The Open University | PolicyWISE

Wise in 5: Smart Ports

Wise in 5 is a snapshot comparative guide to a public policy issue across the nations of the UK and Ireland. It helps you be PolicyWISE (Wales, Ireland, Scotland, England) in 5 (it takes just five minutes to read).

This briefing was published November 2025. It includes a summary of the latest policy developments across the nations, as well as related research from PolicyWISE, The Open University and PolicyWISE's university partners.

PolicyWISE creates neutral and constructive spaces for policy professionals and academics across the nations to develop relationships, respect and knowledge. We support and nurture a common culture of developing and sharing insight, knowledge, ideas and context from across the nations in a comparative and collaborative way.

	Engagement with Maritime 2050	Legislative duty for cybersecurity	Formal Ports policy	Smart ports strategy document
England	Strong	✚	✚	✚
Northern Ireland	Limited	▲	▲	▲
Republic of Ireland	N/A	✚	✚	▲
Scotland	Strong	▲	✚	▲
Wales	Moderate	▲	▲	▲
Key	✚ Yes		▲ No	

Wise in 5: Smart Ports

Overview

With around 95% of the UK's goods being transported by sea, ports play a pivotal role in national trade and economic performance. As such, their modernisation is no longer a choice – it is a necessity. Smart Ports, which integrate digital technologies and big data analytics with more traditional maritime operations, have driven early advances and will continue to be central in transforming shipping. They also provide relief to a sector facing increasing pressures and growing uncertainties, whilst offering an uplift to regional economies through the creation of high-skilled jobs. However, unlocking this potential at a national scale demands a coherent policy approach to ensure these systems are secure and interoperable.

This challenge is acute in the UK, where devolved governance means responsibilities and strategies surrounding port developments are distributed across the four nations. While ports policy – covering areas like planning and standards – is devolved, key functions such as customs, security, and international trade remain reserved to Westminster. The varying ownership structures also confound the issue, with ports being designated as private, municipal, or trust . Given this complex landscape, a more collaborative intergovernmental approach on matters of shared interest could overcome the fragmented governance structure and deliver more coherent outcomes.

Globally, maritime hubs such as Rotterdam and Hamburg are advancing the digital transformation of port infrastructure at pace. This is facilitated by strong collaborative ties between industry and academia that are further motivated by government-backed initiatives. In contrast, the UK's policy approach to Smart Ports remains fragmented. Yet without the coordinated and considered integration of technology into the underlying framework, the UK risks weakening its economic and competitive position, creating a digital divide between ports – home or away – and exposing critical infrastructure to cyber threats. The Huawei 5G controversy highlighted how a disjointed approach in matters relating to national infrastructure could result in long-term security implications.

Wise in 5: Smart Ports

Maritime Strategies

The UK Government's intentions for the sector are outlined in the Maritime 2050 strategy (2019), which is described as the "maritime strategy to take the UK into the second half of the 21st century." Technology and infrastructure were identified explicitly as two themes for focus, with recommendations of varying timelines laid out for each. A series of route maps were also published to outline how Government and industry would achieve those ambitions together. However, the 184 recommendations have been described within a Report of Session by the House of Commons Transport Committee as lacking focus and key performance indicators. Nevertheless, the UK Government continues to demonstrate its commitment through initiatives like Innovate UK Business Connect's Smart Shipping Community.

In comparison, owing to the scale of its maritime area compared to land, the Irish Department of Defence is leading efforts to create a National Maritime Security Strategy. This is intended to be in place by the end of 2025 and outlines plans for the domain over the next five years.

Matters of safety have also been openly recognised in regards to maritime autonomy, with the Maritime 2050 Report Summary stating, "Innovation needs to be able to flourish whilst safety standards are maintained". With port infrastructure forecast to be "'smart' by default" by 2050, the report similarly warns that "the rate of technological change is likely to make critical national infrastructure increasingly vulnerable to cyber-attack." However, current legislation fails to address the specific risks associated with Smart Ports.

Cyber Security

A cyber security code of practice is available for shipping alongside a Good Practice Guide for ports. Yet both documents are designed to help organisations identify potential risks and ways to mitigate them rather than setting an industry-specific standard that can safeguard the network for decades to come. The latter also relegates the management of digital assets to another specification of best practice, PAS 1192-5:2015. However, with more stakeholders involved than legacy infrastructure, closer scrutiny is needed of the technologies being installed and of who holds the resulting data – especially considering the military's renewed dependence on Britain's ports.

The UK Government intended for the National Cyber Strategy to inform the maritime sector of evolving threats and its responsibilities in facing them. It also identified that such an effort would require "a resilient cyber security and risk management capability". However, despite ambitions to remain by 2030 "a leading responsible and democratic cyber power," it has somewhat resigned itself to a supporting role. Instead, the responsibility has been largely transferred to industry at a time when cyber-attacks on ports and harbours are reported as having increased by 900%: "Whilst 'the onus is on industry to protect themselves' the UK aims to remain 'a centre of excellence for the provision of maritime cybersecurity solutions.'"

This introduces a degree of unpredictability to the standard of measures that are taken across the UK along with a lack of oversight on the technologies employed. It also relies on a willingness in industry to adopt any advised strategy when costs and over-regulation are already cited as potential disincentives – a fact that is not lost on the Government as it "is … seeking to improve uptake of the NCSC's cyber-security guidance".

Nation by Nation

England

The UK Government, through the Department for Transport, holds responsibility for ports in England. Relevant policies are laid out in the National Policy Statement for Ports, which is currently under review (as of August 2025). This is complemented by wider UK-level initiatives, such as those outlined in Maritime 2050 and the Freeports strategy, which encourage ports to develop as technologically advanced trading hubs. Tangible examples of digitisation also include the digital twin at the Port of Dover, partly funded by a grant from Innovate UK (a non-departmental public body), and the 5G network at the Thames Freeport. However, despite such implementations, there remains no specific government policy dedicated solely to Smart Ports or their technological consequences.

Smart Ports do feature as a subheading within Maritime 2050, which is consequently supported by stakeholders in England. Yet despite "outdated systems inside ports [being] particularly vulnerable to cyber-threats, and new digital systems [creating] new opportunities for intrusion", "any technological development in the UK's ports will be led by industry". Nevertheless, there is the expectation of 'Secure by Design' in their implementation.

The Government's intentions to improve cyber security capabilities within the sector are detailed in the National Strategy for Maritime Security. The Network and Information Systems Regulations (NIS) 2018 was also viewed as a viable tool to bring about such an uplift in standards. But this is sector agnostic and has not been updated to match the rapid pace of technological change that society is experiencing. Meanwhile, the threats posed within the maritime domain are monitored and acted upon by the Joint Maritime Security Centre, whilst overriding responsibility for UK cybersecurity, including that of UK ports, is held by the National Cyber Security Centre.

Wales

Ports governance in Wales is largely devolved, with Milford Haven the notable exception as a reserved trust port. However, the Welsh Government has not produced a single, comprehensive ports policy. Rather, ports are legislated through a mixture of transport and marine strategies, harbour orders and targeted, issue-driven initiatives – for example the Welsh National Marine Plan and ferry-port measures after Brexit.

The Welsh Government stated within The Wales Transport Strategy 2021 that it was its intention to "work with the Welsh Ports Group and other partners on a Welsh Ports and Maritime Strategy for Wales". However, no evidence has materialised publicly (as of August 2025).

Comparatively, Wales has shown active engagement with Maritime 2050, although it is not referenced within its own strategic frameworks and alignment is skewed towards areas of decarbonisation. Nevertheless, the Anglesey Freeport has been proposed in partnership with the UK Government to create a Digital Trade Corridor between Holyhead and Dublin. Business Wales has also promoted Innovate UK's Smart Shipping Community, and highlighted the potential for innovation within ports so much as aboard ships.

The Cyber Resilience Centre for Wales is the local provider of strategic cybercrime advice and protection for private organisations, although its services are focused on SMEs.

Scotland

Ports are a devolved matter in Scotland, with responsibility being held by Transport Scotland. Ports policy is also delivered within Scotland's National Transport Strategy and is supported by specific guidance such as Transport Scotland's Modern Trust Ports for Scotland: Guidance for Good Governance. Similarly, harbour orders made under the Harbours Act 1964 and other local instruments provide the statutory powers for individual ports.

To facilitate economic and sector growth, the UK Government proposed the development or advancement of regional maritime clusters within Maritime 2050 – collaborative partnerships between industry stakeholders, for which, Scotland is one. The Trust Port in Aberdeen is also benefiting from £1 million in funding, which is facilitating the rollout of 5G.

Scottish Enterprise published the Digital Voyage for Ports in Scotland during 2025 to serve as an initial exploration of opportunities "to boost smarter ports across … Scotland … [and] set the direction for future studies, plans, and investments across the sector." It is a comprehensive study, spanning all facets of the maritime world, and is the closest document any devolved nation has with regards to a national Smart Ports strategy.

Despite cybersecurity being a reserved policy, the Cyber and Fraud Centre Scotland supports the private sector in aligning with the Scottish Government's Cyber Resilience Strategy. In this, ministers recognise that "digital technology is key to Scotland's future" but that it must also be a nation that's "digitally secure and resilient."

Nation by Nation

Northern Ireland

Ports are a devolved matter in Northern Ireland, with oversight delegated to the Department for Infrastructure. However, there is no unified policy. Instead, ports are governed through a mixture of legislation (notably, the Harbours Act (Northern Ireland) 1970), harbour orders, trust-port arrangements and departmental guidance. This includes the Ports Review Policy (2025), which proposes greater commercial autonomy to aid investment in infrastructure. Consequently, there is no dedicated Smart Ports policy at the Executive level.

Belfast Harbour intends to become "the smartest regional port" through the Smart Port initiatives laid out in its 2035 Strategic Outlook. Admittedly, this will involve "an era of accelerated automation and artificial intelligence." Stena Line Freight has introduced a Smart Gate system to the same harbour, which involves online pre-registration and number plate recognition. It has also received funding in tandem with Manfreight through the Belfast 5G Innovation Region programme to utilise the technology within its daily operations; this scheme is led by the Department for Science, Innovation and Technology but funded by the UK Government.

Cybersecurity is missing from the 2035 Strategic Outlook, further highlighting the disparate approach that is being taken with regards to it and emerging technology. However, opportunities for the industry to align on such matters could be facilitated by the Centre for Secure Information Technologies at Queen's University Belfast, which is the UK's Innovation & Knowledge Centre for cyber security funded by EPSRC, Innovate UK, and Invest Northern Ireland. It is particularly experienced in delivering targeted skills development and industrial collaborations, making it a strategic asset , and has advised several departments within the UK Government on related matters.

Republic of Ireland

The Department for Transport in the Republic of Ireland has published the National Ports Policy (2013), which categorises ports by their national, regional, or local significance and provides a framework for their development. Owing to the economic contribution it brings, the exploitation of sea-borne income is also emphasised as a strategic priority within the national integrated marine plan, Our Ocean Wealth. While port infrastructure is managed by autonomous port authorities, neither the National Ports Policy nor Our Ocean Wealth refer to Smart Ports or the related issue of cybersecurity for digital infrastructure.

The 2024 Defence Policy Review and National Risk Assessment highlighted a range of risks and vulnerabilities that arise from Ireland's dependency on the maritime domain. In response, a public consultation was launched in early 2025 to shape an actionable maritime security strategy, which is expected to be finalised by the end of the year. While emphasis is placed upon infrastructure that is at sea or undersea, the strategy will also address "emerging threats and vulnerabilities", which could encompass those arising from Smart Ports. Such technologies are already being implemented – for example, the Innovez One port management system at the Port of Cork. A dedicated Maritime Security Unit was also established in late 2024, marking a significant institutional milestone toward safeguarding national interests at sea.

The nation's intentions around cybersecurity resilience are outlined within The Digital Ireland Framework, whilst the complementary National Cyber Security Strategy is currently being updated (as of August 2025). Meanwhile, the AI – Here for Good: National Artificial Intelligence Strategy for Ireland outlines how the nation can harness the potential of AI for economic and societal benefit, including smart capabilities. Yet the documents largely ignore the maritime setting. Little more can be gleaned from the European Good Practices for Cybersecurity in the Maritime Sector, which only makes the recommendation that such risks are considered throughout a project's lifecycle. This again relies on the expectations placed on industry rather than future-proofed standards. However, specificities surrounding digital vulnerabilities with regards to critical national infrastructure are managed by the National Cyber Security Centre while the Centre for Cybersecurity and Cybercrime Investigation at University College Dublin advises both the Irish Government and Garda.

In late 2024, the Smart Maritime and Offshore Wind Event was organised to consider "the challenges, opportunities and future directions across smart maritime technologies, cybersecurity, … and digitization" of Ireland's maritime sector. The bringing together of stakeholders in this way, including governmental representation, was designed to mark the beginning "of a cybersecure future for this sector."

Wise up – 5 policy points to take away

Five key points from what we've learnt above, which could be considered as part of further policy development and delivery in any or all of the nations.

1. Smart Ports call upon several areas of policy, which has resulted in disjointed and inapplicable strategies. As a result, there is now a clear need for more coordinated and focussed action that brings together expertise from devolved governments, industry stakeholders, and regulators.
2. Despite their growing importance, the explicit mention of Smart Ports is an obvious omission from many existing policy frameworks and published guidelines. These emerging technologies will only be considered fully if their terminology and objectives are consistently included in policy planning.
3. Cybersecurity is acknowledged within UK policy and remains largely reserved due to its sensitive nature. However, there is a critical need to explicitly integrate smart technologies and data-sharing initiatives into the policy framework. Establishing clear standards and protocols before widespread adoption is essential to safeguard national security and mitigate potential long-term consequences.
4. The UK's mix of private, public, and trust ports brings valuable diversity and flexibility to the sector. However, there would be a benefit to the UK Government clearly defining its overarching role and governance framework to ensure consistency, security, and alignment with national interests across all port types and nations.
5. Ports are central to the UK's economy, yet political attention often focuses on environmental initiatives. While decarbonisation is important, equal priority should be given to the security implications of Smart Ports to guarantee they remain competitive but safe, and capable of meeting future security demands. This includes ensuring that staff are trained to use these emerging technologies effectively and responsibly.

This briefing was authored by Hannah Ellis, PolicyWISE Intern, with support from Catherine May and the PolicyWISE team.

PolicyWISE

The Open University

Our focus and way of working makes us unique:

1. **Space:** We create and maintain neutral but constructive spaces for policy professionals and academics across the nations **to develop relationships, respect and** knowledge.
2. **Sharing:** We develop and support a common culture of sharing and developing insight, knowledge, ideas and context from across the nations in a comparative and collaborative way.
3. **Solutions:** We help governments focus on evidence-informed policy solutions for citizens and communities across the nations, informed by comparative and collaborative research and methods.

The Open University has been awarded £1m in funding from Dangoor Education to establish and run PolicyWISE. The funding has supported the launch of PolicyWISE in 2023 and our development over the following four years.

DANGOOR EDUCATION

Our offer

PolicyWISE works cross-nation on comparative research and knowledge exchange which will change and improve how governments and academics work together in and across nations to solve policy challenges.

Rapid Response Capability
We work at pace to support policy analysis, development, and consideration.

Comparative and Collaborative Analysis & Understanding
We are a partner of choice for collaborative and comparative projects, and we work across The Open University's four nations.

Wise in 5
The only regular snapshot comparative guide to public policy issues across the nations of the UK and Ireland.

Training
Utilising our distinct focus and skills we deliver impactful and dynamic training for any audience interested in learning how a comparative policy analysis and knowledge exchange can benefit their work.

Dewi Knight, Director

Get in Touch

www.policywise.org.uk

policywise@open.ac.uk

Follow us

policywise.bsky.social

PolicyWISE

Published November 2025