivos y sistemas digitales, por lo que su control tiene un gran valor económico y estratégico.

En cuanto a las perspectivas futuras, se prevé que el enfoque *security by design* constituya una de las principales orientaciones emergentes en el ámbito de la ciberseguridad contemporánea. Este modelo propone un replanteamiento de la responsabilidad en materia de ciberseguridad, que consiste en anticiparse y reducir las amenazas desde el origen, incorporando mecanismos de protección en la propia arquitectura del sistema. Para ello, es esencial asignar un papel

central a los desarrolladores, fabricantes y proveedores de servicios digitales. Así, la seguridad se configura como un elemento intrínseco al proceso de desarrollo tecnológico, lo que permite fortalecer la resiliencia global del entorno digital.

Asimismo, la UE orienta su política hacia el refuerzo de su capacidad tecnológica e industrial europa en cuestiones como la inteligencia artificial, la ciberseguridad o la nube, con el programa *Digital Europe* 2025-2027, adoptado por la Comisión en marzo 2025 (European Commission, 2025). Con este programa se pretende pasar de una posición principalmente reguladora a otra más autónoma y competitiva para reducir dependencias estratégicas externas. Se plantea reforzar su cooperación digital con países afines como Japón, Corea del Sur, Canadá, Singapur o India, con el fin de fomentar un espacio digital seguro justo e inclusivo (European Commission, s. f.). Estos países reúnen tres rasgos que interesan potencialmente a la Unión Europa: capacidad tecnológica, alineamiento político-normativo y utilidad estratégica que permita la construcción de estándares globales.

En conjunto, puede afirmarse que ambos actores seguirán desempeñando un papel central en la configuración del orden digital global, aunque desde enfoques diferentes. Mientas la Unión Europea aspira a construir soberanía digital a través de la regulación y la autonomía estratégica, Estados Unidos busca consolidar su liderazgo global mediante la seguridad nacional.

7. Conclusiones y recomendaciones

Tras el análisis de la ciberseguridad y diplomacia digital en perspectiva comparada abordado en el presente trabajo de fin de grado, se confirma que la transformación digital ha alterado profundamente la naturaleza de las Relaciones Internacionales. Lejos de ser un ámbito únicamente técnico, el ciberespacio se ha consolidado como terreno de importancia política y estratégica, parecido a otros espacios tradicionales como el mar, territorio o aire. El futuro del ciberespacio dependerá en gran medida de la capacidad de los actores internacionales para equilibrar sus intereses estratégicos con la necesidad de mantener un entorno digital seguro y estable.

En primer lugar, la digitalización del sistema internacional no puede analizarse desde un único enfoque teórico que capte su complejidad. El ciberespacio introduce dinámicas simultáneas de competencia, cooperación y construcción normativa, lo que obliga a adoptar una perspectiva plural. En ese sentido, el realismo permite explicar la creciente competencia tecnológica y el

uso de la ciberseguridad como instrumento de poder, especialmente en el caso de Estados Unidos. Por otro lado, el liberalismo permite comprender la cooperación y la creación de normas. Este enfoque subraya el reconocimiento de los Estados a la interdependencia digital y al esfuerzo de establecer normas comunes, algo muy destacado en la Unión Europea. Por último, el constructivismo aporta una dimensión fundamental al destacar que el ciberespacio no solo queda determinado por intereses materiales, sino también por ideas, valores o identidades. En este ámbito, la Unión Europea vuelve a ser especialmente relevante, ya que, en su acción exterior, los valores como la protección de datos, los derechos digitales, y la defensa de la democracia frente a la desinformación, tienen especial relevancia.

En relación con la Unión Europea, la evolución de la política europea de ciberseguridad evidencia un proceso de institucionalización y europeización, articulada en torno a la construcción de una soberanía digital compartida. Este proceso ha aumentado el protagonismo de estructuras comunes de coordinación y respuesta, como son la Directiva NIS2, que refuerza las obligaciones de ciberseguridad en sectores críticos, y la Agencia de la Unión Europea para la Ciberseguridad (ENISA), cuyo papel se ha visto progresivamente fortalecido. En este contexto, la ciberseguridad deja de concebirse como una cuestión sectorial y se transforma en una dimensión estructural de la resiliencia europea.

En el ámbito de la diplomacia digital europea, el análisis confirma que la UE actúa fundamentalmente como una potencia normativa, cuyo poder se ejerce de manera más indirecta que el de otras potencias, pero no por ello menos efectiva, al influir en la configuración de estándares, reglas y prácticas en el entorno digital. Esto se explica por su capacidad para configurar marcos regulatorios que trascienden su propio espacio jurídico y condicionan el comportamiento de actores externos. Sin embargo, también es identificado una tensión de fondo en la estrategia europea, puesto que su liderazgo normativo no siempre va acompañado de suficientes capacidades tecnológicas propias. La UE continúa dependiendo en gran medida de actores externos, especialmente en ámbitos clave como los servicios en la nube, los semiconductores o plataformas digitales, lo que plantea interrogantes sobre la viabilidad de una autonomía estratégica plenamente efectiva en el entorno digital.

Por su parte, el análisis de Estados Unidos evidencia un modelo diferente al europeo, en el que la seguridad nacional y el mantenimiento del liderazgo tecnológico, mantienen una relación directa con la seguridad nacional y la diplomacia digital. Se refleja una creciente securitización del ciberespacio, donde las tecnologías digitales no solo impulsan la innovación, sino que

también consideran recursos estratégicos esenciales en la competencia geopolítica. Esta dinámica refuerza la consolidación de políticas orientadas al control de infraestructuras críticas y al impulso de alianzas internacionales en materia de ciberseguridad.

Su diplomacia digital se caracteriza por un enfoque más pragmático y orientado a resultados, en el que destacan la proyección de influencia, la cooperación estratégica y el papel central del sector privado. Sin embargo, este modelo no está exento de problemas, ya que surgen tensiones entre seguridad y derechos fundamentales, en ciertas políticas diseñadas para reforzarla ciberseguridad o control tecnológico. Esta dualidad de modelos refleja como el poder ya no se define exclusivamente en términos materiales, sino también, en función de la capacidad de establecer reglas o controlar tecnologías.

A partir de los resultados obtenidos, pueden formularse varias recomendaciones orientadas a reforzar la coherencia y la eficiencia de las estrategias de ciberseguridad y diplomacia digital en ambas potencias. En primer lugar, se recomienda el avance hacia una mayor integración entre las dimensión tecnológica, normativa y estratégica, evitando enfoques fragmentados que limiten la capacidad de respuesta ante amenazas complejas. Aplicado a la UE, este actor ha sido muy fuerte en el plano normativo, es decir, en la creación de normas y estándares internacionales, pero necesita reforzar más su base tecnológica e industrial. Esto significa invertir de forma sostenida en sectores críticos como semiconductores, inteligencia artificial, y crear infraestructuras estratégicas propias, para no depender siempre de capacidades externas.

En segundo lugar, resulta fundamental promover una cooperación transatlántica más estructurada y operativa en materia digital. Esto se consigue mediante la creación de mecanismos institucionalizados de cooperación, como el foro conocido como *Trade and Technology Council (TTC)* entre la Unión Europea y Estados Unidos. Aunque existen intereses divergentes, la convergencia en valores democráticos y en la percepción de amenazas comunes ofrece una base sólida para el desarrollo de marcos conjuntos de ciberseguridad con sistemas de alerta temprana o canales de comunicación permanentes entre autoridades competentes. La inclusión de enfoques preventivos, como el *security by design,* permite reducir riesgos antes de que se conviertan en crisis y mejora la capacidad de respuesta de las instituciones y de la sociedad.

Asimismo, se recomienda fortalecer la cooperación público-privada, especialmente en el caso de Estados Unidos, donde el sector tecnológico desempeña un papel fundamental. Grandes empresas tecnológicas concentran una parte significativa de las capacidades digitales. Por ello,

los gobiernos necesitan cooperar con ellas para afrontar desafíos como la ciberseguridad o la gestión de infraestructuras digitales. Sin embargo, esta cooperación no debe producirse sin control, sino que debe estar acompañada por mecanismos de supervisión que garanticen la transparencia y el respeto por los derechos fundamentales.

En definitiva, el trabajo permite concluir que la ciberseguridad y la diplomacia digital no solo constituyen nuevas áreas de política pública, sino que representan una transformación profunda de las lógicas del poder internacional, en la que la tecnología, las normas y las narrativas se entrelazan para configurar el sistema internacional del siglo XXI. La rivalidad en materia de ciberseguridad y diplomacia digital entre los principales actores internacionales no depende únicamente a diferencias regulatorias, sino que va más allá y se inserta en una competencia geopolítica más amplia por el poder y el control de los recursos estratégicos.

8. Bibliografía

Akamai. (s. f.). *What is a computer security incident response team (CSIRT)?* https://www.akamai.com/es/glossary/what-is-computer-security-incident-response-team-csirt#:~:text=Un%20CSIRT%20es%20un%20grupo,datos%20o%20ataques%20de%20ransomware

Alonso Lecuit, J. (2018). *Evolución de la agenda de ciberseguridad de la Unión Europea*. Real Instituto Elcano. https://media.realinstitutoelcano.org/wp-content/uploads/2018/11/ari121-2018-lecuit-evolucion-agenda-ciberseguridad-union-europea.pdf

Amazon Web Services (AWS). (s. f.). *What is a bot?* https://aws.amazon.com/es/what-is/bot/

Castro Martínez, A. (2019). *Ciberdiplomacia y comunicación institucional: La presencia de la diplomacia digital española en redes sociales*. *Revista Estudios Institucionales, 6*(10), 45–72. https://www.researchgate.net/publication/333605048_Ciberdiplomacia_y_comunicacion_institucional_La_presencia_de_la_diplomacia_digital_espanola_en_redes_sociales_Cyber-diplomacy_and_institutional_communication_The_presence_of_Spanish_digital_diplomacy_

Centro Criptológico Nacional. (s. f.). *Glosario y abreviaturas (CCN-STIC-401)* *https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=173.html*

Consejo de la Unión Europea. (2024, noviembre 18). *Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace*. https://www.consilium.europa.eu/es/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/

Cybersecurity and Infrastructure Security Agency. (s. f.). *Russia threat overview and advisories*. U.S. Department of Homeland Security. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia

Daim, T., Yalcin, H., Mermoud, A., & Mulder, V. (2024). *Exploring cybertechnology standards through bibliometrics: Case of National Institute of Standards and Technology*. *World Patent Information*. https://technology-observatory.ch/academic_publication/exploring-cybertechnology-standards-through-bibliometrics-case-of-national-institute-of-standards-and-technology/article.pdf

Deltek GovWin. (2024, mayo 8). *Defense IT and cyberspace activities FY 2025 budget highlights*. https://iq.govwin.com/neo/marketAnalysis/view/Defense-IT-and-Cyberspace-Activities-FY-2025-Budget-Highlights/7785

Department of Homeland Security. (2026, February 19). *About DHS*. https://www.dhs.gov/about-dhs

Dirección General de Seguros y Fondos de Pensiones. (n.d.). *Reglamento de resiliencia operativa digital (DORA)*. Ministerio de Economía, Comercio y Empresa. https://dgsfp.mineco.gob.es/es/Paginas/Reglamento-de-Resiliencia-Operativa-Digital-DORA.aspx

El Economista. (2023, agosto 12). *Qué es el "splinternet" y por qué perjudica el ecosistema de internet y a sus millones de usuarios*. https://www.eleconomista.es/telecomunicaciones/noticias/12403114/08/23/que-es-el-splinternet-y-por-que-perjudica-el-ecosistema-de-internet-y-a-sus-millones-de-usuarios.html

Estrella Digital. (2025, mayo 3). *El ciberataque que dejó sin luz a Ucrania: así fue el ataque a la red eléctrica.* https://www.estrelladigital.es/articulo/seguridad-defensa/ciberataque-que-dejo-luz-ucrania-asi-fue-ataque-red-electrica/20250503171316430896.html

European Commission. (2020, diciembre 16). *The EU's cybersecurity strategy for the digital decade*. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2024). *EU-US Trade and Technology Council*. https://commission.europa.eu/topics/international-partnerships/eu-us-trade-and-technology-council_es

European Commission. (2025, marzo 28). *Work programme 2025–2027 of the Digital Europe Programme (DIGITAL)*. https://digital-strategy.ec.europa.eu/en/library/work-programme-2025-2027-digital-europe-programme-digital

European Commission. (s. f.). *Digital Europe programme*. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

European Commission. (s. f.). *International digital strategy for the European Union*. https://digital-strategy.ec.europa.eu/en/policies/international-digital-strategy

European Commission. (s.f.). *Digital partnerships*. https://digital-strategy.ec.europa.eu/en/policies/partnerships

European Union Agency for Cybersecurity (ENISA). (2025, diciembre 8). *NIS investments 2025*. https://www.enisa.europa.eu/publications/nis-investments-2025

Forbes. (2025, octubre 10). *El 69% del mercado cloud y el 90% de los datos europeos, en manos estadounidenses*.https://forbes.es/economia/812244/el-69-del-mercado-cloud-y-el-90-de-los-datos-europeos-en-manos-estadounidenses/

Foreign and Commonwealth Office. (2014, May 28). *Digital diplomacy, social media and the Holy See*. GOV.UK. https://www.gov.uk/government/news/digital-diplomacy-social-media-and-the-holy-see

Fortinet. (s. f.). *Ataque a la cadena de suministro de SolarWinds*. https://www.fortinet.com/lat/resources/cyberglossary/solarwinds-cyber-attack

Forus. (2025). *The Internet Governance Forum: Why civil society should engage in IGF 2025*. https://www.forus-international.org/es/news/the-internet-governance-forum-why-civil-society-should-engage-in-igf-2025

GÉANT. (2025). *Global cyber attacks surge 21% in Q2 2025 — Europe experiences the highest increase of all regions.* https://security.geant.org/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/

Goss, C. (2023, April 17). *DOD's FY24 cyber budget*. Federal Budget IQ. https://federalbudgetiq.com/insights/dods-fy24-cyber-budget/

Hernández Mendoza, A., & Hernández Martínez, A. M. (2025). *Las Relaciones Internacionales en la era digital*. *Anuario Mexicano de Asuntos Globales, 3*(3), 231–

264. https://anuarioasuntosglobalesumar.com/ojs/index.php/AMAG/article/view/113/113

Hurst Publishers. (2024). *Waste Land: A World in Permanent Crisis. Robert D. Kaplan* [Video]. YouTube. https://www.youtube.com/watch?v=0uXCfeZOWjw

IBF Solutions. (s. f.). *El nuevo Cyber Resilience Act.* https://www.ibf-solutions.com/es/noticias-y-conocimientos/articulos-tecnicos-y-noticias-sobre-el-marcado-ce/il-nuevo-cyber-resilience-act

IBM. (s.f.). *What is ransomware?* https://www.ibm.com/es-es/think/topics/ransomware

International Telecommunication Union. (s. f.). *Cybersecurity*. ITU. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Internet Governance Forum. (s. f.) The Internet we want. https://www.intgovforum.org/en/content/the-internet-we-want

IT User. (2021, septiembre 13). *Así ha cambiado la seguridad nacional y la ciberdefensa tras el 11-S.* https://www.ituser.es/actualidad/2021/09/asi-ha-cambiado-la-seguridad-nacional-y-la-ciberdefensa-tras-el-11s

Jack Donnelly. (2000). *Realism and international relations*. Cambridge University Press. https://assets.publishing.service.gov.uk/media/5a74ee6040f0b65c0e845a62/AB_12-11-14_Digital_strategy.pdf

Jorge Ricart, R. (2021). *Aprendizajes para el contexto empresarial ante ciberataques por ransomware: el caso del Colonial Pipeline*. Fundación ESYS. https://fundacionesys.com/wp-content/uploads/2022/12/Paper-Aprendizajes-Colonial-Pipeline-RaquelJorgeRicart-CC.pdf

Kaspersky. (s. f.). *Ransomware WannaCry: todo lo que necesita saber*.https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

Kaspersky. (s. f.). *What is an IP address?* https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address

Kirchgaessner, S. (2025, febrero 28). *Trump administration retreats in fight against Russian cyber threats*. The Guardian. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia

Malwarebytes. (s.f.). *¿Qué es el malware?* https://www.malwarebytes.com/es/malware

Manili, A. (2019). *Perspective trends of international cooperation in the field of cybersecurity* (tesis de grado). LUISS UNIVERSITY . https://tesi.luiss.it/25416/1/634812_MANILI_ARIANNA.pdf

National Association of Criminal Defense Lawyers. (s. f.). *Computer Fraud and Abuse Act (CFAA)*. https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

Observatorio de Ciberseguridad. (2024). *El ciberataque a Estonia de 2007*. https://observatoriociber.org/el-ciberataque-a-estonia-de-2007/

Organización del Tratado del Atlántico Norte. (1949). *The North Atlantic Treaty*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty

Ottis, R. (2008). *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Pankov, N. (2021, mayo 12). *How Colonial Pipeline managed its ransomware attack*. Kaspersky.https://www.kaspersky.es/blog/pipeline-ransomware-mitigation/25302/

Philpot, J. (2025, noviembre 5). *ENISA cybersecurity threat landscape report 2025: Key takeaways for SMEs*. European DIGITAL SME Alliance. https://www.digitalsme.eu/enisa-cybersecurity-threat-landscape-report-2025-key-takeaways-for-smes/

Reyes, E. (2025, junio 23). *Crecen 900% los ciberataques por tensiones entre EU e Irán*. *Expansión*. https://expansion.mx/tecnologia/2025/06/23/conflcito-estados-unidos-iran-crece-ciberataques

Rockwell Automation. (s. f.). *Las lecciones del ciberataque a Colonial Pipeline*. https://www.rockwellautomation.com/es-mx/company/news/articles/lecciones-del-ciberataque-a-colonial-pipeline.html

Roudani, C. (2025, marzo 13). *Hybrid warfare and defense 5.0: Morocco, a strategic ally of the United States*. Modern Diplomacy.: https://moderndiplomacy.eu/2025/03/13/hybrid-warfare-_and-defense-5-0-morocco-a-strategic-ally-of-the-united-states/

Saaid, Z. (2025). *Cyberspace reading through the prism of international relations theories: Morocco as a practical case*. *European Open Science Journal*. https://eu-opensci.org/index.php/politics/article/view/8172

Sevilla Robles, M. A. (2020). *Resumen del contenido de la unidad*. Universidad de Guadalajara Virtual. http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/3088/1/Resumen%20del%20Contenido%20de%20la%20Unidad.pdf

SPYSCAPE. (2023). *Inside the troll factory: Russia's Internet Research Agency*. https://spyscape.com/article/inside-the-troll-factory-russias-internet-research-agency

The White House. (2003, February). *The national strategy to secure cyberspace*. https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf

The White House. (2018, September). *National cyber strategy of the United States of America*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Theohary, C. A. (2024). *Use of force in cyberspace* (IF11995). Congressional Research Service. https://www.congress.gov/crsproduct/IF11995#:~:text=According%20to%20State's%20then%2Dlegal,causing%20airplanes%20to%20crash%20by

Towards connecting through conflicting: Book review of *The Age of Unpeace: How connectivity causes conflict* by Mark Leonard. (n.d.). Institute for a Greater Europe. https://institutegreatereurope.com/publications/commentary-pieces/mark-ruttes-imminent-european-union-leadership-opportunity/

U.S. Department of Commerce. (s. f.). *Data Privacy Framework program overview*. https://www.dataprivacyframework.gov/Program-Overview

U.S. Government Accountability Office. (2025, April 29). *Cyber diplomacy: The Bureau of Cyberspace and Digital Policy's efforts to advance U.S. interests* (GAO-25-108445) https://www.gao.gov/products/gao-25-108445

Unión Europea. (s. f.). *Agencia de la Unión Europea para la Ciberseguridad (ENISA)*. https://european-union.europa.eu/institutions-law-budget/institutions-and-

bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_es

UNIR. (s. f.). *¿Qué es hardware?* https://www.unir.net/revista/ingenieria/que-es-hardware/

UNIR. (s. f.). *¿Qué es software?* https://www.unir.net/revista/ingenieria/que-es-software/

United Nations General Assembly. (2021, July 14). *Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (A/76/135)*. https://docs.un.org/es/a/76/135

United Nations Office for Disarmament Affairs. (2022, March). *The UN norms of responsible state behaviour in cyberspace*, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

9. Anexos:

Anexo 1. *Contexto geopolítico contemporáneo: aportaciones de Kaplan y Leonard*

La obra *Waste Land: A World in Permanent Crisis* de Robert D.Kaplan ofrece un análisis del debilitamiento del orden liberal internacional caracterizado por un escenario inestable entre actores con intereses divergentes. Tras la caída de la URSS se pensaba que Internet sería abierto, global y cooperativo, con poca rivalidad digital. Sin embargo, en los años 2000, con casos como las operaciones de ciberespionaje atribuidas a China contra Estados Unidos o los ataques en Estonia, se observan los primeros indicios que sostienen la idea de Kaplan, de que el sistema internacional se encuentra en una crisis permanente, donde se desarrollan constantes tensiones, conflictos regionales y rivalidades estratégicas que configuran un entorno internacional volátil.

Este enfoque resulta especialmente útil para analizar el papel del ciberespacio en la geopolítica contemporánea, puesto que el ámbito digital se ha convertido en un nuevo escenario de competencia estratégica donde se plantean tensiones del sistema internacional. Las rivalidades entre potencias se trasladan al entorno digital en forma de ciberataques contra infraestructuras críticas, campañas de desinformación o incluso robos de propiedad intelectual. Estas prácticas no constituyen actos de guerra en el sentido tradicional, pero demuestran una crisis permanente porque generan tensiones de forma continua que traspasan las fronteras.

Asimismo, Mark Leonard, en *The Age of Unpeace*, demuestra cómo la conexión entre países también crea conflictos. Esto aplicado al ciberespacio, significa que los Estados, al estar interconectados, pueden utilizar esa conexión como una herramienta de presión o conflicto. Por ejemplo, Estados Unidos ha restringido el acceso de China a determinados semiconductores avanzados, utilizando la interdependencia como forma de presión.

En conjunto, estas aportaciones permiten entender el cómo el comportamiento de las potencias en el ciberespacio son el reflejo de cambios globales. Las tensiones en el ciberespacio no son puramente técnicas, sino que se producen como consecuencia de la rivalidad entre países. Internet se ha convertido en un espacio donde los Estados defienden sus intereses y ejercen poder, igual que el mundo real.

COMILLAS UNIVERSIDAD PONTIFICIA CIHS

Curso 2025/2026

Anexo 2*: Declaración de uso de herramientas de IA generativa*

Nombre Grado/Máster:	**Business Analytics y Relaciones Internacionales (E6-Analytics)**
Nombre Alumno:	**Claudia García García**
Coordinador/a TFG/TFM:	**Daniel Pérez Fernández**
Nombre Director/a de TFG/TFGM:	**Juan Gonzalo Lugo Sanchiz**

Declaro que para la elaboración del presente Trabajo Fin de Grado / Trabajo Fin de Máster se ha utilizado inteligencia artificial generativa como herramienta de apoyo.	SÍ X	NO

1) Uso de la IA Generativo

Si tu respuesta ha sido SÍ, contesta a las siguientes preguntas. Si has contestado NO, pasa al apartado 2.

Uso ético

	SÍ	NO
¿A la hora de usar la herramienta IA, en los *prompts* utilizados has incluido datos de carácter sensible o de carácter personal (fotos de personas reales, datos personales, etc.)? *Si tu respuesta es afirmativa especifica cuáles.*		X
¿Has orientado tu uso a suplantar tu trabajo personal sin hacer una revisión crítica de la extraído en la herramienta IA? *Si tu respuesta es afirmativa especifica cuáles.*		X
¿Has tenido en cuenta las recomendaciones académicas que te han hecho específicamente en el Grado/Máster sobre lo que está permitido o no con la IA?	X	

Uso técnico realizado:

¿Qué herramientas has utilizado (ChatGPT, Copilot, Claude, Nano Banana….)? Especifica la versión o tipo de licencia.

ChatGPT 5

Marcar lo que corresponda:

☒ Generación de texto *(Especificar qué herramientas)* → ChatGPT 5

☒ Reformulación *(Especificar qué herramientas)* → ChatGPT 5

☒ Traducción / corrección *(Especificar qué herramientas)* → ChatGPT 5

☒ Sugerencia de estructura *(Especificar qué herramientas)* → ChatGPT 5

☒ Apoyo metodológico *(Especificar qué herramientas)* → ChatGPT 5

☒ Buscar o citar bibliografía *(Especificar qué herramientas)* → ChatGPT 5

☐ Generar contenido audiovisual (videos, infografías, audios, imágenes, gráficos. *Especifica en concreto qué contenidos has generado con IA además de citarlo correctamente en el trabajo.*

☐ Otros *(Especificar qué herramientas)* →

Confirmo que el contenido final ha sido revisado, corregido y validado íntegramente por mí como autor/a y asumo la plena responsabilidad académica del mismo.
La utilización de la IA no ha sustituido el análisis crítico, la reflexión personal ni el trabajo intelectual propio exigido en un TFG/TFM.

Firma: Claudia García García