Capítulo segundo

La gobernanza portuaria. Un elemento clave de la defensa nacional

Nicoletta González-Cancelas

Resumen

El presente capítulo defiende la necesidad urgente de repensar la gobernanza portuaria más allá de su tradicional enfoque logístico-comercial, situándola como una herramienta estratégica al servicio de la seguridad nacional. En un contexto marcado por amenazas híbridas, inestabilidad geopolítica e interdependencia tecnológica, gestionar bien los puertos significa proteger el interés general, garantizar la resiliencia del Estado y salvaguardar la seguridad ciudadana.

Se destaca que los puertos, como infraestructuras críticas, presentan vulnerabilidades estructurales que ya no pueden tratarse como cuestiones accesorias. La propuesta central del capítulo gira en torno a un nuevo modelo de gobernanza basado en tres pilares: integración funcional, anticipación estratégica y corresponsabilidad institucional.

Una de las carencias más notables es la ausencia de indicadores estratégicos homogéneos que permitan evaluar no solo la eficiencia, sino la preparación, la resiliencia y la capacidad de respuesta del sistema portuario ante situaciones críticas.

Asimismo, se subraya la necesidad de abordar la condición dual (civil-militar) de muchas infraestructuras portuarias, promoviendo la planificación conjunta con las Fuerzas Armadas y los organismos de seguridad como un deber institucional, no como una excepción voluntaria.

El capítulo pone también el foco en Ceuta y Melilla, dos enclaves de alta sensibilidad geoestratégica que requieren una gobernanza diferenciada, inversiones sostenidas y protocolos de seguridad adaptados a su singularidad territorial.

En suma, se aboga por una visión de la gobernanza portuaria que combine liderazgo institucional, cultura de defensa y orientación al bien común como pilares para sostener la soberanía, la cohesión y la seguridad del país.

Palabras clave

Gobernanza, Seguridad nacional, Infraestructuras críticas, Integración, Resiliencia.

Port governance. A key element of national defence

Abstract

This chapter defends the urgent need to rethink port governance beyond its traditional logistic-commercial approach, placing it as a strategic tool at the service of national security. In a context marked by hybrid threats, geopolitical instability and technological interdependence, good management of ports means protecting the general interest, ensuring the resilience of the State and safeguarding citizen security.

It is emphasized that ports, as critical infrastructures, present structural vulnerabilities that can no longer be treated as ancillary issues. The central proposal of the chapter revolves around a new governance model based on three pillars: functional integration, strategic anticipation and institutional co-responsibility.

One of the most notable shortcomings is the absence of homogeneous strategic indicators to assess not only the efficiency, but also the preparedness, resilience and responsiveness of the port system in critical situations. It also underlines the need to address the dual status (civil-military) of many port infrastruc-

tures, promoting joint planning with the Armed Forces and security agencies as an institutional duty, not a voluntary exception.

The chapter also focuses on Ceuta and Melilla, two highly sensitive geostrategic enclaves that require differentiated governance, sustained investments and security protocols adapted to their territorial uniqueness. In short, it advocates a vision of port governance that combines institutional leadership, defence culture and orientation towards the common good as pillars to sustain the country's sovereignty, cohesion and security.

Key words

Governance, National security, Critical infrastructure, Integration, Resilience.

1 Introducción

La conexión entre los puertos y la defensa nacional no es nueva. A lo largo de la historia, los puertos han sido mucho más que espacios logísticos o comerciales; han sido puntos de apoyo estratégico, puertas de entrada y salida, y nodos fundamentales para garantizar la soberanía territorial. Hoy, en un contexto de incertidumbre geopolítica, de amenazas híbridas y con una creciente dependencia de las cadenas logísticas globales, esta dimensión estratégica se hace aún más evidente.

Este capítulo aborda la cuestión de la gobernanza portuaria desde una óptica que trasciende lo puramente económico o logístico (Bagchi y Paik, 2001). Las condiciones actuales exigen algo más: una mirada estructural que incorpore la seguridad, la resiliencia y la capacidad de respuesta ante riesgos complejos y cambiantes (Mohsendokht et al., 2025).

No se trata de militarizar la gestión portuaria, sino de comprender que los puertos, como infraestructuras críticas del Estado, deben estar preparados para proteger sus funciones esenciales. Esto implica revisar marcos normativos, repensar relaciones institucionales y proponer esquemas de coordinación que integren a actores civiles y militares en un plano operativo y no solo protocolario.

El texto se articula en seis apartados que no buscan cerrar un modelo, sino explorar críticamente los límites y potenciales de la gobernanza portuaria desde una perspectiva estratégica. En primer lugar, se cuestiona la suficiencia del modelo tradicional ante los desafíos actuales y, a continuación, se examina la condición de los puertos como infraestructuras críticas y vulnerables. En tercer lugar, se esbozan elementos que podrían orientar una gobernanza más adaptada al siglo XXI, sin imponer un marco definitivo. El cuarto apartado se centra en Ceuta y Melilla, no como casos periféricos, sino como espacios cuya singularidad requiere atención prioritaria. En quinto lugar, se recogen propuestas operativas y cuestiones abiertas que podrían orientar un debate más profundo sobre el rediseño institucional. Finalmente, se ofrecen unas conclusiones que no pretenden cerrar la discusión, sino invitar al diálogo informado y a la construcción colectiva de soluciones.

En definitiva, este capítulo no pretende ofrecer una respuesta cerrada ni definitiva, sino aportar una base crítica y argumentada

desde la que repensar el papel de los puertos en un entorno cada vez más inestable, interdependiente y vulnerable. Se analiza cómo la condición de infraestructura crítica exige nuevas formas de protección y coordinación, y se identifican debilidades estructurales en la actual gobernanza en materia de seguridad. Quedan cuestiones abiertas, entre otras, cómo integrar eficazmente esta dimensión sin renunciar al carácter civil, abierto y orientado al desarrollo económico del sistema portuario, que se desarrollan más adelante en el texto. La intención es clara: contribuir a una reflexión colectiva y plural sobre cómo adaptar la gobernanza portuaria a los desafíos estratégicos del presente sin perder de vista a las personas, a quienes, en última instancia, este sistema debe servir y proteger.

2 Límites del modelo tradicional de gobernanza portuaria

2.1 Evolución normativa e institucional

Durante las últimas décadas, la gobernanza portuaria en España se ha configurado a través de un modelo descentralizado, de carácter landlord, que ha permitido a las autoridades portuarias gestionar con un notable grado de autonomía bajo la coordinación de Puertos del Estado (Notteboom y Winkelmans, 2001). Este diseño institucional ha respondido con eficacia a los retos derivados del crecimiento del tráfico marítimo, la modernización de infraestructuras y la necesidad de atraer inversión privada. Sin embargo, en su desarrollo, ha primado una lógica centrada en la eficiencia económica, el equilibrio financiero y la competitividad, dejando en un segundo plano cuestiones clave como la seguridad integral o la protección frente a riesgos no convencionales.

Este desfase normativo no es solo una cuestión técnica o semántica: tiene consecuencias prácticas que comprometen la capacidad del sistema portuario para responder adecuadamente a escenarios de crisis. Mantener una visión exclusivamente logística-comercial de los puertos implica que muchas decisiones clave, desde la asignación de recursos hasta la planificación de infraestructuras, sigan guiándose por criterios de eficiencia o rentabilidad económica, sin integrar de forma estructural la dimensión de seguridad y protección. Esto limita la capacidad de anticipación frente a amenazas híbridas, ralentiza la coordinación con organismos de defensa o interior y dificulta la inclusión de los puertos en estrategias nacionales de seguridad.

En última instancia, no redefinir esta base jurídica y conceptual conlleva un riesgo claro: que los puertos continúen siendo tratados como meros espacios de tránsito de mercancías cuando en realidad ya son, y cada vez más, nodos geoestratégicos cuya protección forma parte del interés general del Estado y de la seguridad de la sociedad a la que sirven.

2.2 Reduccionismo logístico: carencias frente a amenazas híbridas

El enfoque tradicional ha tendido a reducir la gobernanza portuaria a una cuestión de rendimiento operativo y servicio al cliente. Esta visión, sin duda útil para mejorar la competitividad del sistema portuario español, presenta límites claros cuando se trata de anticipar o gestionar amenazas complejas como los ciberataques, las interferencias extranjeras, el sabotaje o la disrupción de las cadenas de suministro.

En un contexto de amenazas híbridas, donde las fronteras entre lo civil y lo militar se difuminan, los puertos requieren marcos de gobernanza capaces de integrar de forma estructural la seguridad, no como un añadido, sino como un componente esencial de la toma de decisiones. La ausencia de estructuras estables de coordinación entre organismos de defensa y seguridad, más allá de protocolos puntuales o figuras de enlace, representa una debilidad del sistema actual.

Este enfoque limitado a la eficiencia logística no ha sido exclusivo del sistema portuario español. En el contexto europeo, las políticas de transporte han priorizado durante años la competitividad del mercado interior y la liberalización de servicios, relegando la dimensión estratégica de los puertos a un plano secundario.

Aunque existen marcos normativos como la Directiva 2008/114/CE sobre infraestructuras críticas o iniciativas como el Centro Europeo de Excelencia para Contrarrestar Amenazas Híbridas *(Hybrid CoE),* los propios estudios del Parlamento Europeo han reconocido la falta de aplicación práctica coherente en muchos Estados miembros (Parlamento Europeo, 2021).

Esta desconexión entre discurso político y realidad operativa ha producido vacíos institucionales y una escasa preparación ante escenarios de amenaza compleja. En Estados Unidos, en cambio, se ha avanzado con anterioridad hacia una visión más estratégica, con leyes como el *Maritime Transportation Security*

Act (2002) (U. S. Congress, 2002) y programas como el *National Port Readiness Network,* que obligan a los puertos a integrar planes de seguridad ante situaciones de defensa nacional *(U. S. Department of Transportation,* 2024).

En Asia-Pacífico, regiones como el estrecho de Malaca han empezado a experimentar con marcos de protección híbrida ante ciberamenazas y piratería, reconociendo la urgencia de actuar desde una lógica multidimensional (Soh y Mak, 2024).

En este contexto, persistir en un modelo centrado exclusivamente en la eficiencia operativa implica asumir riesgos crecientes: desde ciberataques y sabotajes hasta fallos sistémicos en la cadena de suministros, pérdida de resiliencia territorial y erosión de la confianza ciudadana en la capacidad del Estado para proteger servicios esenciales *(Seattle Port Authority,* 2024).

Las consecuencias de mantener una visión excesivamente logística del puerto, sin una integración efectiva de la seguridad en la gobernanza, no son teóricas: ya se han materializado en impactos sociales y económicos concretos. Como referencias más recientes, en agosto de 2024, el puerto de Seattle sufrió un ciberataque que comprometió sus sistemas informáticos, afectando la operativa diaria y exponiendo datos personales de empleados y actores portuarios. Aunque no paralizó el tráfico marítimo, el incidente obligó a activar protocolos de emergencia, generó retrasos logísticos y evidenció la vulnerabilidad real de infraestructuras consideradas críticas *(Seattle Port Authority,* 2024).

Más grave fue el caso del puerto de Baltimore, donde el colapso del puente Francis Scott Key tras el choque de un buque portacontenedores en marzo de 2024 bloqueó durante casi tres meses el acceso a varias terminales. El incidente afectó a miles de trabajadores; interrumpió cadenas de suministro clave, como la del automóvil, y generó costes millonarios, poniendo de manifiesto la dependencia social de una gobernanza portuaria resiliente, integral y anticipatoria (Wikipedia, 2024).

Estos casos recuerdan que no adaptar los modelos de gestión portuaria al nuevo contexto de riesgo no solo compromete la eficiencia, sino también el bienestar de la sociedad y la seguridad nacional.

2.3 Hacia una visión sistémica y estratégica

Reconocer las limitaciones del modelo tradicional no implica deslegitimar sus logros. Al contrario, se trata de construir sobre sus fortalezas para dar un salto cualitativo. La gobernanza portuaria del siglo XXI debe incorporar una lectura estratégica que vincule directamente la gestión con la seguridad nacional y la resiliencia del Estado.

Esto exige reforzar la capacidad de anticipación, fomentar la interoperabilidad entre actores civiles y militares e introducir indicadores que midan no solo eficiencia logística, sino también vulnerabilidad, capacidad de respuesta y robustez institucional. El tránsito hacia esta visión sistémica pasa también por revisar la formación de los equipos directivos, la naturaleza de los órganos de gobernanza y los canales de colaboración con organismos de defensa y seguridad.

Uno de los déficits más evidentes en el modelo actual de gobernanza portuaria es la ausencia de indicadores específicos y comparables que midan la seguridad, la resiliencia o la capacidad de respuesta de los puertos frente a amenazas complejas. Si bien existen métricas de eficiencia operativa o rentabilidad económica, no se dispone de un sistema homologado que permita evaluar el grado de protección crítica, la interoperabilidad institucional o la madurez en ciberseguridad. La integración de estos indicadores en los cuadros de mando portuarios —en línea con los estándares que ya promueven organizaciones como EMSA, la Organización Marítima Internacional (OMI) o la Comisión Europea en el ámbito de la protección marítima— resulta indispensable para avanzar hacia un modelo de gobernanza transparente, proactivo y orientado al interés general.

La adaptación del modelo de gobernanza portuaria a las exigencias de seguridad del siglo XXI requiere una arquitectura institucional más interconectada, donde no solo intervengan Puertos del Estado y las autoridades portuarias, sino también actores clave en defensa y protección civil como todas las Fuerzas Armadas, la Guardia Civil, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), el CNI, el Instituto Nacional de Ciberseguridad INCIBE, Protección Civil, las capitanías marítimas o las agencias tributarias. A nivel europeo, la coordinación con EMSA (2020), ENISA (2022) y la Comisión Europea resulta igualmente imprescindible. Sin una visión compartida y sin indi-

cadores que permitan medir avances reales, en ciberseguridad, interoperabilidad o resiliencia crítica, se corre el riesgo de quedar en reformas discursivas sin operatividad concreta. Solo desde la colaboración, la transparencia y la evaluación continua se podrá construir un sistema portuario verdaderamente al servicio de la seguridad nacional y del bienestar social.

En definitiva, el actual modelo portuario ha sido útil y eficaz en un contexto de estabilidad, pero muestra signos de insuficiencia ante los retos que plantea un entorno global marcado por la inestabilidad, la presión tecnológica y los riesgos multidimensionales. La superación de estos límites es el primer paso para avanzar hacia un modelo de gobernanza que proteja eficazmente los derechos de la ciudadanía y esté genuinamente al servicio de la seguridad nacional y del bienestar colectivo.

3 Los puertos como infraestructuras críticas del Estado

3.1 Enfoque legal y técnico: normativa nacional y europea

El reconocimiento de los puertos como infraestructuras críticas ha dejado de ser una formulación simbólica para convertirse en una realidad jurídica con consecuencias operativas. Tanto la legislación europea como la normativa española han establecido un marco legal que obliga a tratar la seguridad portuaria como una dimensión estructural de la gestión, no como un elemento accesorio.

En el ámbito europeo, el primer gran impulso normativo fue la Directiva 2008/114/CE, centrada en la identificación y protección de infraestructuras críticas europeas (ICE). Esta norma, sustituida recientemente por la Directiva (UE) 2022/2557 (CER [Comisión Europea, 2022a]), (CER Directiva (UE) 2022/2557 [Directiva de Resiliencia de Entidades Críticas]) amplía el concepto de entidad crítica, introduce obligaciones específicas en materia de resiliencia y exige una evaluación de riesgos continua. Esta nueva directiva reconoce expresamente el papel de los puertos como nodos esenciales para la economía y la seguridad, y obliga a los Estados miembros a establecer marcos de cooperación interinstitucional entre autoridades civiles, militares y operadores privados.

En el plano nacional, la Ley 8/2011 y el Real Decreto 704/2011 articulan el Sistema de Protección de las Infraestructuras Críticas (SPIC). Este sistema, gestionado por el CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas), establece obli-

gaciones para los operadores designados como críticos (incluidas varias autoridades portuarias) como la elaboración de planes de seguridad del operador (PSO) y planes de protección específicos (PPE). Estos documentos deben coordinarse con todas las fuerzas y cuerpos de seguridad del Estado y actualizarse periódicamente.

Sin entrar en los aspectos operativos que otros capítulos abordarán con mayor profundidad, cabe señalar que la utilidad real de estos instrumentos depende en gran medida de su integración en la estrategia general de gobernanza portuaria. Cuando estos planes se gestionan como requisitos burocráticos o se mantienen aislados de la planificación estratégica, pierden eficacia como herramientas de protección. De ahí la importancia de que su elaboración, actualización y evaluación se vinculen estrechamente con la toma de decisiones, el reparto de competencias y los recursos asignados a la seguridad dentro del puerto.

Pese a la abundancia normativa, el marco legal presenta problemas de fragmentación y desconexión operativa. En muchas autoridades portuarias, los aspectos relacionados con la protección crítica siguen gestionándose como una función aislada, desconectada del núcleo estratégico y presupuestario. La falta de transversalidad entre los departamentos técnicos, los órganos de gobernanza y los responsables de seguridad dificulta una implementación coherente del enfoque de infraestructura crítica.

3.2 Vulnerabilidades actuales: físicas, operativas y digitales

Reconocer a los puertos como infraestructuras críticas implica asumir que están expuestos a una multiplicidad de riesgos, no solo desde una perspectiva externa, sino también desde dentro del propio sistema. Las vulnerabilidades físicas siguen siendo relevantes: accesos no controlados, zonas mal iluminadas, insuficiencia de barreras físicas o escasa capacidad de respuesta ante sabotajes o ataques deliberados (Comisión Europea, 2008a)[1]. A ello se suman los efectos del cambio climático, con infraestructuras expuestas al ascenso del nivel del mar, temporales más intensos o erosión costera. Casos como el colapso parcial del dique de abrigo del puerto de Gijón en 2014 o las inundaciones

[1] Esta directiva establece la necesidad de identificar y proteger infraestructuras críticas frente a amenazas físicas y lógicas, señalando expresamente la importancia de evaluar accesos, iluminación, y medidas de contención frente a sabotajes.

en infraestructuras del litoral andaluz muestran que los riesgos climáticos ya no son teóricos, sino una realidad operativa.

En el plano operativo, la comunidad portuaria española presenta una notable asimetría en capacidades y enfoques de seguridad, derivada de la convivencia de múltiples operadores (públicos, privados y mixtos) con niveles desiguales de responsabilidad, protocolos y cultura organizativa. Esta heterogeneidad ha dado lugar a élites técnico-operativas concentradas en determinados enclaves, mientras que otros puertos aún dependen de respuestas reactivas, escasamente profesionalizadas.

En muchos casos, las rutinas operativas no incorporan simulacros conjuntos ni ejercicios reales de coordinación, lo que compromete seriamente la capacidad de respuesta ante amenazas súbitas. La mera realización puntual de estos ejercicios no es suficiente: resulta imprescindible que estén enmarcados dentro de planes previamente definidos, con objetivos claros, responsabilidades asignadas y protocolos de coordinación interinstitucional validados. Solo así podrán cumplir su función real de preparación y evaluación continua del sistema.

La digitalización acelerada del entorno portuario ha abierto además nuevas ventanas de riesgo. Sistemas como los PCS *(Port Community Systems)*, TOS *(Terminal Operating Systems),* sensores, *Internet of Things* (internet de las cosas, IoT), cámaras de vigilancia, herramientas predictivas de tráfico o plataformas de trazabilidad son ya indispensables para la eficiencia. Sin embargo, esta infraestructura tecnológica ha crecido en muchos casos de forma descoordinada, sin un marco común de ciberseguridad ni una cultura de gestión de riesgos digitales. Esta fragmentación convierte a los puertos en blancos potenciales para ciberataques, sabotajes internos o manipulación de datos críticos (GonzálezCancelas, Molina y Soler., 2022: 340).

Los incidentes vividos en los últimos años en puertos internacionales han dejado claro que los riesgos digitales tienen impacto real. En 2022, un ciberataque contra el puerto de Amberes afectó gravemente la gestión de la carga durante varios días (Maritime Cyber Attack Database, 2022).

En 2021, el puerto de Marsella sufrió una intrusión que obligó a suspender temporalmente la operativa de varias terminales. Más conocido aún es el ataque al sistema de gestión de Maersk en 2017 (NotPetya) (Greenberg, 2018: 45), que paralizó el tráfico marítimo de la compañía a nivel global y afectó también a termi-

nales en España. En todos estos casos, el verdadero punto débil no fue la tecnología en sí, que, como cualquier sistema complejo, puede ser atacada, sino la ausencia de planes de contingencia sólidos, estructuras de respaldo funcionales y personal preparado para actuar ante una disrupción digital. La vulnerabilidad no residía tanto en el software como en la falta de gobernanza efectiva frente a una amenaza inminente.

En el caso español, aunque algunos puertos han tomado la delantera, el conjunto del sistema portuario carece todavía de una estrategia nacional de ciberseguridad homogénea. No todos los puertos tienen planes de contingencia digitales actualizados, ni protocolos de coordinación en caso de ataques múltiples ni personal con formación específica en gestión de incidentes críticos. Esto los convierte en puntos débiles ante amenazas híbridas, donde los ciberataques pueden coincidir con sabotajes físicos, desinformación o presión geopolítica coordinada.

A estas vulnerabilidades se suma una falta generalizada de inversión en resiliencia estructural. Pocos puertos españoles han incorporado metodologías avanzadas como el análisis de vulnerabilidad cruzada, que permite anticipar cómo un fallo en un sistema puede afectar a otros, o la simulación de escenarios de disrupción compleja, fundamentales para entrenar respuestas en situaciones extremas. Además, la dependencia de proveedores únicos para servicios críticos, unida a una escasa planificación ante colapsos operativos y a una cultura de prevención todavía débil, limita la capacidad del sistema portuario para adaptarse, resistir y recuperarse. Esta fragilidad no solo compromete la seguridad portuaria, sino que puede poner en riesgo funciones esenciales para la defensa y la seguridad nacional.

3.3 La seguridad portuaria como función de la gobernanza

La protección de los puertos no puede seguir tratándose como un subsistema aislado o accesorio, al margen del resto de funciones estratégicas. La seguridad, física, digital y operativa, debe formar parte del núcleo estructural de la gobernanza portuaria, al mismo nivel que la planificación logística o la gestión económica. Gobernar un puerto es también garantizar que su comunidad esté protegida frente a riesgos reales y emergentes. No como un trámite final, sino como una responsabilidad pública irrenunciable, porque todo modelo de gobernanza que aspire a ser legítimo debe comenzar por asegurar el derecho a una infraestructura

segura, estable y confiable para todos (Instituto Español de Estudios Estratégicos, 2020).

Del mismo modo, las inversiones en ciberseguridad, especialmente aquellas vinculadas a infraestructuras críticas o sistemas operativos estratégicos, deben coordinarse con el Ministerio de Defensa y los organismos competentes en ciberseguridad nacional, como el Mando Conjunto del Ciberespacio, el CNPIC o el INCIBE, con el fin de garantizar su coherencia, eficacia y alineamiento con las prioridades de la seguridad del Estado (Ministerio de Defensa, 2023).

Esta perspectiva coincide con los resultados presentados por Gómez Díaz et al. (2023: 7), quienes destacan que la gobernanza digital portuaria requiere estructuras sólidas de coordinación institucional y marcos estandarizados de actuación que integren desde el inicio la seguridad como variable estructural del desarrollo tecnológico.

Esta integración exige una redefinición del reparto de competencias y de las responsabilidades institucionales. Si bien el modelo landlord ha favorecido la autonomía portuaria y la eficiencia operativa, también ha propiciado una notable disparidad en la implementación de políticas de seguridad. Algunos puertos han avanzado en protocolos específicos y sistemas de protección más integrados, mientras que otros aún operan con esquemas básicos o poco actualizados. Esta asimetría de capacidades y de prioridades debilita la cohesión del sistema portuario en su conjunto y entra en tensión con los principios de seguridad nacional, que exigen una respuesta homogénea y coordinada ante riesgos que no distinguen entre nodos «mayores» y «menores» (Comisión Europea, 2008b).

El establecimiento de un marco común de gobernanza en materia de seguridad no puede quedar supeditado a la voluntad o capacidad individual de cada autoridad portuaria. La protección de los puertos como infraestructuras críticas requiere una coordinación estructural que trascienda el nivel local y se integre como parte del mandato estratégico de Puertos del Estado y los ministerios competentes en colaboración directa y permanente con los organismos competentes en defensa, inteligencia y seguridad nacional. Esta articulación interinstitucional no solo es deseable, sino necesaria, si se pretende construir un sistema portuario cohesionado, resiliente y alineado con los principios de seguridad del Estado (España, 2011).

La cooperación interinstitucional debe convertirse en una práctica ordinaria. La gobernanza portuaria necesita abrirse más decididamente a la colaboración estable con todas las Fuerzas Armadas, los servicios de inteligencia, la Guardia Civil, el CNPIC, el Departamento de Seguridad Nacional y los organismos responsables de ciberseguridad (Dunn-Cavelty, 2008). Esta colaboración no debe limitarse a emergencias ni a ejercicios anuales, sino formar parte de la gobernanza diaria. Esto implica participar en órganos de decisión, compartir la información y diseñar conjuntamente escenarios de crisis y protocolos de respuesta.

Además, la resiliencia debe ser una dimensión clave en la planificación de inversiones. La gobernanza futura no puede medir únicamente rendimiento económico o eficiencia operativa, sino también capacidad de resistencia. Se necesitan nuevos indicadores de evaluación que incluyan la robustez de los sistemas ante eventos disruptivos, la rapidez de recuperación, la redundancia de las infraestructuras críticas y la sostenibilidad institucional del puerto ante amenazas prolongadas; en definitiva, que incorporen criterios de defensa y continuidad institucional.

La seguridad debe entenderse no solo como protección, sino como condición de posibilidad para el funcionamiento del puerto y su contribución al interés general. Su integración efectiva en la gobernanza es una cuestión estratégica que afecta a la autonomía del Estado, a la robustez de la economía y a la estabilidad del entorno geopolítico.

Para avanzar hacia una gobernanza portuaria centrada en la protección como función estructural, es imprescindible ampliar y sistematizar la red de actores implicados. Además de las autoridades portuarias y Puertos del Estado, esta debe integrar de forma operativa a organismos como el CNPIC, todas las Fuerzas Armadas, el Centro Nacional de Inteligencia (CNI), Instituto Nacional de Ciberseguridad (INCIBE), las capitanías marítimas y Protección Civil, así como a agencias europeas como Agencia Europea de Seguridad Marítima *(European Maritime Safety Agency,* EMSA) o Agencia de la Unión Europea para la Ciberseguridad *(European Union Agency for Cybersecurity,* ENISA). La colaboración con la Agencia Tributaria y las fuerzas y cuerpos de seguridad del Estado debe pasar de ser reactiva a formar parte de una planificación estructurada y permanente. Solo así puede configurarse un modelo de gobernanza que anticipe, coordine y proteja en un

entorno marcado por la volatilidad y la complejidad de las amenazas contemporáneas.

4 Hacia un modelo de gobernanza portuaria adaptado al siglo XXI

4.1 Elementos clave del nuevo modelo: integración, anticipación y corresponsabilidad

Avanzar hacia un modelo de gobernanza portuaria adaptado al siglo XXI requiere integrar la seguridad como un eje estructural de gestión, reforzar la capacidad de anticipación frente a riesgos complejos y establecer mecanismos de corresponsabilidad entre todos los actores implicados. La seguridad debe dejar de ser un apéndice técnico para convertirse en un principio transversal que guíe las decisiones sobre inversiones, concesiones o diseño infraestructural. Del mismo modo, los puertos necesitan herramientas que les permitan anticiparse a amenazas híbridas mediante análisis de riesgos, simulaciones estratégicas o tecnologías predictivas. Por último, resulta indispensable redefinir las relaciones entre Puertos del Estado, las autoridades portuarias y los organismos de defensa y seguridad, bajo un marco común de responsabilidades compartidas, información coordinada y estándares homogéneos. Sin cohesión institucional y operativa, el sistema portuario seguirá siendo vulnerable.

4.2 Limitaciones institucionales y necesidad de un rediseño consensuado

Una de las debilidades más persistentes del sistema portuario español es la ausencia de una arquitectura institucional pensada para operar bajo presión estratégica o en escenarios de disrupción compleja. Aunque las autoridades portuarias cuentan con herramientas de planificación y operativas contrastadas en contextos normales, no disponen de una estructura de gobernanza adaptada a situaciones que requieren cooperación rápida, decisiones coordinadas y liderazgo compartido entre organismos civiles, militares y tecnológicos.

El caso del Prestige demuestra con crudeza lo que puede pasar cuando la gobernanza, la coordinación y la respuesta institucional no están a la altura del riesgo (Comisión Europea, 2003: 8). En 2002, el petrolero Prestige sufrió un accidente estructural

frente a la costa de Galicia, provocando un vertido masivo de fuel que afectó miles de kilómetros de costa, la pesca, el turismo, la salud pública y el medioambiente. Este episodio mostró no solo fallos técnicos, sino carencias profundas en la toma de decisiones, como la demora en conceder puerto refugio, la falta de protocolos para incidentes de contaminación de gran magnitud y los vacíos de responsabilidad institucional, lo cual intensificó el daño social y ambiental (Caballero-Miguez y Fernández-González, 2015).

Por tanto, situaciones como esta evidencian que la protección de infraestructuras críticas portuarias no puede limitarse a la eficiencia operativa: hace falta una gobernanza institucional robusta, estándares claros y coordinación anticipada entre autoridades locales, estatales y nacionales, así como capacidad real para actuar en crisis, no solo para reaccionar.

Esta carencia se traduce en fallos estructurales de coordinación horizontal y vertical. A nivel local, las relaciones entre autoridades portuarias, fuerzas de seguridad, servicios de inteligencia, operadores y administraciones locales no siempre están regladas ni protocolizadas más allá de marcos normativos generales. En el ámbito nacional, la vinculación entre Puertos del Estado y el conjunto del sistema de seguridad e inteligencia es fragmentaria, dependiente a menudo de la voluntad individual de los responsables institucionales.

Tampoco existe aún un espacio de gobernanza estratégica donde puedan confluir de forma estable todas las partes implicadas en la seguridad portuaria: operadores logísticos, administraciones públicas, cuerpos y fuerzas de seguridad, organismos de defensa y seguridad, centros de ciberseguridad, municipios, etc. Esta ausencia de espacios de encuentro impide la construcción de una visión compartida, la identificación conjunta de vulnerabilidades y la definición colectiva de objetivos de mejora.

En otros ámbitos estratégicos, como los corredores ferroviarios europeos de uso dual (civil y militar), la Unión Europea ha impulsado la creación de marcos de gobernanza integrados para facilitar la movilidad militar sin menoscabar la operatividad civil. Programas como el Military Mobility de la UE, coordinado por la Agencia Europea de Defensa (2023) y la Comisión Europea (2022b: 12), han promovido estándares comunes, interoperabilidad técnica e inversión conjunta en infraestructuras clave. Este modelo demuestra que la cooperación civil-militar es posible si se articula sobre estructuras compartidas, liderazgos coordinados

y objetivos claramente definidos (Agencia Europea de Defensa, 2023: 5). La gobernanza portuaria española, al no contar aún con mecanismos similares de integración, pierde la oportunidad de consolidar un espacio de corresponsabilidad estratégica con Defensa en un contexto de creciente complejidad geopolítica.

El desafío, por tanto, no es solo técnico, sino institucional y cultural. Requiere transitar desde un modelo basado en competencias estancas hacia uno que se fundamente en la corresponsabilidad operativa, el intercambio de información cualificada, la interoperabilidad de sistemas y la toma de decisiones colaborativa.

Este rediseño no puede imponerse desde un marco normativo unilateral. Debe construirse a través de un proceso deliberativo, abierto y basado en el consenso, en el que participen tanto los actores tradicionales de la gobernanza portuaria como los nuevos actores estratégicos que hoy forman parte esencial de su protección: servicios de inteligencia, centros tecnológicos, operadores digitales, instituciones europeas, etc.

Asimismo, distintos expertos han señalado que los actuales mecanismos de gobernanza en escenarios de emergencia presentan un grado elevado de dispersión, con protocolos poco integrados y una dependencia excesiva de terceros actores ajenos a la estructura portuaria o estatal. Esta fragmentación dificulta la respuesta rápida y coordinada ante crisis complejas y pone en evidencia la ausencia de un sistema que garantice liderazgo unificado, interoperabilidad funcional y mando efectivo cuando más se necesita (Tribunal de Cuentas Europeo, 2021).

La creación de este modelo renovado no puede limitarse a la adaptación formal de normas o a la introducción de nuevas estructuras. Exige una revisión profunda de los principios y valores que orientan la gestión portuaria: desde el principio de eficiencia hacia el principio de resiliencia, desde la descentralización sin coordinación hacia la gobernanza coherente, desde la lógica exclusivamente económica hacia una lógica integrada de servicio público estratégico (Linkov y Palma-Oliveira, 2017).

La experiencia europea en materia de movilidad militar ha puesto de relieve la necesidad de mecanismos de gobernanza integrados entre actores civiles y militares. El Action Plan on Military Mobility 2.0 de la Comisión Europea insiste en que las infraestructuras de doble uso, como los puertos, requieren marcos de cooperación estructurados que garanticen la interoperabilidad entre administraciones de transporte, organismos de defensa, autoridades

aduaneras y operadores privados. Este enfoque coordinado no solo mejora la eficiencia logística en tiempos de paz, sino que también refuerza la resiliencia estratégica ante crisis híbridas, ciberataques o despliegues de emergencia. Para ello, se promueve la creación de estructuras estables de gobernanza multinivel y planes conjuntos de protección, planificación y respuesta (Unión Europea, 2025: 7-9).

4.3 Formación, innovación y alineamiento europeo

Ninguna transformación será posible sin una evolución cultural interna. Es imprescindible reforzar la formación especializada del personal directivo portuario en materias como gestión del riesgo, defensa nacional, ciberseguridad, cultura de protección y cooperación civil-militar. Estos contenidos deben integrarse en los programas de Puertos del Estado, pero también en másteres universitarios y cursos técnicos ofrecidos a nivel nacional.

La innovación debe situarse al servicio de la protección estratégica. Muchas tecnologías disruptivas —*blockchain*, inteligencia artificial, sensórica inteligente y plataformas colaborativas— pueden ser grandes aliadas para mejorar la seguridad portuaria. Pero solo lo serán si se despliegan con criterio, interoperabilidad y visión de sistema.

Por último, este modelo debe alinearse con las principales estrategias europeas: la Directiva CER[2], la Estrategia Europea de Movilidad Sostenible[3], el Pacto Verde Europeo, la Brújula Estratégica de la UE y el marco de gobernanza digital definido por la Directiva Directiva (UE) 2022/2555 *(Network and Information Security 2)* NIS2[4]. España no puede permitirse una gobernanza portuaria anclada en el siglo XX si quiere seguir jugando un papel clave en la soberanía logística europea.

La dimensión europea también ofrece aprendizajes útiles. Las respuestas de la Comisión Europea y del Servicio Europeo de Acción Exterior al Tribunal de Cuentas subrayan la urgencia de mejo-

[2] *Directiva CER*: Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, relativa a la resiliencia de las entidades críticas, por la que se deroga la Directiva 2008/114/CE.

[3] Estrategia de Movilidad Sostenible e Inteligente: encauzar el transporte europeo hacia el futuro.

[4] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, sobre medidas para garantizar un elevado nivel común de ciberseguridad en toda la Unión.

rar la coordinación institucional en movilidad militar, alertando sobre la fragmentación normativa, la lentitud en la implementación de proyectos y la falta de visión compartida en situaciones críticas. Estos desafíos reflejan también disfunciones observables en la gobernanza portuaria nacional, especialmente en lo relativo a la articulación civil-militar en infraestructuras estratégicas (Comisión Europea y SEAE, 2025: 4-5).

5 Ceuta y Melilla como espacios estratégicos y prioritarios

5.1 Singularidad geoestratégica y funcional de los puertos de Ceuta y Melilla

Los puertos de Ceuta y Melilla representan una excepción dentro del sistema portuario español, no por su tamaño o volumen de tráfico, sino por el papel que desempeñan en la seguridad nacional, la soberanía territorial y la proyección exterior del Estado. Enclavadas en el norte de África, constituyen las únicas fronteras marítimas exteriores de la Unión Europea en dicho continente, lo que les confiere una función fronteriza única tanto en términos logísticos como geopolíticos (Comisión Europea, 2021).

Situados en el estrecho de Gibraltar, uno de los pasos marítimos más estratégicos del mundo, estos puertos actúan como nodos clave en el control del tránsito marítimo internacional, el abastecimiento energético, la movilidad de bienes y personas, y la proyección de capacidades del Estado en el entorno del Mediterráneo occidental y el Magreb.

Más allá de su dimensión geoestratégica, Ceuta y Melilla son infraestructuras esenciales para garantizar la continuidad de los servicios públicos, el acceso a productos básicos y la conectividad con la península. Su carácter insular y fronterizo, sin alternativa terrestre ni ferroviaria, les confiere una dependencia total del transporte marítimo, lo que incrementa su criticidad en términos de operatividad, abastecimiento y bienestar ciudadano.

El valor de Ceuta y Melilla radica en su función estructural para la seguridad nacional, la soberanía territorial y la proyección marítima del Estado. Ceuta (España, 1995a) y Melilla (España, 1995b) no son solo enclaves singulares por su localización geográfica, sino territorios plenamente integrados en la soberanía nacional,

cuya presencia institucional y funcional debe ser garantizada de forma continua y prioritaria (Cortes Generales, 1978)[5].

5.2 Vulnerabilidades específicas y retos no resueltos

A pesar de su importancia, ambos enclaves muestran signos de fragilidad institucional y operativa. El primer gran factor de riesgo es su aislamiento logístico: una interrupción en la cadena de suministro marítima (ya sea por un conflicto, un sabotaje, una crisis energética o un ciberataque) tendría un impacto inmediato en la población. La falta de redundancia convierte cada operación portuaria en una línea de vida.

Asimismo, la presión migratoria ha sido utilizada en ocasiones como elemento de desestabilización, lo que introduce una variable de seguridad híbrida constante. Las zonas portuarias, pese a contar con medidas de protección física y protocolos del Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (Código PBIP), no siempre disponen de sistemas específicos para gestionar situaciones de entrada masiva o tránsito irregular por vía marítima. A ello se suma un déficit estructural en inversión tecnológica, digitalización y protección cibernética, lo que limita su capacidad de respuesta ante amenazas complejas.

En materia de gobernanza, las autoridades portuarias de Ceuta y Melilla trabajan en un entorno institucional particular, en el que la colaboración con fuerzas de seguridad y cuerpos militares es frecuente, pero no siempre está sistematizada en estructuras estables o marcos normativos específicos. La dependencia de la voluntad de actores individuales o del contexto político ha generado desequilibrios en la continuidad institucional y en la implantación de soluciones de largo plazo.

5.3 Necesidad de un tratamiento estratégico diferenciado

Este diagnóstico evidencia la necesidad de avanzar hacia un modelo de gobernanza específico para Ceuta y Melilla, basado en su condición de puertos de Estado y de nodos geopolíticos

[5] «Las Cortes Generales podrán, por motivos de interés nacional, autorizar la constitución de una Comunidad Autónoma cuando su ámbito territorial no supere el de una provincia y no cuente con las características señaladas en el artículo 143.1» (artículo 144.b). Base legal de los estatutos de Ceuta y Melilla.

prioritarios. No se trata de establecer privilegios ni excepciones arbitrarias, sino de reconocer una realidad operativa que exige soluciones adaptadas, sostenibles y sólidamente integradas en la arquitectura nacional de seguridad.

Una propuesta de enfoque diferenciado debería incluir:

- El desarrollo de una estrategia nacional específica para enclaves fronterizos, que combine gobernanza portuaria, planificación de la defensa y proyección diplomática.
- La inclusión obligatoria de Ceuta y Melilla en los grandes programas de inversión, innovación y ciberseguridad impulsados por el Estado para las infraestructuras críticas.
- El diseño de protocolos de cooperación institucional permanentes, con participación de Puertos del Estado, las autoridades portuarias, organismos de defensa y seguridad y otros actores relevantes.
- La incorporación de estos puertos en foros internacionales sobre seguridad marítima, gestión de fronteras y protección de nodos estratégicos.
- El refuerzo de la dimensión ciudadana de la gobernanza: asegurar que la población perciba la seguridad, la continuidad de servicios y la presencia efectiva del Estado como garantías reales de cohesión e igualdad territorial.

En definitiva, Ceuta y Melilla deben ser tratadas como lo que son: espacios de soberanía estratégica. Proteger su operatividad, gobernanza y resiliencia no es solo una necesidad logística o territorial, sino una obligación institucional con las personas que allí viven y con la estabilidad del conjunto del Estado.

6 Propuestas operativas y conclusiones orientadas al debate

La seguridad portuaria no puede desvincularse de la defensa nacional. Los puertos son infraestructuras críticas cuya protección forma parte integral del sistema de seguridad del Estado. En un contexto de amenazas híbridas, interdependencia tecnológica y presión geoestratégica, cualquier vulnerabilidad en el sistema portuario compromete directamente la soberanía, la resiliencia institucional y el bienestar ciudadano. Por tanto, su gobernanza debe estar plenamente alineada con una visión de seguridad integral.

Una primera lección de este análisis es que el actual modelo de gobernanza, aunque eficaz en términos operativos y económicos, no está preparado para actuar bajo presión estratégica. Su diseño responde a un entorno estable, pero se muestra insuficiente ante riesgos complejos y cambiantes. La falta de una estrategia nacional coordinada de seguridad portuaria acentúa esa debilidad.

En segundo lugar, resulta evidente que la seguridad no puede gestionarse como una función aislada. Debe formar parte estructural de las decisiones sobre inversiones, planificación, digitalización y relaciones institucionales. La fragmentación normativa y la asimetría de capacidades entre puertos debilitan la cohesión del sistema, generando desigualdad en la protección que reciben las personas según el territorio donde viven o trabajan.

Para avanzar en esta integración real, es imprescindible desarrollar sistemas de indicadores estratégicos homogéneos que midan la preparación, resiliencia y capacidad de respuesta ante amenazas en todos los puertos del sistema. Estos indicadores deben formar parte de los cuadros de mando institucionales y ser utilizados en la toma de decisiones, auditorías y planificación presupuestaria. Sin métricas comunes no puede haber seguridad compartida.

Tercero, la protección de los puertos debe construirse desde una gobernanza compartida, donde participen activamente todas las Fuerzas Armadas, organismos de seguridad y ciberseguridad, autoridades civiles, sector privado y ciudadanía. La seguridad no puede depender de voluntades individuales, sino de estructuras permanentes y una cultura organizativa orientada al interés general.

Esta gobernanza debe asumir también el carácter dual de muchos componentes del sistema portuario, cuya infraestructura, conectividad y tecnología pueden y deben servir tanto a fines civiles como a necesidades estratégicas y de defensa. La planificación conjunta en este marco es una obligación institucional, no una opción.

En cuarto lugar, se subraya la relevancia geoestratégica de Ceuta y Melilla como enclaves singulares. No pueden ser tratadas como excepciones residuales. Su especificidad operativa y territorial exige una atención diferenciada y sostenida, basada en su valor como símbolos de presencia y compromiso del Estado.

Por último, este capítulo sostiene que cualquier transformación en la gobernanza portuaria debe tener un motor claro: el liderazgo institucional y una cultura orientada al servicio público. Gobernar bien los puertos no es solo optimizar flujos, sino gestionar riesgos, proteger soberanía y sostener la confianza del Estado, porque, al final, lo que está en juego no es solo la competitividad de las infraestructuras españolas, sino la seguridad y la dignidad de las personas.

Bibliografía

Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2022). Threat Landscape for Critical Sectors. ENISA.

Agencia Europea de Defensa. (2023). Military Mobility: Progress and Way Forward. Bruselas: Agencia Europea de Defensa.

Bagchi, P. K. y Paik, S. K. (2001). The role of public-private partnership in port information systems development. International Journal of Public Sector Management. 14(6), pp. 482-499.

CaballeroMiguez, G. y. Fernández-González, R. (2015). Institutional analysis, allocation of liabilities and third-party enforcement via courts: The case of the Prestige oil spill. Marine Policy. 55, pp. 90101. https://doi.org/10.1016/j.marpol.2015.01.003

Comisión Europea. (2003). Final report on the Prestige disaster (COM(2003) 105 final). Bruselas, Comisión Europea.

—. (2008a). Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Bruselas.

—. (2008b). Directiva 2008/114/CE del Consejo, relativa a la identificación y designación de infraestructuras críticas europeas y a la evaluación de la necesidad de mejorar su protección. Diario Oficial de la Unión Europea, L(345), pp. 75-82.

—. (2019). El Pacto Verde Europeo. Bruselas, Consejo de la Unión Europea.

—. (2020). Estrategia de Movilidad Sostenible e Inteligente: encauzar el transporte europeo hacia el futuro. Bruselas, Comisión Europea.

—. (2021). Schengen Borders Code Implementation Report. Bruselas.

—. (2022a). The Directive on the Resilience of Critical Entities (CER Directive) [en línea]. Bruselas, Comisión Europea. [Consulta: 2026]. Disponible en: https://ec.europa.eu

—. (2022b). Action Plan on Military Mobility 2.0 (COM(2022) 222 final). Bruselas: Comisión Europea.

Comisión Europea y Servicio Europeo de Acción Exterior. (2025). Replies to the European Court of Auditors Special Report on Military Mobility. COM-Replies-SR-2025-04 [en línea]. Unión Europea. [Consulta: 2026]. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2509

Consejo de la Unión Europea. (2022). Una Brújula Estratégica para la Seguridad y la Defensa – Por una UE que proteja a sus ciudadanos, valores e intereses. Bruselas.

Cortes Generales. (1978). Constitución Española [en línea]. Boletín Oficial del Estado, núm. 311, de 29 de diciembre de 1978. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/c/1978/12/27/(1)/con

Dunn-Cavelty, M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge.

EMSA. (2020). Overview of *Maritime Security* Measures in EU Ports. European Maritime Safety Agency.

España. (1995a). Ley Orgánica 1/1995, de 13 de marzo, del Estatuto de Autonomía de Ceuta [en línea]. Boletín Oficial del Estado, núm. 61, de 13 de marzo. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1995-6354

—. (1995b). Ley Orgánica 2/1995, de 13 de marzo, del Estatuto de Autonomía de Melilla [en línea]. Boletín Oficial del Estado, núm. 61, de 13 de marzo. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1995-6355

—. (2011). Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas [en línea]. Boletín Oficial del Estado, núm. 121, de 21 de mayo. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/rd/2011/05/20/704/con

Gómez Díaz, C. et al. (2023). Digital Governance Approach to the Spanish Port System: Proposal for a Port. Journal of Marine Science and Engineering. 11(2), p. 311. MDPI. https://doi.org/10.3390/jmse11020311

GonzálezCancelas, N., Molina Serrano, B. y SolerFlores, F. (2022). El impulso de la digitalización de los puertos del sistema portuario: gobernanza como factor clave [en línea]. Revista de la Facultad de Ingeniería. 38(2), pp. 338-352. Bogotá, Universidad de los Andes. [Consulta: 2026]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-34612020000200338

Greenberg, A. (2018). Sandworm: A New Era of Cyberwar. Nueva York, Doubleday.

Instituto Español de Estudios Estratégicos (IEEE). (2020). Seguridad marítima y gobernanza portuaria en España. Cuadernos de Estrategia. Madrid.

Linkov, I. y Palma-Oliveira, J. M. (eds.). (2017). Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains. Springer.

Maritime Cyber Attack Database (MCAD). (2022). Belgian port organisation SeaInvest hit by a ransomware attack [en línea]. Fruitnet. [Consulta: 2026]. Disponible en: https://maritimecybersecurity.nl/incident/B3KzwvQmVX

Ministerio de Defensa. (2023). Directrices para la coordinación en ciberdefensa nacional [en línea]. Gobierno de España. [Consulta: 2026]. Disponible en: https://www.defensa.gob.es/

Mohsendokht, M. et al. (2025). Resilience analysis of seaports: a critical review of development and research directions. Maritime Policy & Management, pp. 1-36.

Notteboom, T. y Winkelmans, W. (2001). Structural changes in logistics: how will port authorities face the challenge?. Maritime Policy & Management. 28(1), pp. 71-89.

Parlamento Europeo. (2021). Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats [en línea]. Directorate-General for External Policies. [Consulta: 2026]. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf

Port of Antwerp-Bruges. (2022). Cyberattack Disrupts Port Operations [en línea]. [Consulta: 2026]. Disponible en: https://www.portofantwerpbruges.com/en/news/cyberattack

Seattle Port Authority. (2024). Cyber Incident Briefing Report [en línea]. Seattle, Seattle Port Authority. [Consulta: 2026]. Disponible en: https://www.portseattle.org/news/port-cyberattack-archive

Soh, K. K. y Mak, C. K. (2024). Preventing Catastrophic Cyber–Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid *Maritime Security* in the Straits of Malacca and Singapore. Journal of Marine Science and Engineering. 12(3), p. 510. https://doi.org/10.3390/jmse12030510

Tribunal de Cuentas Europeo. (2021). The EU Civil Protection Mechanism: A rapid response tool, but value added limited by weaknesses in design and management. Luxemburgo, Oficina de Publicaciones de la Unión Europea. https://doi.org/10.2865/521161

Unión Europea. (2022). Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, relativa a la resiliencia de las entidades críticas, por la que se deroga la Directiva 2008/114/CE. Diario Oficial de la UE, L333, de 27 de diciembre, pp. 164-192.

—. (2025). Military Mobility: Annual Progress Report 2025. Bruselas, Servicio Europeo de Acción Exterior.

U.S. Congress. (2002). Maritime Transportation Security Act of 2002. Public Law 107-295. Washington D.C., Government Printing Office.

U.S. Department of Transportation. (2024). Francis Scott Key Bridge Incident Report. Washington D.C., U.S. Department of Transportation.

Wikipedia. (2024). Francis Scott Key Bridge collapse [en línea]. Wikipedia. [Consulta: 2026]. Disponible en: https://en.wikipedia.org/wiki/Francis_Scott_Key_Bridge_collapse